Sentinel™

Installations- und Konfigurationshandbuch

Juli 2018

Rechtliche Hinweise

Info zu diesem Handbuch und zur Bibliothek

Das *Installations- und Konfigurationshandbuch* enthält eine Einführung zu Sentinel und Informationen zur Installation und Konfiguration von Sentinel.

Zielgruppe

Dieses Handbuch ist für Sentinel-Administratoren und -Consultants gedacht.

Weitere Informationen in der Bibliothek

Die Bibliothek enthält folgende Informationsressourcen:

Verwaltungshandbuch

Enthält Informationen zur Verwaltung und zu den erforderlichen Aufgaben für die Verwaltung einer Sentinel-Bereitstellung.

Benutzerhandbuch

Enthält Informationen zum Konzept von Sentinel. Dieses Handbuch bietet außerdem einen Überblick der Benutzeroberflächen und Schritt-für-Schritt-Anweisungen für verschiedene Aufgaben.

Sentinel

Dieser Abschnitt enthält detaillierte Informationen zu Sentinel und dazu, wie Sie mit Sentinel eine Ereignisverwaltungslösung in Ihrer Organisation bereitstellen.

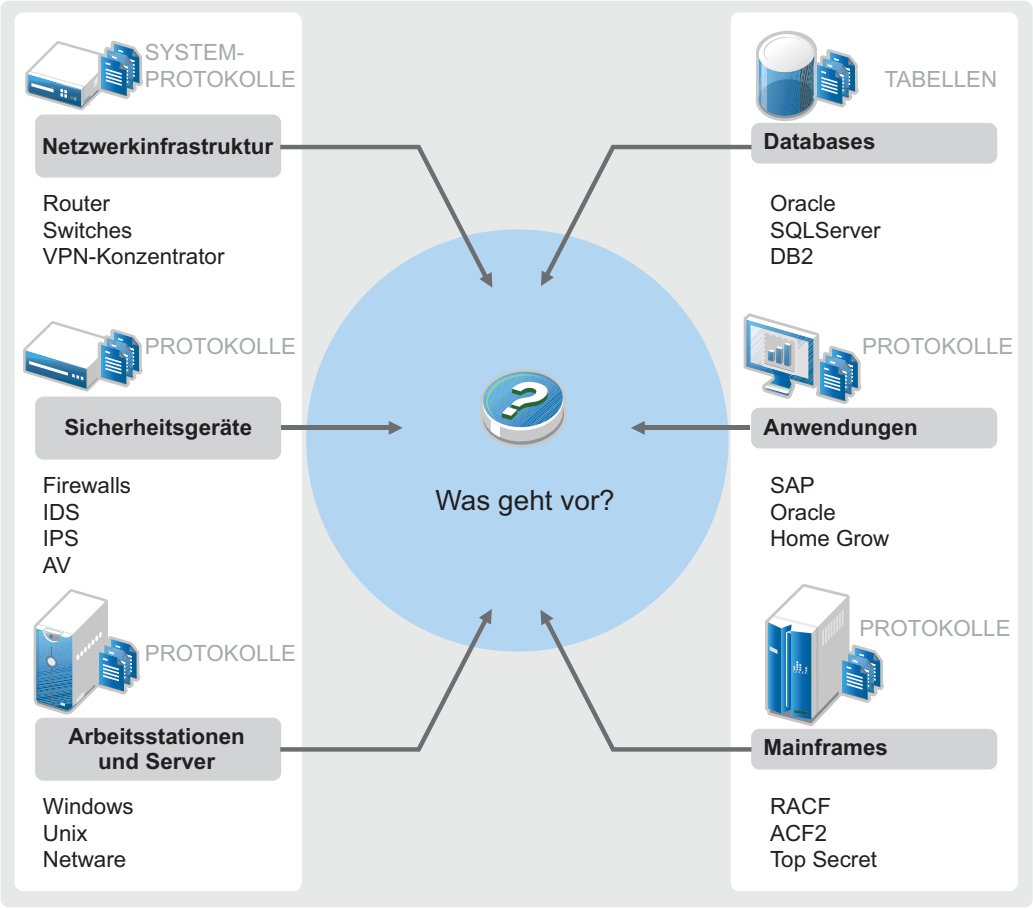
1 Was ist Sentinel?

Sentinel ist eine Lösung für das Sicherheitsinformations- und Ereignismanagement (SIEM) und die Compliance-Überwachung. Sentinel überwacht die komplexesten IT-Umgebungen automatisch und stellt die für den Schutz der IT-Umgebung erforderliche Sicherheit bereit.

Herausforderungen bei der Absicherung einer IT-Umgebung

Aufgrund der Komplexität Ihrer IT-Umgebung ist deren Absicherung eine Herausforderung. Üblicherweise umfasst eine IT-Umgebung eine Vielzahl von Anwendungen, Datenbanken, Mainframes, Arbeitsstationen und Servern. All diese Elemente generieren Ereignisprotokolle. Möglicherweise umfasst die IT-Umgebung zudem Sicherheits- und Netzwerkinfrastrukturgeräte, die Ereignisprotokolle generieren.

Abbildung 1-1 *Was geschieht in Ihrer Umgebung?*



Aufgrund folgender Umstände kommt es zu Problemen:

- Ihre IT-Umgebung besteht aus sehr vielen Geräten.
- Die Protokolle haben verschiedene Formate.
- Protokolle werden an unterschiedlichen Speicherorten gespeichert.
- Die Protokolldateien enthalten große Informationsmengen.
- Ereignisauslöser lassen sich nur durch manuelle Analyse der Protokolldateien identifizieren.

Sie müssen die folgenden Aufgaben durchführen können, damit die Protokollinformationen für Sie nützlich sind:

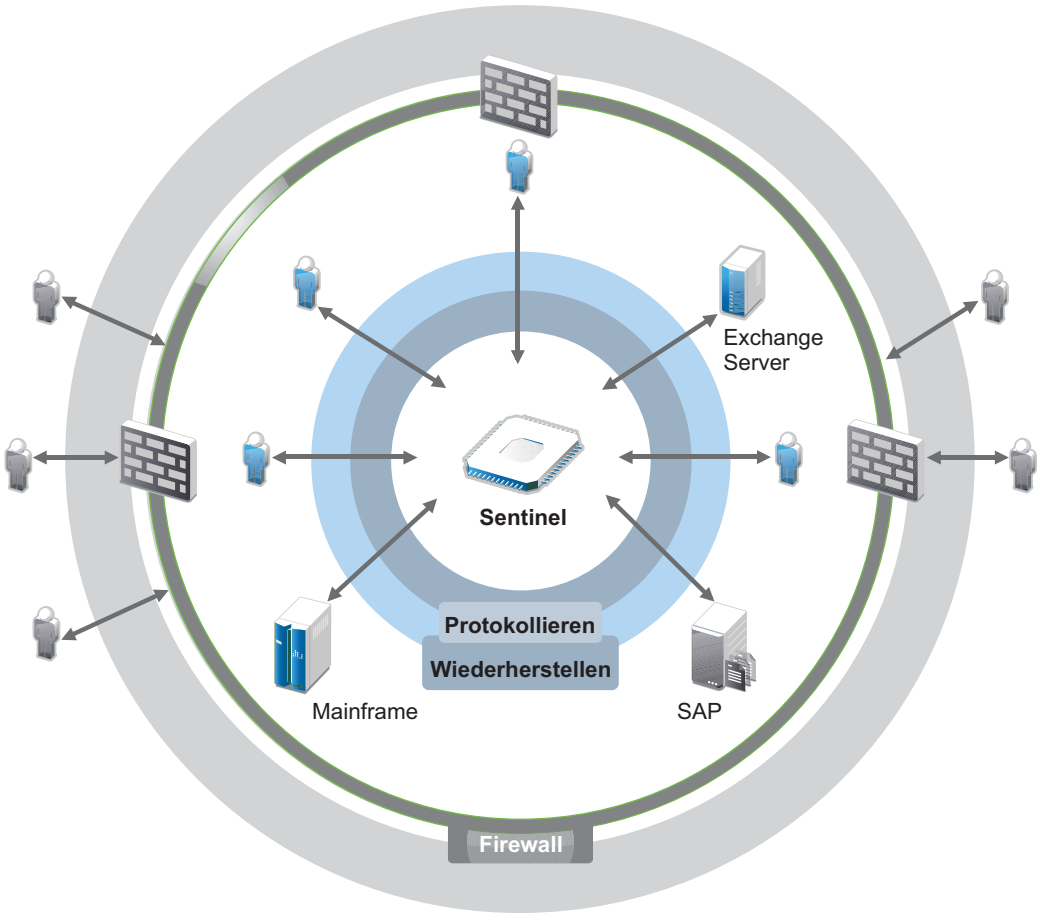
- Daten erfassen.
- Daten konsolidieren.
- Unterschiedliche Daten in Ereignissen normalisieren, die leicht verglichen werden können.
- Ereignisse Standardvorschriften zuordnen.
- Daten analysieren.
- Ereignisse aus mehreren Systemen vergleichen, um festzustellen, ob ein bestimmtes Muster auf ein Sicherheitsproblem hinweist.
- Benachrichtigungen senden, wenn Daten die Vorgaben nicht erfüllen.
- Bei Benachrichtigungen entsprechende, mit den Geschäftsrichtlinien konforme Aktionen veranlassen.
- Berichte zum Nachweis der Compliance generieren.

Wenn Sie die Probleme im Zusammenhang mit der Sicherung Ihrer IT-Umgebung eingegrenzt haben, müssen Sie festlegen, wie Sie das Unternehmen für die und vor den Benutzern schützen, ohne die Benutzerfreundlichkeit zu beeinträchtigen. Sentinel stellt die Lösung bereit.

Die Lösung, die Sentinel bietet

Sentinel ist das zentrale Nervensystem der Unternehmenssicherheit. Es erfasst Daten aus Ihrer gesamten Infrastruktur – von Anwendungen, Datenbanken, Servern, Speichereinheiten und Sicherheitsgeräten. Es analysiert und korreliert die Daten und macht sie umsetzbar – entweder automatisch oder manuell.

Abbildung 1-2 *Die Lösung, die Sentinel bietet*



Mit Sentinel wissen Sie immer darüber Bescheid, was in Ihrer IT-Umgebung vor sich geht, und können an Ressourcen vorgenommene Aktionen mit den Personen in Verbindung bringen, die diese Aktionen ausgeführt haben. Auf diese Weise können Sie das Benutzerverhalten erkennen und Aktivitäten effektiv überwachen, um Missbrauch zu verhindern.

Sentinel erreicht dies durch Folgendes:

- Bereitstellung einer umfassenden Lösung für IT-Kontrollen zu mehreren Sicherheitsstandards gleichzeitig.
- Keine Diskrepanzen zwischen dem, was eigentlich passieren sollte, und dem, was tatsächlich in Ihrer IT-Umgebung passiert.
- Erfüllung von Sicherheitsstandards.
- Bereitstellen eines einsatzbereiten Programms für die Compliance-Überwachung und Berichterstellung.

Sentinel protokolliert Erfassungs-, Analyse- und Berichtsprozesse automatisch, um zu gewährleisten, dass die Bedrohungserkennung und die Audit-Anforderungen durch IT-Steuerelemente effektiv unterstützt werden. Dabei bietet Sentinel eine automatische Überwachung der Sicherheits- und Compliance-Ereignisse sowie der implementierten IT-Kontrollen. So können Sie bei Sicherheitsverstößen oder nicht konformen Ereignissen umgehend Maßnahmen ergreifen. Mit Sentinel können Sie zudem Zusammenfassungsinformationen zur Umgebung erfassen und für wichtige Stakeholder freigeben.

2 Funktionsweise von Sentinel

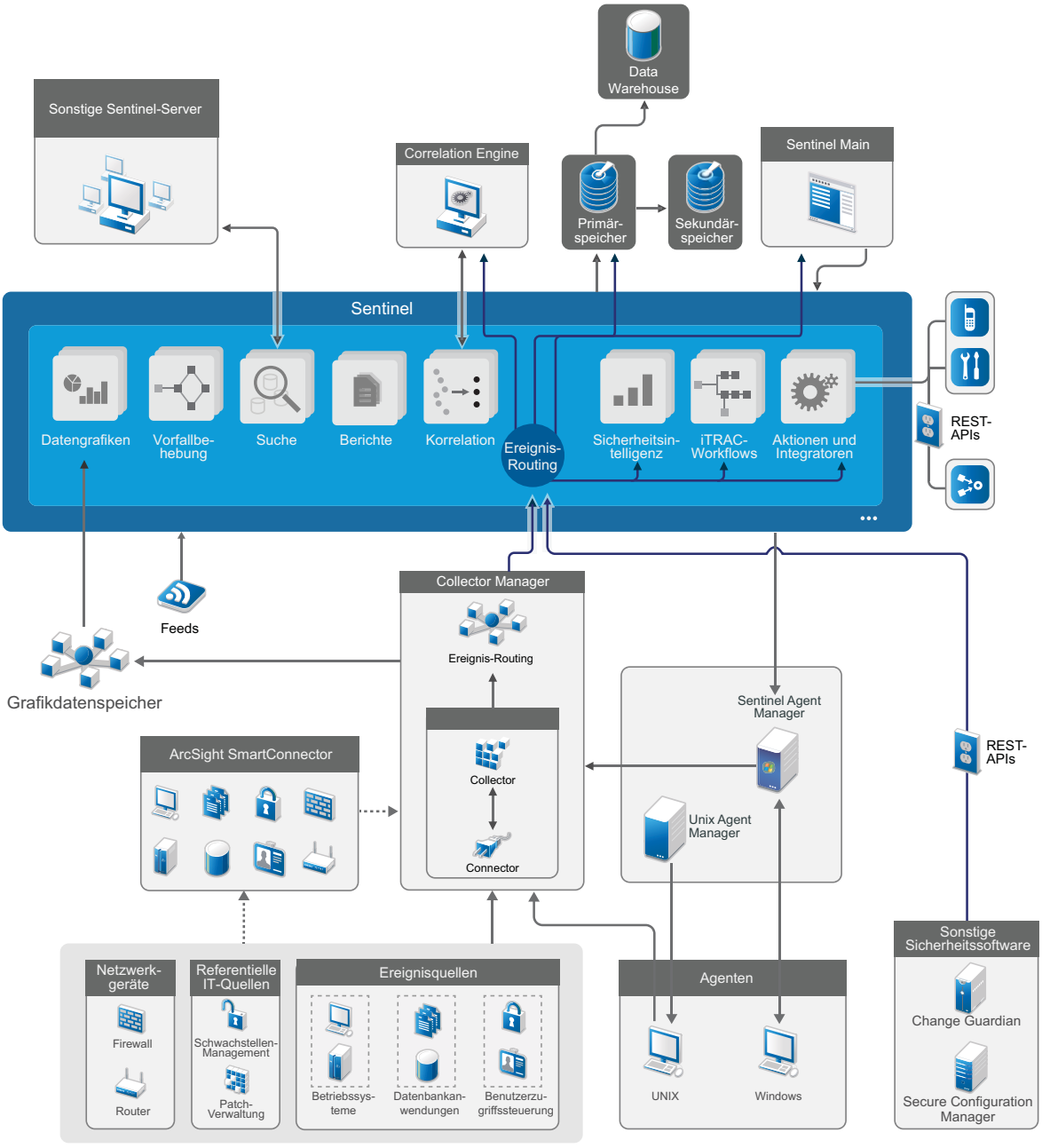
Sentinel verwaltet kontinuierlich sicherheitsrelevante Informationen und Ereignisse in Ihrer IT-Umgebung und bietet so eine vollständige Überwachungslösung.

Sentinel führt folgende Aufgaben aus:

- Erfassung von Protokoll-, Ereignis- und Sicherheitsinformationen aus den verschiedenen Quellen Ihrer IT-Umgebung
- Konvertierung der erfassten Protokoll-, Ereignis- und Sicherheitsinformationen in ein Sentinel-Standardformat
- Speicherung von Ereignissen in einem dateibasierten Datenspeicher oder einem skalierbaren Hadoop-basierten Speicher mit flexibel benutzerdefinierbaren Datenbeibehaltungsrichtlinien
- Erfassen von IP-Flussdaten und Hilfe bei der detaillierten Überwachung der Netzwerkaktivitäten.
- Fähigkeit zur hierarchischen Verknüpfung mehrerer Sentinel-Systeme, einschließlich Sentinel Log Manager
- Suche nach Ereignissen auf dem lokalen sowie auch auf weltweit verteilten Sentinel-Servern
- Durchführung statistischer Analysen zur Definition einer Baseline und Vergleich mit den aktuell einlaufenden Informationen, um verdeckte Probleme zu erkennen
- Korrelation einer Gruppe ähnlicher oder vergleichbarer Ereignisse, die innerhalb eines bestimmten Zeitraums stattgefunden haben, um ein Muster zu erkennen
- Einteilen von Ereignissen in Vorfälle, wodurch sich Response Management und Nachverfolgung effizienter gestalten
- Berichterstellung auf Basis aktueller und alter Ereignisse

In der folgenden Abbildung ist dargestellt, wie Sentinel herkömmlichen Speicher zur Datenspeicherung nutzt:

Abbildung 2-1 *Sentinel-Architektur*



In den folgenden Abschnitten werden die Sentinel-Komponenten im Detail beschrieben:

- „Ereignisquellen“, auf Seite 21
- „Sentinel-Ereignis“, auf Seite 21
- „Collector Manager“, auf Seite 23

Ereignisquellen

Sentinel erfasst Sicherheitsinformationen und Ereignisse aus verschiedenen Quellen Ihrer IT-Umgebung. Diese Quellen werden als Ereignisquellen bezeichnet. In einem Netzwerk kommen üblicherweise die folgenden Ereignisquellen vor:

Sicherheitsbereich: Sicherheitsgeräte einschließlich Hardware und Software für den Aufbau eines Sicherheitsperimeters für Ihre Umgebung wie Firewalls, Intrusion Detection Systems (IDS) und Virtual Private Networks (VPN).

Betriebssysteme: Verschiedene Betriebssysteme, die im Netzwerk ausgeführt werden.

IT-Referenzquellen: Software für die Verwaltung und Nachverfolgung von Inventar, Patches, Konfigurationen und Anfälligkeiten.

Anwendungen: Verschiedene Anwendungen, die im Netzwerk installiert sind.

Benutzerzugriffssteuerung: Anwendungen oder Geräte, über die Benutzer auf Unternehmensressourcen zugreifen.

Weitere Informationen zur Erfassung von Ereignissen aus Ereignisquellen finden Sie unter „Collecting and Routing Event Data“ (Erfassung und Routing von Ereignisdaten) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Sentinel-Ereignis

Sentinel empfängt Informationen von Geräten, standardisiert diese Informationen in einer als Ereignis bezeichneten Struktur, klassifiziert das Ereignis und sendet es zur Verarbeitung.

Ein Ereignis ist definiert als normalisierter Protokolldatensatz, der Sentinel von einem Drittanbieter-Sicherheitsgerät, -Netzwerk oder -Anwendungsgerät bzw. von einer internen Sentinel-Quelle übermittelt wird. Es gibt unterschiedliche Ereignistypen:

- Externe Ereignisse (von einem Sicherheitsgerät übermittelt), z. B.:
  - Ein von der Eindringversuchserkennung (Intrusion Detection System, IDS) erkannter Angriff

    - Eine von einem Betriebssystem gemeldete erfolgreiche Anmeldung
    - Eine kundenspezifische Situation wie der Dateizugriff durch einen Benutzer
- Interne Ereignisse (von Sentinel erzeugt), z. B.:
    - Eine deaktivierte Korrelationsregel
    - Zur Neige gehender Datenbankspeicherplatz

Sentinel fügt Ereignissen Kategorieinformationen (Taxonomie) hinzu, damit sich Ereignisse unterschiedlicher Systeme mit unterschiedlicher Erfassung einfacher vergleichen lassen. Ereignisse werden in der Echtzeitanzeige, von der Correlation Engine, von Dashboards sowie vom Back-End-Server verarbeitet.

Ein Ereignis umfasst über 200 Felder unterschiedlicher Typen mit unterschiedlichen Zwecken. Es gibt einige vordefinierte Felder, beispielsweise für den Schweregrad, die Gefährlichkeit, die Ziel-IP-Adresse und den Ziel-Port.

Es gibt zwei Gruppen konfigurierbarer Felder:

- Reservierte Felder: zur internen Verwendung durch Sentinel für zukünftige Funktionserweiterungen.
- Kundenfelder: zur Verwendung durch Kunden zu Anpassungszwecken.

Felder können eine externe oder eine referenzielle Quelle haben:

- Der Wert externer Felder wird ausdrücklich durch das Gerät oder den entsprechenden Collector festgelegt. Ein Feld kann beispielsweise der Gebäudecode des Gebäudes sein, in dem sich das Inventar befindet (die Angabe erfolgt als Ziel-IP-Adresse eines Ereignisses).
- Der Wert eines referenziellen Felds wird unter Verwendung des Zuordnungsservice als Funktion eines oder mehrerer weiterer Felder berechnet. Ein Feld kann beispielsweise vom Zuordnungsservice als kundendefinierte Zuordnung berechnet werden (unter Verwendung der Ziel-IP-Adresse aus dem Ereignis).

- „Zuordnungsservice“, auf Seite 22
- „Streaming von Zuordnungen“, auf Seite 23
- „Exploit-Erkennung“, auf Seite 23

Zuordnungsservice

Der Zuordnungsservice verteilt unternehmensrelevante Daten im gesamten System. Diese Daten reichern Ereignisse mit Referenzinformationen an.

Sie können die Ereignisdaten anreichern, indem Sie über Zuordnungen zusätzliche Informationen wie Host- und Identitätsinformationen zu den von den Quellgeräten eingehenden Ereignissen hinzufügen. Anhand dieser zusätzlichen Informationen kann Sentinel erweiterte Korrelationen und Berichte erstellen. Sentinel unterstützt eine Reihe integrierter Zuordnungen sowie angepasste benutzerdefinierte Zuordnungen.

In Sentinel definierte Zuordnungen werden auf zwei verschiedene Weisen gespeichert:

- Integrierte Zuordnungen werden in der Datenbank gespeichert, intern aktualisiert und automatisch an den Zuordnungsservice exportiert.
- Benutzerdefinierte Zuordnungen werden als CSV-Dateien gespeichert und können im Dateisystem oder über die Benutzeroberfläche für die Zuordnungsdatenkonfiguration aktualisiert werden. Anschließend werden sie vom Zuordnungsservice geladen.

In beiden Fällen werden die CSV-Dateien auf dem zentralen Sentinel-Server bewahrt. Änderungen an den Zuordnungen werden jedoch an die einzelnen Collector Manager-Instanzen verteilt und lokal angewendet. Diese verteilte Verarbeitung gewährleistet, dass die Zuordnungsaktivität den Hauptserver nicht überlastet.

Streaming von Zuordnungen

Der Zuordnungsservice setzt ein Modell zur dynamischen Aktualisierung ein und überträgt die Zuordnungen per Streaming von einem Punkt an den nächsten. Auf diese Weise wird verhindert, dass sich große Datenmengen an statischen Zuordnungen im dynamischen Speicher ansammeln. Dies ist bei unternehmenskritischen Echtzeitsystemen wie Sentinel entscheidend, die stabile, planbare und agile Datenbewegungen unabhängig von vorübergehenden Systemlasten erfordern.

Exploit-Erkennung

In Sentinel können Querverweise zwischen den Signaturen von Ereignisdaten und den Daten von Anfälligkeitsabsuchen erstellt werden. Sentinel benachrichtigt Benutzer automatisch sofort bei Versuchen, Schwachstellen in einem System auszunutzen. Dazu nutzt Sentinel die folgenden Funktionen:

- Advisor-Feed
- Intrusion Detection
- Anfälligkeitsabsuchen
- Firewalls

Ein Advisor-Feed enthält Informationen zu Schwachstellen und Bedrohungen sowie eine Standardisierung von Ereignissignaturen und Schwachstellen-Plugins. So wird einen Querverweis zwischen Ereignisdatensignaturen und Schwachstellen-Absuchdaten hergestellt. Weitere Informationen zu Advisor-Feeds finden Sie im Abschnitt „Detecting Vulnerabilities and Exploits“ (Erkennen von Schwachstellen und Exploits) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Collector Manager

Collector Manager verwaltet die Datenerfassung, überwacht Meldungen zum Systemstatus und filtert Ereignisse. Zu den Hauptaufgaben von Collector Manager zählen die folgenden Funktionen:

- Datenerfassung mithilfe von Connectors.
- Analyse und Standardisierung von Daten mithilfe von Collectors.

Collectors

Collectors erfassen Informationen von den Connectors und standardisieren diese Daten. Sie führen folgende Funktionen aus:

- Empfangen der Rohdaten von den Connectors
- Analyse und Standardisierung der Daten
  - Konvertierung ereignisquellenspezifischer Daten in Sentinel-spezifische Daten

    - Anreicherung von Ereignissen durch Änderung der Informationen in den Ereignissen in ein durch Sentinel lesbares Format
    - Ereignisquellenspezifische Ereignisfilterung
- Hinzufügen einer Geschäftsrelevanz zu Ereignissen durch den Zuordnungsservice:
    - Zuordnung von Ereignissen zu Identitäten
    - Zuordnung von Ereignissen zum Bestand
- Weiterleiten der Ereignisse
- Weiterleiten der standardisierten, analysierten und formatierten Daten an Collector Manager
- Senden von Statusmeldungen an den Sentinel-Server

Weitere Informationen zu Collectors finden Sie auf der Website für Sentinel-Plugins.

Connectors

Connectors stellen die Verbindungen zwischen den Ereignisquellen und dem Sentinel-System her.

Connectors führen folgende Funktionen aus:

- Transport der Ereignisrohdaten von den Ereignisquellen zum Collector
- Verbindungsspezifische Filterung
- Fehlerbehandlung im Rahmen der Verbindungen

ArcSight SmartConnectors

Sentinel nutzt ArcSight SmartConnector zum Erfassen von Ereignissen von verschiedenen Arten von Ereignisquellen, die in Sentinel nicht direkt unterstützt werden. SmartConnectors erfassen Ereignisse von unterstützten Geräten, normalisieren Ereignisse in CEF (Common Event Format) und leiten sie über den Syslog-Connector an Sentinel weiter. Der Connector leitet die Ereignisse dann zur Analyse an Universal Common Event Format Collector weiter.

Weitere Informationen zum Konfigurieren von Sentinel mit SmartConnectors finden Sie in der Dokumentation zu Universal Common Event Format Collector auf der Website für Sentinel-Plugins.

Agent Manager

Agent Manager sorgt ergänzend zu der agentenlosen Datenerfassung für die hostbasierte Datenerfassung, indem Sie folgende Aufgaben ausführen können:

- Zugriff auf Protokolle, die nicht über das Netzwerk verfügbar sind
- Betrieb in streng kontrollierten Netzwerkumgebungen.
- Verbesserung der Sicherheit durch Reduzierung der Angriffsfläche auf kritischen Servern.
- Zuverlässigere Datenerfassung während Netzwerkunterbrechungen..

Mit Agent Manager können Sie Agenten bereitstellen, die Agentenkonfiguration verwalten und einen Erfassungspunkt für in Sentinel eingehende Ereignisse bereitstellen. Weitere Informationen zu Agent Manager finden Sie in der Agent Manager-Dokumentation.

Daten-Routing und Datenspeicherung in Sentinel

Sentinel bietet mehrere Optionen für Routing, Speicherung und Extrahierung erfasster Daten. Standardmäßig empfängt Sentinel die analysierten Ereignisdaten und die Rohdaten von den Collector Manager-Instanzen. Sentinel speichert die Rohdaten, um für eine sichere Nachweiskette zu sorgen, und leitet die analysierten Ereignisdaten entsprechend den von Ihnen festgelegten Regeln weiter. Sie können die analysierten Ereignisdaten filtern, an einen Speicher oder zur Echtzeitanalyse senden oder an externe Systeme weiterleiten. Darüber hinaus gleicht Sentinel alle Ereignisdaten, die an den Speicher gesendet werden, mit benutzerdefinierten Beibehaltungsrichtlinien ab. Diese Richtlinien bestimmen, wann Ereignisdaten aus dem System gelöscht werden.

Je nach EPS-Rate (Ereignisse pro Sekunde) und Ihren Bereitstellungsanforderungen können Sie sich für den herkömmlichen dateibasierten Datenspeicher oder den skalierbaren Hadoop-basierten Speicher entscheiden. Weitere Informationen finden Sie unter „Überlegungen zum Datenspeicher“, auf Seite 39.

Ereignisgrafiken

Sentinel stellt Ereignisgrafiken bereit, die Daten in Diagrammen, Tabellen und Karten präsentieren. Diese Grafiken erleichtern die Darstellung und Analyse großer Ereignismengen einschließlich IP-Flussereignisse. Sie können auch eigene Ereignisgrafiken und Dashboards erstellen.

Ereignisgrafiken sind standardmäßig in Sentinel mit skalierbarem Speicher verfügbar. Bei einer Einrichtung mit herkömmlichem Speicher sind die Ereignisgrafiken nur verfügbar, wenn Sie den Grafikdatenspeicher (Elasticsearch) zum Speichern und Indexieren von Daten aktiviert haben. Weitere Informationen über das Aktivieren von Elasticsearch finden Sie in „Grafikdatenspeicher konfigurieren“, auf Seite 43.

Korrelation

Ein einzelnes Ereignis mag bedeutungslos erscheinen. Zusammen mit anderen Ereignissen kann es jedoch auf ein potenzielles Problem hinweisen. Sentinel erleichtert Ihnen die Korrelation solcher Ereignisse mithilfe von Regeln, die Sie in der Correlation Engine erstellen und implementieren, sodass Sie rechtzeitig entsprechende Aktionen durchführen können, um Probleme zu vermeiden.

Die Korrelation steigert die Informationsausbeute bei der Verwaltung von Sicherheitsereignissen, indem sie die Analyse des eingehenden Ereignisstroms automatisiert, um relevante Muster zu erkennen. Durch Korrelation lassen sich Regeln definieren, durch die kritische Bedrohungen und komplexe Angriffsmuster identifiziert werden. Dies ermöglicht die vorrangige Behandlung bestimmter Ereignisse, wodurch die Vorfallsverwaltung und -behandlung an Effizienz gewinnt. Weitere Informationen zur Korrelation finden Sie unter „Correlating Event Data“ (Korrelation von Ereignisdaten) im *Sentinel User Guide* (NetIQ Sentinel-Benutzerhandbuch).

Um Ereignisse entsprechend den Korrelationsregeln zu überwachen, müssen die Regeln in der Correlation Engine bereitgestellt werden. Wenn ein Ereignis eintritt, das den Regelkriterien entspricht, generiert die Correlation Engine ein Korrelationsereignis, das das Muster beschreibt. Weitere Informationen finden Sie unter „Correlation Engine“ im *Sentinel User Guide* (Sentinel-Benutzerhandbuch).

Sicherheitsintelligenz

Mit der Korrelationsfunktion in Sentinel können Sie nach bekannten Aktivitätsmustern suchen, die Sie dann zu Sicherheits-, Compliance- und sonstigen Zwecken analysieren können. Die Sicherheitsintelligenzfunktion sucht nach Aktivitäten, die ungewöhnlich und möglicherweise schädlich sind, aber mit keinem bekannten Muster übereinstimmen.

Die Sentinel-Sicherheitsintelligenzfunktion setzt in erster Linie auf die statistische Analyse von Zeitreihendaten. Die Funktion ermöglicht Analysten die Erkennung und Analyse von Anomalien mithilfe einer automatisierten Statistik-Engine bzw. durch manuelle Interpretation grafischer Statistiken. Weitere Informationen finden Sie im Abschnitt „Analyzing Trends in Data“ (Datentrends analysieren) im *Sentinel User Guide* (Sentinel-Benutzerhandbuch).

Problembehebung

Sentinel bietet eine automatisierte Vorfallsreaktionsverwaltung, mit der Sie den Prozess der Statusüberwachung, Eskalation und Reaktion auf Vorfälle und Richtlinienverstöße dokumentieren und formalisieren können. Außerdem ist die bidirektionale Integration in Problemberichtssysteme möglich. Mit Sentinel können Sie prompt reagieren und Vorfälle auf effiziente Weise aus der Welt schaffen. Weitere Informationen finden Sie unter „Configuring Incidents“ (Vorfälle konfigurieren) im *Sentinel User Guide* (Sentinel-Benutzerhandbuch).

iTRAC-Workflows

iTRAC-Workflows bieten eine einfache und flexible Lösung für die Automatisierung und Statusüberwachung von Vorfallsbehandlungsprozessen in Unternehmen. iTRAC nutzt das interne Vorfallsystem von Sentinel zur Statusüberwachung von Sicherheits- und Systemproblemen von ihrer Identifizierung (mithilfe von Korrelationsregeln oder durch manuelle Erkennung) bis hin zu ihrer Behebung.

Sie können Workflows anhand manueller und automatisierter Schritte erstellen. iTRAC-Workflows unterstützen erweiterte Funktionen wie Verzweigungen, zeitbasierte Eskalation und lokale Variablen. Die Möglichkeit der Integration externer Skripts und Plugins bietet Raum für die flexible Interaktion mit Systemen von Drittanbietern. Dank umfassender Berichtsfunktionen können Administratoren den Vorfallsbehandlungsprozess besser verstehen und anpassen. Weitere Informationen finden Sie im Abschnitt „Configuring iTRAC Workflows“ (iTRAC-Workflows konfigurieren) im *Sentinel User Guide* (Sentinel-Benutzerhandbuch).

Aktionen und Integratoren

Mit Aktionen wird entweder manuell oder automatisch eine bestimmte Aktion ausgeführt, beispielsweise das Senden einer Email. Aktionen können durch Routing-Regeln, durch die manuelle Ausführung eines Ereignisses oder eines Vorfalls und durch Korrelationsregeln ausgelöst werden. Sentinel enthält eine Liste vordefinierter Aktionen. Sie können die standardmäßigen Aktionen verwenden und je nach Bedarf neu konfigurieren oder neue Aktionen hinzufügen. Weitere Informationen finden Sie unter „Configuring Actions“ (Konfigurieren von Aktionen) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).

Eine Aktion kann selbständig ausgeführt werden oder über eine Integratorinstanz, die über ein Integrator-Plugin konfiguriert wurde. Integrator-Plugins erweitern die Funktionen der in Sentinel verfügbaren Behebungsaktionen. Integratoren bieten die Möglichkeit, zur Ausführung einer Aktion

eine Verbindung zu einem externen System herzustellen, beispielsweise einem LDAP-, SMTP- oder SOAP-Server. Weitere Informationen finden Sie unter „Configuring Integrators“ (Konfigurieren von Integratoren) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).

Suchvorgänge

Sentinel bietet eine Option zum Suchen nach Ereignissen. Mit der notwendigen Konfiguration können Sie auch nach von Sentinel erzeugten Systemereignissen suchen und die Rohdaten zu den einzelnen Ereignissen anzeigen. Weitere Informationen finden Sie im Abschnitt „Searching Events“ (Suchen von Ereignissen) im *Sentinel User Guide* (NetIQ Sentinel-Benutzerhandbuch).

Sie können auch Sentinel-Server durchsuchen, die über verschiedene geografische Standorte verteilt sind. Weitere Informationen finden Sie unter „Configuring Data Federation“ (Konfigurieren eines Datenverbunds) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Berichte

Zu den in Sentinel erfassten Daten können Berichte erstellt werden. Im Lieferumfang von Sentinel ist eine Reihe anpassbarer Berichten enthalten. Einige Berichte sind konfigurierbar, sodass Sie die Spalten angeben können, die in den Ergebnissen angezeigt werden.

Sie können Berichte ausführen, planen und per Email als PDF senden. Sie können jeden Bericht als Suche ausführen und die Ergebnisse dann wie bei jeder Suche verwenden, indem Sie die Suche präzisieren oder bestimmte Aktionen mit dem Ergebnis ausführen. Die Berichte können auch auf geografisch verteilten Sentinel-Servern ausgeführt werden. Weitere Informationen finden Sie unter „Reporting (Berichterstellung)“ im *Sentinel User Guide (NetIQ Sentinel-Benutzerhandbuch)*.

Identitätsnachverfolgung

Sentinel bietet ein Integrations-Framework für Identitätsmanagementsysteme, um den Status der Identitäten jedes Benutzerkontos und der von diesen Identitäten ausgeführten Ereignisse zu überwachen. Sentinel stellt Benutzerinformationen bereit, beispielsweise Kontaktinformationen, Benutzerkonten, kürzlich erfolgte Authentifizierungs- und Zugriffsereignisse und Berechtigungsänderungen. Durch die Anzeige von Informationen zu den Benutzern, die eine bestimmte Aktion initiieren oder von einer Aktion betroffen sind, verbessert Sentinel die Reaktionszeiten bei Vorfällen und ermöglicht eine verhaltensbasierte Analyse. Weitere Informationen finden Sie unter „Leveraging Identity Information“ (Nutzen von Identitätsinformationen) im *Sentinel User Guide* (NetIQ Sentinel-Benutzerhandbuch).

Ereignisanalyse

Sentinel stellt leistungsfähige Tools zur Verfügung, um Sie bei Erkennung und Analyse kritischer Ereignisdaten zu unterstützen. Sentinel optimiert das System für maximale Effizienz bei allen Analysearten und bietet Verfahren für den unkomplizierten, nahtlosen Wechsel von einem Analyseverfahren zum anderen.

Das Untersuchen von Ereignissen in Sentinel beginnt meist mit den „Event Views“ (Ereignisansichten), die Daten in nahezu Echtzeit darstellen. Ergänzend zu erweiterten Tools zeigen „Event Views“ (Ereignisansichten) gefilterte Ereignisströme mit zusammenfassenden Diagrammen an, die zur einfachen Schnellanalyse von Ereignistrends und Ereignisdaten sowie zur Identifizierung bestimmter Ereignisse verwendet werden können. Mit der Zeit erstellen Sie abgestimmte Filter für

bestimmte Datenklassen, zum Beispiel für die Ausgabe von Korrelationen. Sie können „Event Views“ (Ereignisansichten) als Dashboard verwenden, das den allgemeinen Betriebs- und Sicherheitsstand anzeigt.

Mit der interaktiven Suche können Sie die Ereignisse dann detaillierter analysieren. So können Sie schnell und einfach Daten zu einer bestimmten Abfrage finden, zum Beispiel zur Aktivität eines bestimmten Benutzers oder auf einem bestimmten System. Durch Klicken auf die Ereignisdaten oder über den Eingrenzungsbereich auf der linken Seite können Sie bestimmte Ereignisse schnell herausgreifen.

Wenn Sie Hunderte von Ereignissen analysieren, können Sie das Ereignislayout mithilfe der Berichtfunktionen in Sentinel benutzerdefiniert steuern und auch große Datenmengen anzeigen. Sentinel erleichtert den Übergang, da Sie interaktive Suchen, die Sie in der Suchschnittstelle erstellt haben, in eine Berichtsvorlage übertragen können. Auf diese Weise wird direkt ein Bericht mit denselben Daten erstellt, die jedoch in einem Format angezeigt werden, das sich besser für große Ereignismengen eignet.

Zu diesem Zweck umfasst Sentinel eine Vielzahl an Vorlagen. Es gibt zwei Arten von Berichtsvorlagen:

- Auf die Anzeige bestimmter Informationstypen wie Authentifizierungsdaten oder Benutzererstellung abgestimmte Vorlagen
- Vorlagen für allgemeine Zwecke mit der Möglichkeit zur interaktiven Anpassung von Gruppen und Spalten im Bericht

Mit der Zeit werden Sie häufig gebrauchte Filter und Berichte entwickeln, die Ihre Arbeitsabläufe erleichtern. Sentinel unterstützt die Speicherung und Verteilung dieser Informationen an die Mitglieder in Ihrer Organisation. Weitere Informationen finden Sie im *Sentinel User Guide* (NetIQ Sentinel-Benutzerhandbuch).

Planen der Sentinel-Installation

In den nächsten Kapiteln erfahren Sie, wie Sie Ihre Sentinel-Installation planen. Wenden Sie sich an den Technischen Support von , wenn Sie eine Konfiguration installieren möchten, die in den folgenden Kapiteln nicht behandelt wird, oder wenn Sie Fragen haben.

3 Implementierungs-Checkliste

Planen, installieren und konfigurieren Sie Sentinel anhand der folgenden Checkliste.

Verwenden Sie die Checkliste jedoch nicht, wenn Sie von einer älteren Sentinel-Version aufrüsten. Weitere Informationen zur Aufrüstung finden Sie unter Teil V, „Aufrüsten von Sentinel“, auf Seite 147.

❒	Aufgaben	Erklärt in
❒	Sehen Sie sich die Informationen zur Produktarchitektur an, um die Sentinel-Komponenten kennenzulernen.	Teil I, „Sentinel“, auf Seite 13.
❒	Überprüfen Sie anhand der Sentinel-Lizenzierungsinformationen, ob Sie die Evaluierungslizenz oder die Unternehmenslizenz von Sentinel verwenden müssen.	Kapitel 4, „Lizenzinformationen“, auf Seite 33.
❒	Beurteilen Sie Ihre Umgebung, um die Hardware-Konfiguration zu ermitteln. Stellen Sie sicher, dass die Computer, auf denen Sentinel und dessen Komponenten installiert werden sollen, den angegebenen Anforderungen entsprechen.	Kapitel 5, „Erfüllen der Systemanforderungen“, auf Seite 37.
❒	Ermitteln Sie auf Grundlage der Anzahl der Ereignisse pro Sekunde (EPS) die für Ihre Umgebung geeignete Art der Bereitstellung. Ermitteln Sie die Anzahl der Collector Manager- und Correlation Engine-Instanzen, die zur Optimierung der Leistung und für den Lastenausgleich installiert werden müssen.	Kapitel 6, „Überlegungen zur Bereitstellung“, auf Seite 39.
❒	Lesen Sie die aktuellen Sentinel-Versionshinweise, um sich über die neuen Funktionen und bekannten Probleme zu informieren.	Sentinel-Versionshinweise
❒	Installieren Sie Sentinel.	Teil III, „Installieren von Sentinel“, auf Seite 69.
❒	Konfigurieren Sie Sentinel.	Teil IV, „Konfigurieren von Sentinel“, auf Seite 113.
❒	Sentinel umfasst standardmäßige Korrelationsregeln. Einige Korrelationsregeln sind standardmäßig so konfiguriert, dass beim Auslösen der Regel eine Email gesendet wird, beispielsweise die Aktion zum Benachrichtigen des Sicherheitsadministrators. Daher müssen Sie auf dem Sentinel-Server die Einstellungen des Email-Servers konfigurieren, indem Sie den SMTP-Integrator und die Aktion „Email senden“ konfigurieren.	Dokumentation zum SMTP-Integrator und zur Aktion „Email senden“ auf der Website für Sentinel-Plugins.
❒	Installieren Sie je nach den Anforderungen Ihrer Umgebung zusätzliche Collectors und Connectors.	Kapitel 16, „Installieren von zusätzlichen Collectors und Connectors“, auf Seite 109.

❒	Aufgaben	Erklärt in
❒	Installieren Sie je nach den Anforderungen Ihrer Umgebung zusätzliche Collector Manager- und Correlation Engine-Instanzen.	Teil III, „Installieren von Sentinel“, auf Seite 69.

4 Lizenzinformationen

Sentinel bietet ein breites Spektrum an Funktionen für die unterschiedlichen Erfordernisse seines großen Kundenstamms. Wählen Sie das Lizenzierungsmodell, das Ihren Erfordernissen entspricht.

Die Sentinel-Plattform bietet die folgenden beiden Lizenzierungsmodelle:

- **Sentinel Enterprise:** Lösung mit vollständigem Funktionsumfang, die alle Core-Funktionen für die visuelle Analyse in Echtzeit und vieles mehr umfasst. Sentinel Enterprise ist auf SIEM-Anwendungsfälle ausgelegt, wie die Echtzeit-Bedrohungserkennung und Warnung und Abhilfe bei Bedrohungen.
- **Sentinel for Log Management:** Eine Lösung für die Protokollverwaltung, insbesondere zum Erfassen, Speichern und Durchsuchen der Daten und dem Erstellen von Berichten.

  Sentinel for Log Management stellt eine deutliche Verbesserung der Funktionen von Sentinel Log Manager 1.2.2 dar. In einigen Aspekten wurde die Architektur erheblich verändert. Informationen zur Planung der Aufrüstung auf Sentinel für das Protokollmanagement finden Sie auf der Sentinel-FAQ-Seite.

Kaufen Sie je nach den erworbenen Lösungen und Add-ons die entsprechenden Lizenzschlüssel und Berechtigungen, damit in Sentinel die richtigen Funktionen aktiviert werden. Lizenzschlüssel und Berechtigungen legen den Basiszugriff auf Produktfunktionen und Downloads fest. Zusätzliche Bestimmungen und Bedingungen können Sie dem Kaufvertrag und der Endbenutzer-Lizenzvereinbarung entnehmen.

In der folgenden Tabelle finden Sie die Services und Funktionen jeder Lösung:

Tabelle 4-1 *Sentinel-Services und -Funktionen*

Services und Funktionen	Sentinel Enterprise	Sentinel for Log Management
Core-Funktionalität ◆ Erfassung, Analyse, Normalisierung und Klassifizierung von Ereignissen ◆ Erfassung von Nichtereignisdaten (Daten zum Bestand, zu Schwachstellen und zur Benutzeridentität) ◆ Inline-Kontextzuordnung ◆ Ereignisspeicherung nach Beibehaltungsrichtlinien und Nachweisbarkeit ◆ Ereignis-Routing zum herkömmlichen Speicher (intern und extern) ◆ Ereignissuche und -visualisierung ◆ Erfassung, Speicherung und grafische Anzeige von IP-Flussdaten ◆ Berichte ◆ Aktivierung von Federal Information Processing Standard Publication 140-2 (FIPS 140-2) ◆ Manuell ausgelöste Aktionen ◆ Manuelle Erstellung und Verwaltung von Vorfällen	Ja	Ja
Sentinel Link	Ja	Ja
Datensynchronisierung	Ja	Ja
Wiederherstellung von archivierten Ereignisdaten	Ja	Ja
Datenverbund (verteilte Suche)	Ja	Ja
Exploit-Erkennung (Advisor)*	Ja	Ja
Skalierbarer Speicher	Ja	Ja
Korrelation ◆ Echtzeit-Ereignisschemakorrelation ◆ Durch Korrelationsregeln ausgelöste Aktionen ◆ Selektierung von Warnmeldungen ◆ Visualisierung von Warnmeldungen	Ja	Nein
Sicherheitsintelligenz ◆ Anomalieregeln ◆ Statistische Echtzeitanalyse	Ja	Nein

* Advisor von Security Nexus ist ein Add-on-Service. Zur Verwendung dieses Service muss die entsprechende Lizenz erworben werden.

Sentinel-Lizenzen

In diesem Abschnitt erfahren Sie mehr über die einzelnen Sentinel-Lizenztypen.

Evaluierungslizenz

Mit der standardmäßigen Evaluierungslizenz können Sie während eines bestimmten Evaluierungszeitraums alle Funktionen von Sentinel Enterprise nutzen. Die EPS-Grenze wird hierbei nur von der Leistungsfähigkeit Ihrer Hardware bestimmt. Informationen zu den Funktionen von Sentinel Enterprise finden Sie in Tabelle 4-1, „Sentinel-Services und -Funktionen“, auf Seite 34.

Das Ablaufdatum des Systems bezieht sich auf die ältesten Daten im System. Wenn Sie alte Ereignisse im System wiederherstellen, aktualisiert Sentinel das Ablaufdatum entsprechend.

Nach Ablauf der Evaluierungslizenz gilt für Sentinel eine kostenlose Basislizenz mit begrenztem Funktionsumfang und einer EPS-Grenze von 25. Dies gilt nur, fall Sentinel mit herkömmlichem Speicher konfiguriert ist.

Bei der Bereitstellung mit skalierbarem Speicher endet mit Ablauf der Evaluierungslizenz die Speicherung von Ereignissen und Rohdaten.

Sobald Sie auf eine Unternehmenslizenz aufrüsten, verfügt Sentinel wieder über die gesamte Funktionalität. Damit alle Funktionen ununterbrochen zur Verfügung stehen, müssen Sie das System vor dem Ablaufdatum der Evaluierungslizenz auf eine Unternehmenslizenz aufrüsten.

Freie Lizenz

Mit der freien Lizenz verfügt Ihr System über einen eingeschränkten Funktionsumfang und eine EPS-Grenze von 25. Die kostenlose Lizenz gilt nur für Sentinel mit herkömmlichem Speicher.

Mit der freien Lizenz können Sie Ereignisse erfassen und speichern. Bei einer EPS-Rate von über 25 speichert Sentinel die empfangenen Ereignisse zwar, zeigt allerdings ihre Details nicht in Suchergebnissen oder Berichten an. Diese Ereignisse markiert Sentinel mit der Kennung `OverEPSLimit`.

Die freie Lizenz bietet keine Echtzeitfunktionen. Wenn Sie sie zu einer Unternehmenslizenz aufrüsten, erhalten Sie wieder Zugriff auf die gesamte Funktionalität.

HINWEIS: Technischer Support und Produktaktualisierungen sind für die kostenlose Version von Sentinel nicht verfügbar.

Unternehmenslizenzen

Beim Kauf von Sentinel erhalten Sie über das Kundenportal einen Lizenzschlüssel. Der Lizenzschlüssel aktiviert Funktionen, Datenerfassungsraten und Ereignisquellen je nach der erworbenen Lizenz. Unter Umständen werden bestimmte zusätzliche Lizenzbedingungen nicht durch den Lizenzschlüssel umgesetzt. Lesen Sie daher die Lizenzvereinbarung aufmerksam durch.

Wenden Sie sich an Ihren Kundenbetreuer, um Änderungen an Ihrer Lizenz vorzunehmen.

Die Unternehmenslizenz können Sie bereits während der Installation, aber auch später jederzeit hinzufügen. Wie Sie den Lizenzschlüssel hinzufügen, erfahren Sie unter „Adding a License Key“ (Hinzufügen eines Lizenzschlüssels) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

5 Erfüllen der Systemanforderungen

Die Sentinel-Implementierung richtet sich nach den Anforderungen Ihrer Umgebung. Ziehen Sie daher vor der Fertigstellung der Sentinel-Architektur für Ihre Umgebung die Consulting Services oder einen Sentinel-Partner zurate.

Die Hardwarevoraussetzungen sowie die unterstützten Betriebssysteme, Appliance-Plattformen und Browser sind auf der Website Sentinel Technical Information (Technische Informationen für Sentinel) aufgeführt.

Connector- und Collector-Systemanforderungen

Die Systemanforderungen und unterstützten Plattformen sind für jeden Connector bzw. Collector unterschiedlich. Informationen hierzu finden Sie in der Connector- und Collector-Dokumentation auf der Website für Sentinel-Plugins.

Virtuelle Umgebung

Sentinel wird von VMware ESX-Servern unterstützt. Wenn Sie eine virtuelle Umgebung einrichten, müssen die virtuellen Maschinen über mindestens zwei CPUs verfügen. Um auf ESX oder in anderen virtuellen Umgebungen identische Ergebnisse wie bei den Testergebnissen auf physischen Computern zu erzielen, muss die virtuelle Umgebung dieselben Anforderungen an Arbeitsspeicher, CPU, Speicherplatz und E/A erfüllen, die auch für physische Computer gelten.

Informationen zu den Empfehlungen für physische Computer finden Sie auf der Website Sentinel Technical Information (Technische Informationen für Sentinel).

6 Überlegungen zur Bereitstellung

Sentinel verfügt über eine skalierbare Architektur, die je nach zutreffender Last angepasst werden kann. Dieses Kapitel enthält einen Überblick der wichtigsten Punkte, die bei der Skalierung einer Sentinel-Bereitstellung berücksichtigt werden sollten. Ein Experte des Technischen Supports von oder der Partner Services kann Ihnen bei der Auslegung des Sentinel-Systems für Ihre spezielle IT-Umgebung behilflich sein.

Überlegungen zum Datenspeicher

Zur Speicherung und Indexierung Ihrer Sentinel-Daten können Sie sich je nach EPS-Rate für herkömmlichen oder skalierbaren Speicher entscheiden. Ihre Entscheidung beeinflusst die Sentinel-Bereitstellung in Ihrer Umgebung.

Tabelle 6-1 *Vergleich zwischen herkömmlichem und skalierbarem Speicher*

Herkömmlicher Speicher	Skalierbarer Speicher
Daten werden standardmäßig in einem herkömmlichen dateibasierten Speicher abgelegt und lokal auf dem Sentinel-Server indexiert. Zusätzlich zum dateibasierten Datenspeicher können Sie Ereignisse auch im Grafikdatenspeicher speichern und indexieren, um die Datengrafikfunktionen zu nutzen. Weitere Informationen finden Sie unter „Grafikdatenspeicher konfigurieren“, auf Seite 43.	Daten werden in einem skalierbaren Hadoop-basierten Speicher abgelegt und mittels eines skalierbaren, verteilten Indexierungsmechanismus indexiert.
Nahtlose vertikale Skalierung auf ca. 20.000 EPS. Eine noch höhere EPS-Rate erfordert zusätzliche Sentinel-Server.	Nahtlose horizontale Skalierung für sehr hohe EPS-Raten, z. B. 1 Million Ereignisse pro Sekunde.
Der Lastausgleich bei der Datenerfassung erfolgt über mehrere Sentinel-Server. Somit werden die Daten auf mehrere Sentinel-Server verteilt und müssen dort individuell verwaltet werden.	Die Datenerfassung erledigt ein einziger Sentinel-Server. Somit erfolgt auch die Daten- und Ressourcenverwaltung zentral auf einem einzigen Sentinel-Server.
Die Daten werden auf dem Datenträger gemäß Mandant gekennzeichnet, aber nicht nach Mandant getrennt gespeichert.	Die Daten werden auf dem Datenträger gemäß Mandant gekennzeichnet und nach Mandant getrennt gespeichert.
Die Datenreproduktion und -verfügbarkeit muss entweder manuell oder per teuren Speichereinrichtungen wie SAN-Datenträgern sichergestellt werden.	Die Datenreproduktion und -verfügbarkeit ist erschwinglich, da Hadoop auf handelsüblicher Hardware ausgeführt wird.

- „Planen des herkömmlichen Speichers“, auf Seite 41
- „Planen des skalierbaren Speichers“, auf Seite 44
- „Sentinel-Verzeichnisstruktur“, auf Seite 46

Planen des herkömmlichen Speichers

Im dateibasierten Datenspeicher werden Daten in einer Struktur mit drei Ebenen gespeichert:

Onlinespeicher	Primärspeicher, früher als „lokaler Speicher“ bezeichnet.	Für schnelles Schreiben und Abrufen optimiert. Speichert die zuletzt erfassten Ereignisdaten sowie die am häufigsten durchsuchten Ereignisdaten.
	Sekundärspeicher, früher als „Netzwerkspeicher“ bezeichnet. (optional)	Optimiert für eine reduzierte Speicherplatzausnutzung auf eventuell preiswerteren Speichermedien, aber dennoch schnelles Abrufen. Sentinel migriert Datenpartitionen automatisch zum Sekundärspeicher.
	HINWEIS: Die Verwendung des Sekundärspeichers ist fakultativ. Datenbeibehaltungsrichtlinien, Suchen und Berichte werden in den Ereignisdatenpartitionen unabhängig vom Speicherort (primärer oder sekundärer Speicher oder beide) ausgeführt.	
Offlinespeicher	Archivierungsspeicher	Partitionen, die geschlossen werden, können Sie mit einem beliebigen Dateispeicherservice wie beispielsweise Amazon Glacier sichern. Sie können die Partitionen bei Bedarf für die Verwendung in Langzeituntersuchungen jederzeit vorübergehend wieder importieren.

Sie können Sentinel auch so konfigurieren, dass Ereignisdaten und Ereignisdatenzusammenfassungen unter Anwendung von Datensynchronisierungsrichtlinien zu einer externen Datenbank extrahiert werden. Weitere Informationen finden Sie unter „Configuring Data Synchronization (Konfigurieren der Datensynchronisierung)“ im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).

Bei der Installation von Sentinel muss die Datenträgerpartition für den Primärspeicher am Sentinel-Installationsstandort eingehängt werden. Standardmäßig ist dies das Verzeichnis `/var/opt/novell`.

Um die richtige Berechnung der Datenträgerauslastung zu gewährleisten, muss sich die gesamte Verzeichnisstruktur im Verzeichnis `/var/opt/novell/sentinel` auf einer einzigen Datenträgerpartition befinden. Andernfalls werden Ereignisdaten möglicherweise vorzeitig durch die automatische Datenverwaltung gelöscht. Weitere Informationen zur Sentinel-Verzeichnisstruktur finden Sie unter „Sentinel-Verzeichnisstruktur“, auf Seite 46.

Es empfiehlt sich, dieses Datenverzeichnis in einer anderen Datenträgerpartition anzulegen als die Partition, in der die ausführbaren Dateien, die Konfigurations- und die Betriebssystemdateien gespeichert sind. Das separate Speichern von Variablendaten bietet den Vorteil einer einfacheren Sicherung von Dateisätzen, einer einfacheren Wiederherstellung im Falle einer Beschädigung und einer besseren Stabilität, falls die Datenträgerpartition aufgefüllt ist. Außerdem verbessert es die allgemeine Leistung in Systemen, in denen kleinere Dateisysteme effizienter sind. Weitere Informationen finden Sie unter Disk Partitioning (Festplattenpartitionierung).

HINWEIS: Bei ext3-Dateisystemen ist die Dateispeicherung eingeschränkt. Ein Verzeichnis kann maximal 32.000 Dateien oder Unterverzeichnisse enthalten. Wenn Sie eine große Zahl an Beibehaltungsrichtlinien verwenden oder Daten über längere Zeit beibehalten, beispielsweise für ein Jahr, können Sie das XFS-Dateisystem verwenden.

- „Partitionen in herkömmlichen Installationen“, auf Seite 42
- „Partitionen bei Appliance-Installationen“, auf Seite 42
- „Best Practices für Partitionslayouts“, auf Seite 42
- „Grafikdatenspeicher konfigurieren“, auf Seite 43

Partitionen in herkömmlichen Installationen

Bei herkömmlichen Installationen können Sie das Layout der Datenträgerpartition des Betriebssystems vor der Installation von Sentinel ändern. Der Administrator muss hierzu die gewünschten Partitionen erstellen und für die entsprechenden Verzeichnisse mounten. Dabei wird die in „Sentinel-Verzeichnisstruktur“, auf Seite 46 beschriebene Verzeichnisstruktur verwendet. Beim Ausführen des Installationsprogramms wird Sentinel in die vorerstellten Verzeichnisse installiert. Die sich daraus ergebende Installation erstreckt sich über mehrere Partitionen.

HINWEIS:

- Beim Ausführen des Installationsprogramms können Sie mit der Option `--location` einen anderen Standort der obersten Ebene als die Standardverzeichnisse zum Speichern der Datei angeben. Der Wert, den Sie an die Option `--location` weiterreichen, wird den Verzeichnispfaden vorangestellt. Wenn Sie beispielsweise `--location=/foo` angeben, ist das Datenverzeichnis `/foo/var/opt/novell/sentinel/data` und das Konfigurationsverzeichnis `/foo/etc/opt/novell/sentinel/config`.
- Verwenden Sie keine Dateisystemverknüpfungen (zum Beispiel Softlinks) für die Option `--location`.

Partitionen bei Appliance-Installationen

Wenn Sie das DVD-ISO-Appliance-Format verwenden, können Sie die Partitionierung des Appliance-Dateisystems während der Installation gemäß den Anweisungen in den YaST-Bildschirmen konfigurieren. Sie können beispielsweise eine separate Partition für den Mountpunkt von `/var/opt/novell/sentinel` erstellen, um alle Daten in einer separaten Partition zu speichern. Für andere Appliance-Formate kann die Partitionierung erst nach der Installation konfiguriert werden. Mit dem SuSE Yast-Systemkonfigurationswerkzeug können Sie Partitionen hinzufügen und ein Verzeichnis zur neuen Partition hinzufügen. Weitere Informationen zum Erstellen von Partitionen nach der Installation finden Sie unter „Erstellen von Partitionen für herkömmlichen Speicher“, auf Seite 105.

Best Practices für Partitionslayouts

In vielen Organisationen stehen eigene, dokumentierte Empfehlungen für Partitionslayoutschemen zur Verfügung, die für alle installierten Systeme gelten. Die folgende Empfehlung für das Partitionslayout soll Organisationen, die keine definierten Richtlinien haben, als Leitfaden dienen. Sie geht von einer Sentinel-spezifischen Nutzung des Dateisystems aus. Im Allgemeinen befolgt Sentinel den Filesystem Hierarchy Standard, sofern dies umsetzbar ist.

Partition	Einhängepunkt	Größe	Notizen
root	/	100 GB	Enthält Betriebssystemdateien und Sentinel-Binärdaten/ die Sentinel-Konfiguration.
Booten	/boot	150 MB	Bootpartition

Partition	Einhängepunkt	Größe	Notizen
Primärspeicher	`/var/opt/novell/sentinel`	Berechnung anhand der Informationen zur Systemauslegung	Dieser Bereich enthält die erfassten Sentinel-Primärdaten und andere variable Daten wie Protokolldateien. Diese Partition kann mit anderen Systemen gemeinsam verwendet werden.
Sekundärspeicher	Speicherort je nach Speichertyp (NFS, CIFS oder SAN).	Berechnung anhand der Informationen zur Systemauslegung	Dies ist der Sekundärspeicherbereich, der remote oder wie dargestellt lokal eingehängt werden kann.
Archivierungsspeicher	Remote-System	Berechnung anhand der Informationen zur Systemauslegung	Dies ist der Speicher für archivierte Daten.

Grafikdatenspeicher konfigurieren

Sentinel stellt Ereignisgrafiken bereit, die Daten in Diagrammen, Tabellen und Karten präsentieren. Diese Grafiken erleichtern die Darstellung und Analyse großer Ereignismengen. Sie können auch eigene Ereignisgrafiken und Dashboards erstellen.

Sentinel nutzt Kibana, ein browserbasiertes Analyse- und Such-Dashboard, mit dem Sie Ereignisse suchen und grafisch präsentieren können. Kibana greift über den Grafikdatenspeicher (Elasticsearch) auf Daten zu, um die Ereignisse in Dashboards anzuzeigen. Standardmäßig enthält Sentinel einen Elasticsearch-Knoten, der nur Warnmeldungen speichert und indexiert. Sie müssen die Ereignisgrafikfunktion aktivieren, um Ereignisse in Elasticsearch zu speichern und zu indexieren.

Wenn Sie Elasticsearch zum Speichern und Indexieren von Daten aktivieren, indexiert Sentinel nur einige bestimmte Ereignisfelder, die zum Erstellen der Grafiken erforderlich sind, und speichert die indexierten Felder in Elasticsearch. Sentinel erstellt für jeden Tag einen eigenen Index und ermittelt das Indexdatum unter Zuhilfenahme der koordinierten Weltzeit (UTC; Mitternacht bis Mitternacht). Der Indexname hat das Format `security.events.normalized_jjjjMMtt`. So umfasst der Index `security.events.normalized_20160101` alle Ereignisse vom 1. Januar 2016.

Die Konfiguration des Grafikdatenspeichers umfasst Folgendes:

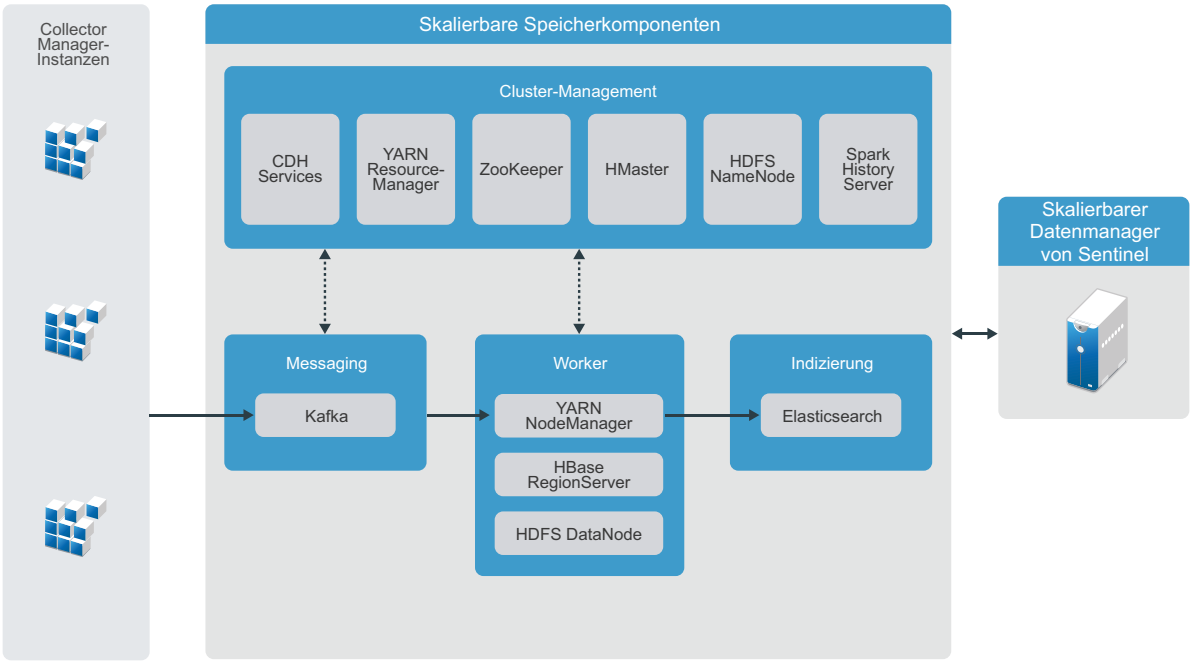
- ❒ **Elasticsearch-Knoten in einem Clustermodus installieren:** Standardmäßig enthält Sentinel einen Elasticsearch-Knoten. Zur Gewährleistung der optimalen Leistung und Stabilität des Sentinel-Servers müssen die Elasticsearch-Knoten in einem Clustermodus installiert werden. Weitere Informationen finden Sie unter Kapitel 12, „Installation und Konfiguration von Elasticsearch“, auf Seite 75.
- ❒ **Ereignisgrafiken aktivieren:** Standardmäßig ist die Ereignisgrafikfunktion deaktiviert. Informationen zur Aktivierung der Ereignisgrafiken finden Sie in Kapitel 20, „Ereignisgrafik aktivieren“, auf Seite 123.
- ❒ **Leistungsoptimierung:** Sentinel konfiguriert bestimmte Elasticsearch-Einstellungen automatisch für eine optimale Leistung. Sie können diese Einstellungen je nach Bedarf anpassen. Beispielsweise können Sie ändern, welche Ereignisfelder Elasticsearch indexieren soll. Weitere Informationen finden Sie unter „Leistungsoptimierung für Elasticsearch“, auf Seite 81.

Planen des skalierbaren Speichers

Sentinel nutzt das CDH-Framework (Distribution Including Apache Hadoop) von Cloudera zur Speicherung und Verwaltung großer Datenmengen. Zur Ereignisindexierung nutzt Sentinel eine skalierbare, verteilte Indexierungs-Engine namens Elasticsearch von Elastic.

Die folgende Abbildung zeigt die diversen Komponenten skalierbaren Speichers:

Abbildung 6-1 *Skalierbare Speicherarchitektur*



- **Messaging:** Sentinel verwendet Apache Kafka als skalierbares Nachrichtensystem zum Empfang normalisierter Ereignisse und Rohdaten von Collector Manager-Instanzen. Collector Manager-Instanzen senden Roh- und Ereignisdaten an Kafka-Cluster.

  Standardmäßig erstellt Sentinel die folgenden Kafka-Kategorien:

  - **security.events.normalized:** Speicherung aller verarbeiteten und normalisierten Ereignisdaten, darunter auch vom System erzeugte Ereignisse und interne Ereignisse
  - **security.events.raw:** Speicherung aller Rohdaten von den Ereignisquellen

  Ereignis- und Rohdaten entsprechen dem Apache Avro-Schema. Weitere Informationen finden Sie in der Apache Avro-Dokumentation. Die Schemadateien befinden sich im Verzeichnis `/etc/opt/novell/sentinel/scalablestore`.

- **Worker:** Dieser Knoten hostet Echtzeitaufträge für die Verarbeitung und Speicherung. Apache Spark ermöglicht die Echtzeit-Datenverarbeitung in großem Maßstab, z. B. die nach Mandanten-ID getrennte Speicherung, die Anforderung großer Datenmengen, die Speicherung von Daten im „System of Record“ (SOR) und die skalierbare Indexierung.

  Apache HBase ist eine verteilte, skalierbare Datenbank auf Hadoop-Basis. Sie dient als SOR für normalisierte Ereignisse und Rohdaten, die darin nach Mandanten-ID getrennt gespeichert werden.

Auf Basis der Mandanten-ID erstellt Sentinel für jeden Mandanten einen eigenen Namespace. Der Namespace des Standardmandanten lautet zum Beispiel „1“. Für jeden Namespace erstellt Sentinel die folgenden Tabellen und speichert Daten gemäß Ereigniszeitpunkt.

- ***<Mandanten-ID>*:security.events.normalized:** Speicherung aller verarbeiteten und normalisierten Ereignisdaten, darunter auch vom System erzeugte Ereignisse und interne Ereignisse
- ***<Mandanten-ID>*:security.events.raw:** Speicherung aller Rohdaten von den Ereignisquellen

- **Cluster-Management:** Dieser Knoten hostet alle Master und Cluster-Management-Services. Apache ZooKeeper ist ein zentraler Service für die Pflege von Konfigurationsdaten, Benennungen, die verteilte Synchronisierung und die Bereitstellung von Gruppenservices.
- **Indexierung:** Sentinel verwendet Elasticsearch als skalierbare und verteilte Indizierungs-Engine zum Indexieren von Ereignissen. Über Elasticsearch lassen sich Daten zur Suche und Visualisierung von Ereignissen nutzen.

  Sentinel erstellt für jeden Tag einen eigenen Index und ermittelt das Indexdatum unter Zuhilfenahme der koordinierten Weltzeit (UTC; Mitternacht bis Mitternacht). Der Indexname hat das Format `security.events.normalized_jjjjMMtt`. So umfasst der Index `security.events.normalized_20160101` alle Ereignisse vom 1. Januar 2016. Für optimale Leistung indexiert Sentinel nur einige spezielle Ereignisfelder. Welche Ereignisfelder Elasticsearch indexieren soll, können Sie bearbeiten. Weitere Informationen finden Sie unter „Leistungsoptimierung für Elasticsearch“, auf Seite 81.

Konfiguration des skalierbaren Speichers

Wenn Sie den skalierbaren Speicher aktivieren, bietet die Benutzeroberfläche des Sentinel-Servers nur noch Optionen für einige der Sentinel-Funktionen, wie Datenerfassung, Korrelation, Ereignis-Routing, Suche und Visualisierung von Ereignissen und Erledigung bestimmter administrativer Aufgaben. Diese verschlankte Version von Sentinel wird als SSDM (Sentinel Scalable Data Manager – skalierbarer Datenmanager) bezeichnet. Um Sentinel-Funktionen wie die Sicherheitsintelligenz und die konventionelle Suche und Berichterstellung zu nutzen, müssen Sie separate Sentinel-Instanzen installieren und für herkömmlichen Speicher konfigurieren. Leiten Sie dann per Sentinel Link bestimmte Ereignisdaten von SSDM zu Sentinel weiter.

Die folgende Liste enthält Informationen zu den Services und Funktionen, die in SSDM nicht verfügbar sind:

- Berichte
- Sicherheitsintelligenz
- Ausführen von Ereignisvorgängen während der Suche
- Testen von Korrelationsregeln
- Erstellung und Verwaltung von Vorfällen
- Manuelles Ausführen von Aktionen für Ereignisse
- Datensynchronisierung
- iTRAC-Workflows
- Forensische Analyse von Ereignissen, die das korrelierte Ereignis auslösen
- Anzeigen von Ereignisanlagen für Secure Configuration Manager- und Change Guardian-Ereignisse

Der skalierbare Speicher lässt sich nur einmal aktivieren; die Entscheidung ist unumkehrbar. Wenn Sie den skalierbaren Speicher deaktivieren und zum herkömmlichen Speicher wechseln möchten, müssen Sie Sentinel neu installieren.

Die folgende Checkliste enthält allgemeine Informationen zu den Aufgaben bei der Konfiguration des skalierbaren Speichers:

Tabelle 6-2 *Checkliste für die Konfiguration des skalierbaren Speichers*

	Aufgaben	Erklärt in
❒	Lesen Sie die Bereitstellungsinformationen im Hinblick auf das Verfahren bei Verwendung von Sentinel mit skalierbarem Speicher.	„Drei-Ebenen-Bereitstellung mit skalierbarem Speicher“, auf Seite 51
❒	Prüfen Sie, ob alle Voraussetzungen erfüllt sind, und führen Sie alle erforderlichen Aktionen durch.	Kapitel 13, „Installation und Einrichtung von skalierbarem Speicher“, auf Seite 85.
❒	Aktivieren Sie den skalierbaren Speicher. Sie können den skalierbaren Speicher sowohl während als auch nach der Installation aktivieren. In Aufrüstungsinstallationen können Sie den skalierbaren Speicher erst nach der Aufrüstung von Sentinel aktivieren.	Um den skalierbaren Speicher während der Installation zu aktivieren, führen Sie eine benutzerdefinierte Installation von Sentinel durch. Weitere Informationen hierzu finden Sie in „Angepasste Sentinel-Serverinstallation“, auf Seite 90. Zur Aktivierung des skalierbaren Speichers nach der Installation oder nach einer Aufrüstung beachten Sie die Informationen unter Enabling Scalable Storage Post-Installation(Aktivieren des skalierbaren Speichers nach der Installation) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).
❒	Konfigurieren Sie die CDH-Komponenten und Elasticsearch mit Sentinel.	Configuring Scalable Storage (Konfigurieren des skalierbaren Speichers) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Sentinel-Verzeichnisstruktur

Standardmäßig befinden sich die Sentinel-Verzeichnisse an folgenden Standorten:

- Die Datendateien befinden sich in den Verzeichnissen `/var/opt/novell/sentinel/data` und `/var/opt/novell/sentinel/3rdparty`.
- Die ausführbaren Dateien und Bibliotheken befinden sich im Verzeichnis `/opt/novell/sentinel/`..
- Die Protokolldateien befinden sich im Verzeichnis `/var/opt/novell/sentinel/log`.
- Temporäre Dateien befinden sich im Verzeichnis `/var/opt/novell/sentinel/tmp`.
- Die Konfigurationsdateien befinden sich im Verzeichnis `/etc/opt/novell/sentinel/`.
- Die Prozess-ID-Datei (PID-Datei) befindet sich im Verzeichnis `/home/novell/sentinel/server.pid`.

  Mit der PID können Administratoren den übergeordneten Prozess des Sentinel-Servers identifizieren und den Prozess überwachen oder beenden.

Vorteile von verteilten Bereitstellungen

Standardmäßig beinhaltet der Sentinel-Server die folgenden Komponenten:

- **Collector Manager:** Collector Manager stellt eine flexible Datenerfassungsstelle für Sentinel bereit.
- **Correlation Engine:** Die Correlation Engine verarbeitet Ereignisse aus dem Echtzeit-Ereignisstrom, um zu ermitteln, ob Korrelationsregeln ausgelöst werden sollen.
- **Elasticsearch:** Optionale Datenspeicherkomponente zum Speichern und Indexieren von Daten. Standardmäßig enthält Sentinel einen Elasticsearch-Knoten. Wenn Sie große EPS über 2.500 erwarten, stellen Sie zusätzliche Elasticsearch-Knoten in einem Cluster bereit.

WICHTIG: Für Produktionsumgebungen sollten Sie eine verteilte Bereitstellung einrichten, da hierbei die Datenerfassungskomponenten auf einem separaten Computer isoliert werden. Dies ist für die Bewältigung von Spitzenlasten und anderen Anomalien mit größtmöglicher Systemstabilität wichtig.

In diesem Abschnitt werden die Vorteile der verteilten Bereitstellung beschrieben.

- „Vorteile zusätzlicher Collector Manager-Instanzen“, auf Seite 47
- „Vorteile zusätzlicher Correlation Engine-Instanzen“, auf Seite 48

Vorteile zusätzlicher Collector Manager-Instanzen

Der Sentinel-Server umfasst standardmäßig einen Collector Manager. Für Produktionsumgebungen bieten verteilte Collector Manager-Instanzen jedoch eine deutlich bessere Isolierung, wenn große Datenmengen empfangen werden. In dieser Situation wird ein verteilter Collector Manager unter Umständen überlastet; der Sentinel-Server verarbeitet die Benutzeranforderungen jedoch weiter.

Die Installation von mehr als einem Collector Manager in einem verteilten Netzwerk bietet die folgenden Vorteile:

- **Verbesserte Systemleistung:** Zusätzliche Collector Manager-Instanzen können Ereignisdaten in einer verteilten Umgebung analysieren und verarbeiten und steigern so die Systemleistung.
- **Zusätzliche Datensicherheit und geringere Anforderungen an die Netzwerkbandbreite:**

  Wenn die Collector Manager-Instanzen gemeinsam mit Ereignisquellen installiert werden, können Filterung, Verschlüsselung und Datenkomprimierung an der Quelle ausgeführt werden.
- **Datei-Caching:** Zusätzliche Collector Manager-Instanzen können große Datenmengen im Cache speichern, während der Server vorübergehend mit dem Archivieren von Ereignissen oder dem Verarbeiten von Ereignisspitzen ausgelastet ist. Diese Funktion ist von Vorteil bei Protokollen wie Syslog, die nicht von vornherein ein Ereignis-Caching unterstützen.

Sie können zusätzliche Collector Manager-Instanzen an den geeigneten Speicherorten in Ihrem Netzwerk installieren. Diese Remote-Instanzen von Collector Manager führen Connectors und Collectors aus und leiten die erfassten Daten zur Speicherung und Verarbeitung an den Sentinel-Server weiter. Weitere Informationen zum Installieren von zusätzlichen Collector Manager-Instanzen finden Sie unter Teil III, „Installieren von Sentinel“, auf Seite 69.

HINWEIS: Sie können immer nur einen Collector Manager auf einem einzelnen System installieren. Sie können zusätzliche Collector Manager-Instanzen auf Remote-Systemen installieren und diese dann mit dem Sentinel-Server verbinden.

Vorteile zusätzlicher Correlation Engine-Instanzen

Sie können mehrere Correlation Engine-Instanzen (jede auf einem eigenen Server) bereitstellen, ohne dass Konfigurationen repliziert oder Datenbanken hinzugefügt werden müssen. In Umgebungen mit vielen Korrelationsregeln oder extrem hohen Ereignisraten ist es von Vorteil, mehr als eine Correlation Engine zu installieren und einige Regeln auf der neuen Correlation Engine erneut bereitzustellen. Wenn das Sentinel-System zusätzliche Datenquellen aufnimmt oder die Ereignisrate steigt, bieten mehrere Correlation Engine-Instanzen die Möglichkeit der Skalierung. Informationen zur Installation von zusätzlichen Correlation Engine-Instanzen finden Sie unter Teil III, „Installieren von Sentinel“, auf Seite 69.

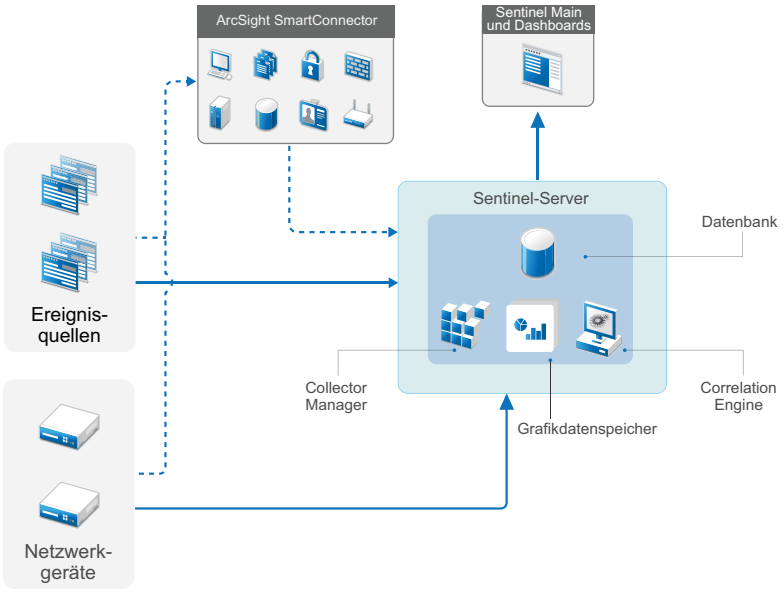
HINWEIS: Sie können immer nur eine Correlation Engine auf einem einzelnen System installieren. Sie können zusätzliche Correlation Engine-Instanzen auf Remote-Systemen installieren und diese dann mit dem Sentinel-Server verbinden.

All-In-One-Bereitstellung

Die einfachste Bereitstellungsoption ist ein All-In-One-System, bei dem alle Sentinel-Komponenten auf nur einem Computer installiert werden. Die All-In-One-Bereitstellung eignet sich nur, wenn die Systemlast relativ klein ist und keine Windows-Computer überwacht werden müssen. In vielen Umgebungen können unvorhersehbare und variierende Lasten und Ressourcenkonflikte zwischen den Komponenten Leistungsprobleme verursachen.

WICHTIG: Für Produktionsumgebungen sollten Sie eine verteilte Bereitstellung einrichten, da hierbei die Datenerfassungskomponenten auf einem separaten Computer isoliert werden. Dies ist für die Bewältigung von Spitzenlasten und anderen Anomalien mit größtmöglicher Systemstabilität wichtig.

Abbildung 6-2 *All-In-One-Bereitstellung*

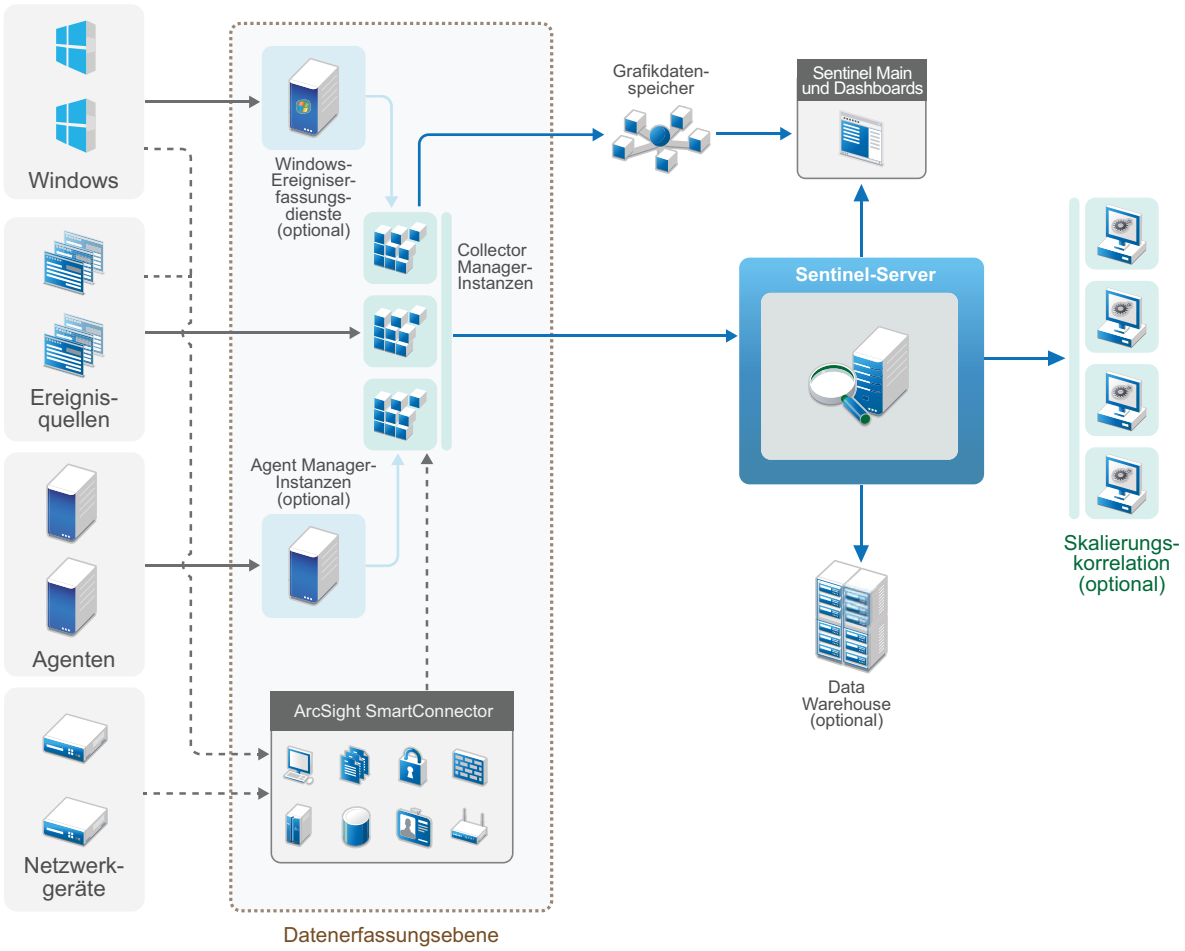


Verteilte Ein-Ebenen-Bereitstellung

Eine Ein-Ebenen-Bereitstellung bietet die Möglichkeit, Windows-Computer zu überwachen und eine höhere Last als mit der All-In-One-Bereitstellung zu verarbeiten. Sie können Datenerfassung und -korrelation horizontal skalieren, indem Sie Collector Manager- und Correlation Engine-Computer hinzufügen, die den zentralen Sentinel-Server von der Verarbeitung entlasten. Remote-Collector-Manager und Remote-Correlation Engines übernehmen die Last der Ereignisse und Korrelationsregeln und geben außerdem Ressourcen auf dem zentralen Sentinel-Server frei, sodass dieser andere Anfragen wie das Speichern von Ereignissen oder das Ausführen von Suchen verarbeiten kann. Bei steigender Last auf dem System kann der zentrale Sentinel-Server einen Engpass darstellen. Zur weiteren Skalierung ist dann eine Bereitstellung mit weitere Ebenen erforderlich.

Sie können Sentinel fakultativ so konfigurieren, dass die Ereignisdaten in ein Data Warehouse kopiert werden. So können eine benutzerdefinierte Berichterstellung, Analysen und andere Verarbeitungen auf ein anderes System übertragen werden.

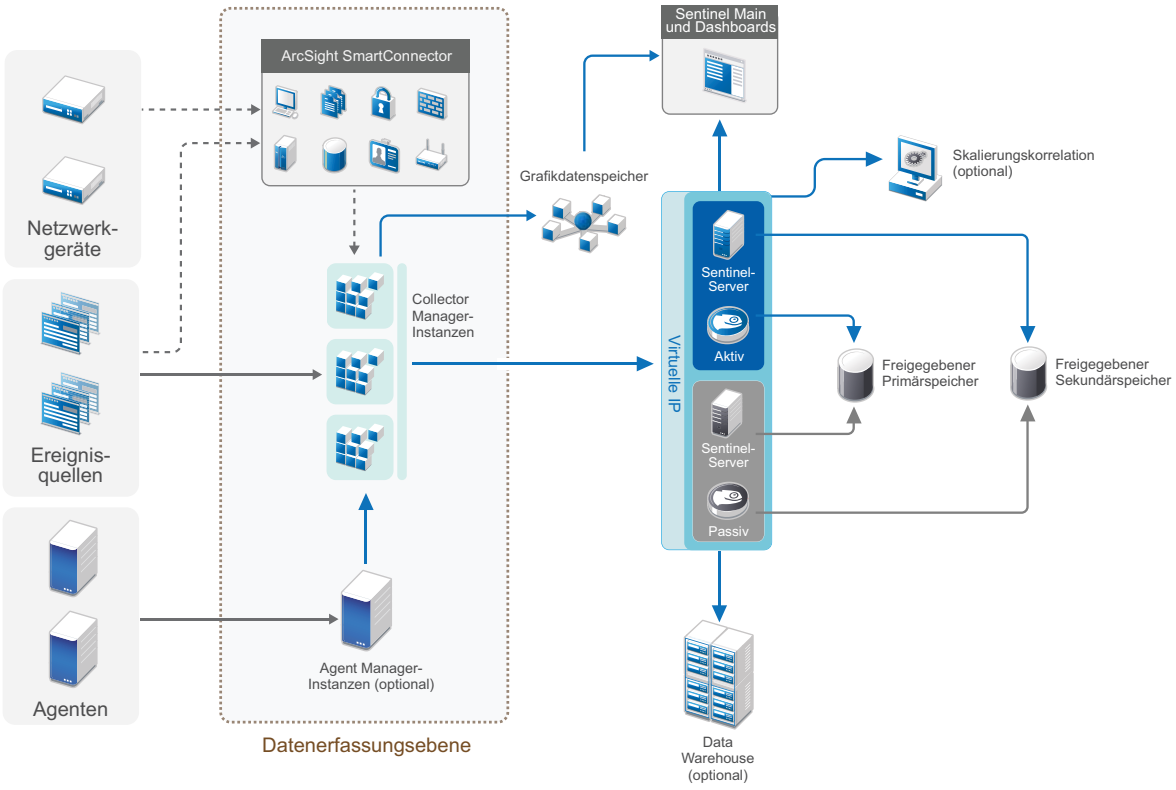
Abbildung 6-3 *Verteilte Ein-Ebenen-Bereitstellung*



Verteilte Ein-Ebenen-Bereitstellung mit hoher Verfügbarkeit

Die verteilte Ein-Ebenen-Bereitstellung kann in ein Hochverfügbarkeitssystem mit Failover-Redundanz umgewandelt werden. Weitere Informationen zur Bereitstellung von Sentinel mit hoher Verfügbarkeit finden Sie unter Teil VII, „Bereitstellen von Sentinel für Hochverfügbarkeitssysteme“, auf Seite 187.

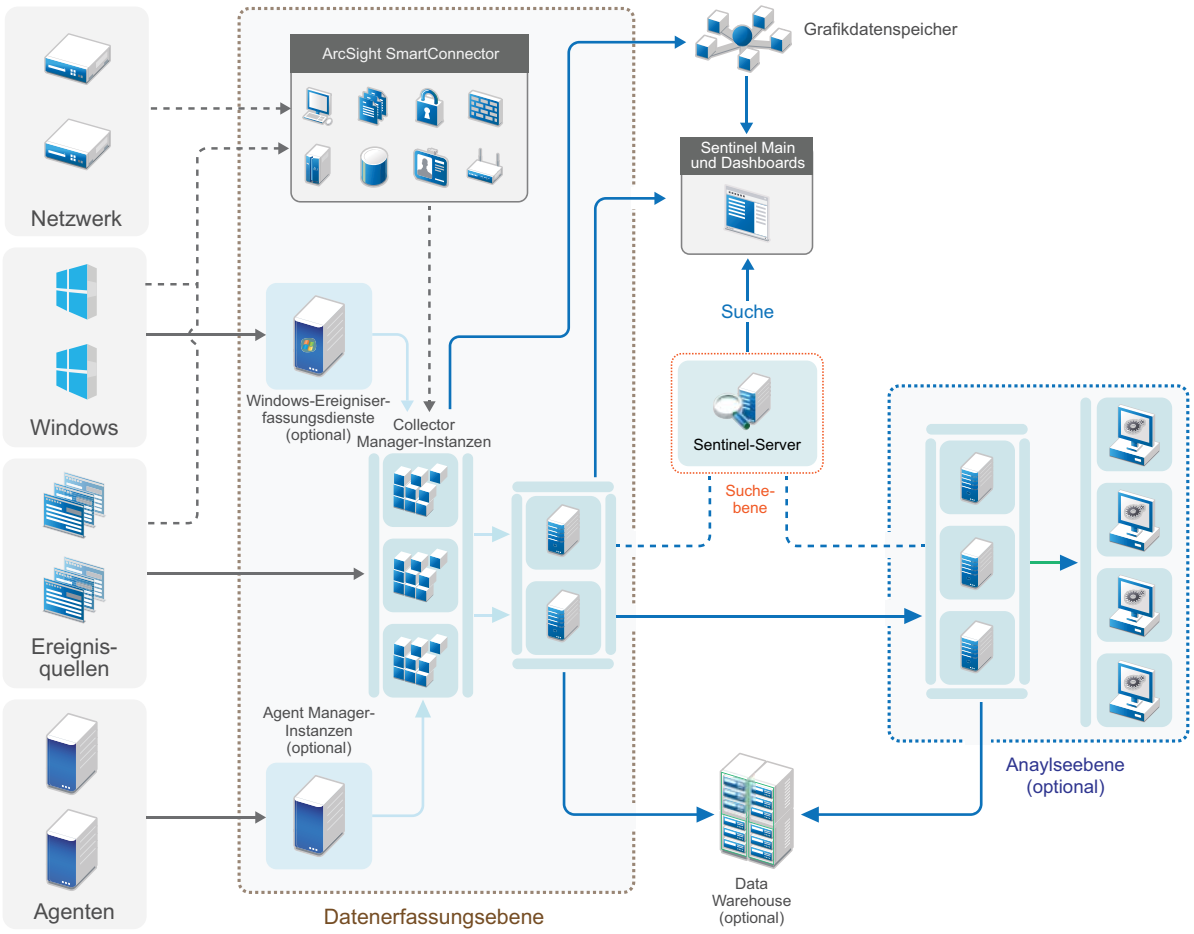
Abbildung 6-4 *Verteilte Ein-Ebenen-Bereitstellung mit hoher Verfügbarkeit*



Verteilte Zwei-Ebenen- und Drei-Ebenen-Bereitstellung

Mit dieser Art der Bereitstellung kann die Lastverarbeitungskapazität eines einzelnen, zentralen Sentinel-Servers übertroffen werden. Die Verarbeitungslast wird auf mehrere Sentinel-Instanzen verteilt, indem die Funktionen von Sentinel Link und Sentinel-Datenverbund optimal ausgenutzt werden. Die Last der Datenerfassung wird über mehrere Sentinel-Server verteilt, die jeweils über mehrere Collector Manager-Instanzen verfügen, wie in der Datenerfassungsebene dargestellt. Wenn Sie eine Ereigniskorrelation oder Sicherheitsintelligenz ausführen möchten, können die Daten fakultativ über Sentinel Link an die Analyseebene weitergeleitet werden. Die Suchebene stellt einen bequemen zentralen Zugriffspunkt für Suchen über den Sentinel-Datenverbund im gesamten System und auf allen Ebenen dar. Da die Suchanforderung über mehrere Instanzen von Sentinel im Verbund ausgeführt wird, sorgt diese Art der Bereitstellung auch für eine Lastverteilung bei Suchen, die bei der Skalierung zwecks Verarbeitung einer hohen Suchlast nützlich ist.

Abbildung 6-5 *Verteilte Zwei-Ebenen- und Drei-Ebenen-Bereitstellung*



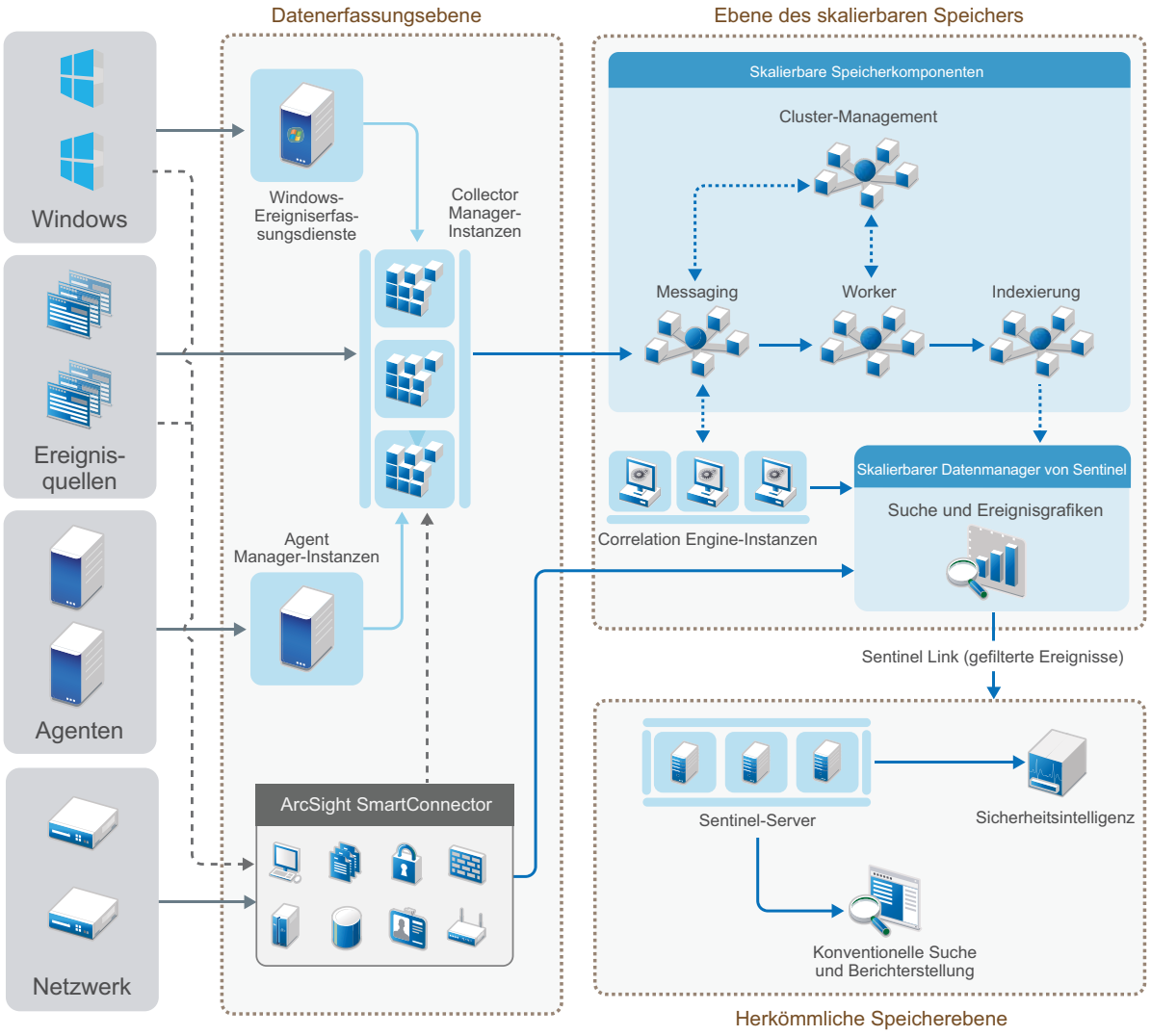
Drei-Ebenen-Bereitstellung mit skalierbarem Speicher

Die Drei-Ebenen-Bereitstellung mit skalierbarem Speicher eignet sich für die umfangreiche Datenspeicherung und -verarbeitung, für die Ereignisse nicht auf mehrere Sentinel-Server verteilt und Konfigurationseinstellungen nicht auf mehrere Instanzen kopiert werden sollen. Bei dieser Art der Bereitstellung speichern und verwalten Sie große Datenmengen auf einem einzigen Sentinel-Server statt auf mehreren, weil dieser mit skalierbarem Speicher arbeitet.

Sie können einen neuen Sentinel-Server mit skalierbarem Speicher einrichten oder einen vorhandenen Sentinel-Server zur Aktivierung des skalierbaren Speichers aufrüsten.

Wählen Sie je nach den von Ihnen gewünschten Sentinel-Funktionen, wie Sie Ihre Sentinel-Bereitstellung einrichten möchten.

Abbildung 6-6 *Drei-Ebenen-Bereitstellung für skalierbaren Speicher*



Die Ebenen dieser Art der Bereitstellung:

- **Datenerfassungsebene:** Zum Erfassen von Ereignissen von einem breiten Spektrum an Ereignisquellen. Wenn Sie Ihre vorhandene Datenerfassungseinrichtung in Sentinel mit herkömmlichem Speicher beibehalten möchten, aber dennoch die Möglichkeiten des skalierbaren Speichers nutzen möchten, können Sie optional die gewünschten Ereignisse vom herkömmlichen Speicher zum skalierbaren Speicher weiterleiten. Verwenden Sie hierzu das Skript `_data_uploader.sh`. Weitere Informationen finden Sie unter Kapitel 32, „Migrieren von Daten zum skalierbaren Speicher“, auf Seite 177.
- **Ebene des skalierbaren Speichers:** Zum Speichern, Indexieren und Analysieren von großen Datenmengen. Mit dem SSDM-Server in dieser Ebene können Sie die Datenerfassung und -korrelation verwalten. Außerdem bietet der SSDM-Server weitere SSDM-Funktionen. Um Sentinel-Funktionen zu nutzen, die in SSDM nicht verfügbar sind, können Sie die herkömmliche Speicherebene einrichten. Sie können die erfassten Daten auch an andere SIEM-Systeme weiterleiten oder weitere Business-Intelligence-Werkzeuge aktivieren, um Daten abzufragen oder Analysen mit den umfangreich unterstützten APIs von Hadoop, Kafka, Spark und Elasticsearch direkt in der Hadoop-Verteilung auszuführen.

- **Herkömmliche Speicherebene:** Für Sentinel-Funktionen wie die Sicherheitsintelligenz und die konventionelle Suche und Berichterstellung müssen Sie separate Instanzen von Sentinel mit herkömmlichem Speicher installieren. Sie können Ereignis-Routing-Regeln konfigurieren, um die gewünschten Ereignisse von SSDM über Sentinel Link zu Sentinel weiterzuleiten.

  Für die Suche und Berichterstellung können Sie auch jeden anderen Sentinel-Server der herkömmlichen Speicherebene verwenden. Optional können Sie eine separate Suchebene einrichten, die einen praktischen, zentralen Zugriffspunkt für die Suche und die Berichterstellung auf allen Sentinel-Servern der herkömmlichen Speicherebene bietet. Wenn Sie Ereignisse im skalierbaren Speicher suchen, verwenden Sie bitte die Suchoption in SSDM.

Weitere Informationen zur Installation und Einrichtung von skalierbarem Speicher finden Sie in Kapitel 13, „Installation und Einrichtung von skalierbarem Speicher“, auf Seite 85.

7 Überlegungen zur Bereitstellung für den FIPS 140-2-Modus

Sie können Sentinel optional so konfigurieren, dass es für die interne Verschlüsselung und andere Funktionen Mozilla Network Security Services (NSS) verwendet, einen nach FIPS 140-2 geprüften Verschlüsselungsanbieter. Dadurch soll sichergestellt werden, dass auf Sentinel „FIPS 140-2 Inside“ zutrifft und dass es die nationalen Einkaufsrichtlinien und -standards der USA erfüllt.

Bei Aktivierung des Sentinel FIPS 140-2-Modus wird für die Kommunikation zwischen dem Sentinel-Server, den Sentinel-Remote-Instanzen von Collector Manager, den Sentinel-Remote-Instanzen von Correlation Engine, der Benutzeroberfläche von Sentinel Main, dem Sentinel Control Center und dem Sentinel Advisor-Service die FIPS 140-2-geprüfte Verschlüsselung verwendet.

WICHTIG: Der FIPS-Modus wird nur für Sentinel unterstützt. Sentinel wird nicht unterstützt, wenn das Betriebssystem im FIPS-Modus ist.

FIPS-Implementierung in Sentinel

Sentinel verwendet die Mozilla-NSS-Bibliotheken, die vom Betriebssystem bereitgestellt werden. Red Hat Enterprise Linux (RHEL) und SUSE Linux Enterprise Server (SLES) verfügen über unterschiedliche NSS-Pakete.

Das NSS-Verschlüsselungsmodul, das von RHEL 6.3 und höher bereitgestellt wird, ist FIPS 140-2-validiert. Das in SLES 11 enthaltene NSS-Verschlüsselungsmodul ist noch nicht offiziell FIPS 140-2-validiert, doch es wird daran gearbeitet, das SUSE-Modul für FIPS 140-2 zu validieren. Wenn die Validierung verfügbar ist, sind keine Änderungen an Sentinel zu erwarten, um „FIPS 140-2 Inside“ auf der SUSE-Plattform bereitstellen zu können.

Weitere Informationen zur FIPS 140-2-Zertifizierung für RHEL finden Sie auf https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2711 und https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1837.

RHEL-NSS-Pakete

Sentinel benötigt die folgenden 64-Bit NSS-Pakete, um den FIPS 140-2-Modus unterstützen zu können:

- nspr-*
- nss-sysinit-*
- nss-util-*

- nss-softokn-freebl-*
- nss-softokn-*
- nss-*
- nss-tools-*

Falls diese Pakete noch nicht installiert sind, müssen Sie sie vor der Aktivierung des FIPS 140-2-Modus in Sentinel installieren.

SLES-NSS-Pakete

Sentinel benötigt die folgenden 64-Bit NSS-Pakete, um den FIPS 140-2-Modus unterstützen zu können:

- libfreebl3-*
- mozilla-nspr-*
- mozilla-nss-*
- mozilla-nss-tools-*

Falls diese Pakete noch nicht installiert sind, müssen Sie sie vor der Aktivierung des FIPS 140-2-Modus in Sentinel installieren.

FIPS-fähige Komponenten in Sentinel

Die folgenden Sentinel-Komponenten unterstützen FIPS 140-2:

- Alle Sentinel-Plattformkomponenten wurden zur Unterstützung des FIPS 140-2-Modus aktualisiert.
- Die folgenden Sentinel-Plugins, die die Verschlüsselung unterstützen, wurden aktualisiert für die Unterstützung des FIPS 140-2-Modus:
  - Agent Manager Connector 2011.1r1 und höher
  - Database (JDBC) Connector 2011.1r2 und höher
  - Datei-Connector 2011.1r1 oder höher (nur bei lokalem oder NFS-Ereignisquellentyp)
  - LDAP Integrator 2011.1r1 und höher
  - Sentinel Link Connector 2011.1r3 und höher
  - Sentinel Link Integrator 2011.1r2 und höher
  - SMTP Integrator 2011.1r1 und höher
  - Syslog Connector 2011.1r2 und höher
  - Windows Event (WMI) Connector 2011.1r2 und höher
  - Check Point (LEA) Connector 2011.1r2 und höher
  - Syslog Integrator 2011.1r1 und höher

  Weitere Informationen zur Konfiguration dieser Sentinel-Plugins für den FIPS 140-2-Modus finden Sie unter „Konfigurieren der Sentinel-Plugins zur Ausführung im FIPS 140-2-Modus“, auf Seite 134.

Die folgenden Sentinel-Connectors, die die optionale Verschlüsselung unterstützen, sind zum Zeitpunkt der Veröffentlichung dieses Dokuments noch nicht aktualisiert für die Unterstützung des FIPS 140-2-Modus. Sie können jedoch weiterhin mit diesem Connector Ereignisse erfassen.

Informationen zur Verwendung dieser Connectors mit Sentinel im FIPS 140-2-Modus finden Sie unter „Verwenden von Connectors im Nicht-FIPS-Modus mit Sentinel im FIPS 140-2-Modus“, auf Seite 141.

- Cisco SDEE Connector 2011.1r1
- Datei-Connector 2011.1r1: Die CIFS- und SCP-Funktionen arbeiten mit Kryptographie und funktionieren nicht im FIPS 140-2-Modus.
- Audit Connector 2011.1r1
- SNMP Connector 2011.1r1

Die folgenden Sentinel-Integratoren, die SSL unterstützen, sind zum Zeitpunkt der Veröffentlichung dieses Dokuments nicht für die Unterstützung des FIPS 140-2-Modus aktualisiert. Sie können jedoch weiterhin nicht verschlüsselte Verbindungen verwenden, wenn diese Integratoren mit Sentinel im FIPS 140-2-Modus verwendet werden.

- Remedy Integrator 2011.1r1 oder höher
- SOAP Integrator 2011.1r1 oder höher

Alle anderen Sentinel-Plugins, die oben nicht genannt wurden, verwenden keine Verschlüsselung und sind von der Aktivierung des FIPS 140-2-Modus in Sentinel nicht betroffen. Sie brauchen keine weiteren Schritte auszuführen, um diese Plugins mit Sentinel im FIPS 140-2-Modus zu verwenden.

Weitere Informationen zu den Sentinel-Plugins finden Sie auf der Website für Sentinel-Plugins. Falls eines der Plugins, das noch nicht aktualisiert wurde, mit FIPS-Unterstützung bereitgestellt werden soll, können Sie eine Anforderung über Bugzilla senden.

Vom FIPS-Modus betroffene Datenverbindungen

Wenn Sentinel im FIPS 140-2-Modus ist, können Sie keine verschlüsselten Verbindungen zu Microsoft SQL Server herstellen. Dies wirkt sich auf die folgenden Arten von Sentinel-Vorgängen aus:

- Datensynchronisierungsrichtlinien zu SQL Server
- Kommunikation zwischen dem Sentinel-Server und der Agent Manager-Datenbank
- Erfassung von Daten von SQL Server durch den Datenbank-Connector

Implementierungs-Checkliste

In der folgenden Tabelle finden Sie einen Überblick über die Aufgaben, die zur Konfiguration von Sentinel für den Betrieb im FIPS 140-2-Modus erforderlich sind.

Aufgaben	Weitere Informationen finden Sie unter…
Planen Sie die Bereitstellung.	„Bereitstellungsszenarien“, auf Seite 58.
Bestimmen Sie, ob Sie den FIPS 140-2-Modus während der Sentinel-Installation aktivieren müssen oder ob Sie ihn später aktivieren möchten. Zur Aktivierung des FIPS 140-2-Modus während der Installation müssen Sie die benutzerdefinierte oder automatische Installationsmethode während des Installationsvorgangs auswählen.	„Angepasste Sentinel-Serverinstallation“, auf Seite 90. „Ausführen einer automatischen Installation“, auf Seite 95 Kapitel 23, „Aktivieren des FIPS 140-2-Modus in einer vorhandenen Sentinel-Installation“, auf Seite 129

Aufgaben	Weitere Informationen finden Sie unter…
Konfigurieren Sie die Sentinel-Plugins zur Ausführung im FIPS 140-2-Modus.	„Konfigurieren der Sentinel-Plugins zur Ausführung im FIPS 140-2-Modus“, auf Seite 134.
Importieren Sie Zertifikate in den Sentinel-FIPS-Keystore.	„Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141

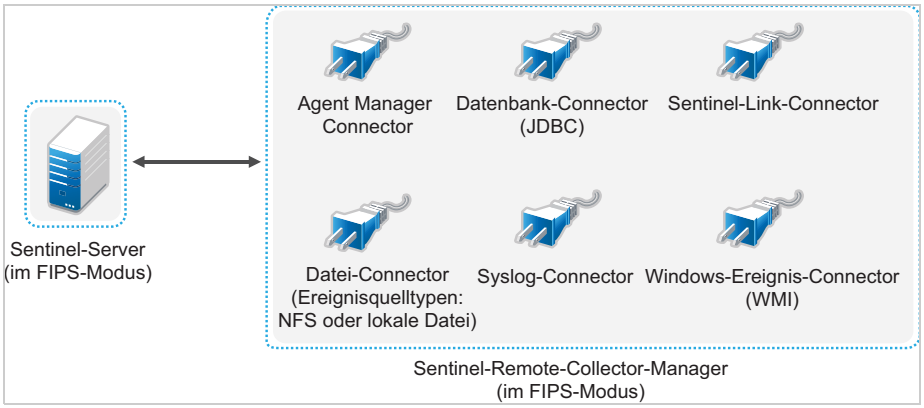
HINWEIS: Sichern Sie Ihre Sentinel-Systeme, bevor Sie die Konvertierung in den FIPS-Modus beginnen. Wenn der Server zu einem späteren Zeitpunkt auf den Nicht-FIPS-Modus zurückgesetzt werden muss, ist dies nur über die Wiederherstellung von einer Sicherung möglich. Weitere Informationen zum Zurücksetzen in den Nicht-FIPS-Modus finden Sie unter „Zurücksetzen von Sentinel in den Nicht-FIPS-Modus“, auf Seite 142.

Bereitstellungsszenarien

In diesem Abschnitt finden Sie Informationen zu den Bereitsstellungsszenarien für Sentinel im FIPS 140-2-Modus.

Szenario 1: Datenerfassung im vollständigen FIPS 140-2-Modus

In diesem Szenario erfolgt die Datenerfassung nur durch die Connectors, die den FIPS 140-2-Modus unterstützen. Wir nehmen an, dass in dieser Umgebung ein Server vorhanden ist und die Daten durch eine Remote-Instanz von Collector Manager erfasst werden. Sie können einen oder mehrere Remote-Instanzen von Collector Manager verwenden.



Sie müssen die folgende Prozedur nur ausführen, wenn in Ihrer Umgebung Daten von Ereignisquellen mit Connectors erfasst werden, die den FIPS 140-2-Modus unterstützen.

1 Sie müssen über einen Sentinel-Server im FIPS 140-2-Modus verfügen.

HINWEIS: Wenn Ihr (neu installierter oder aktualisierter) Sentinel-Server im Nicht-FIPS-Modus ausgeführt wird, müssen sie FIPS am Sentinel-Server aktivieren. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus am Sentinel-Server“, auf Seite 129.

2 Sie müssen über eine Sentinel-Remote-Instanz von Collector Manager verfügen, der im FIPS 140-2-Modus ausgeführt wird.

HINWEIS: Wenn Ihre (neu installierter oder aktualisierter) Remote-Instanz von Collector Manager im Nicht-FIPS-Modus ausgeführt wird, müssen sie FIPS an der Remote-Instanz von Collector Manager aktivieren. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus auf Remote-Instanzen von Collector Manager und Correlation Engine“, auf Seite 130.

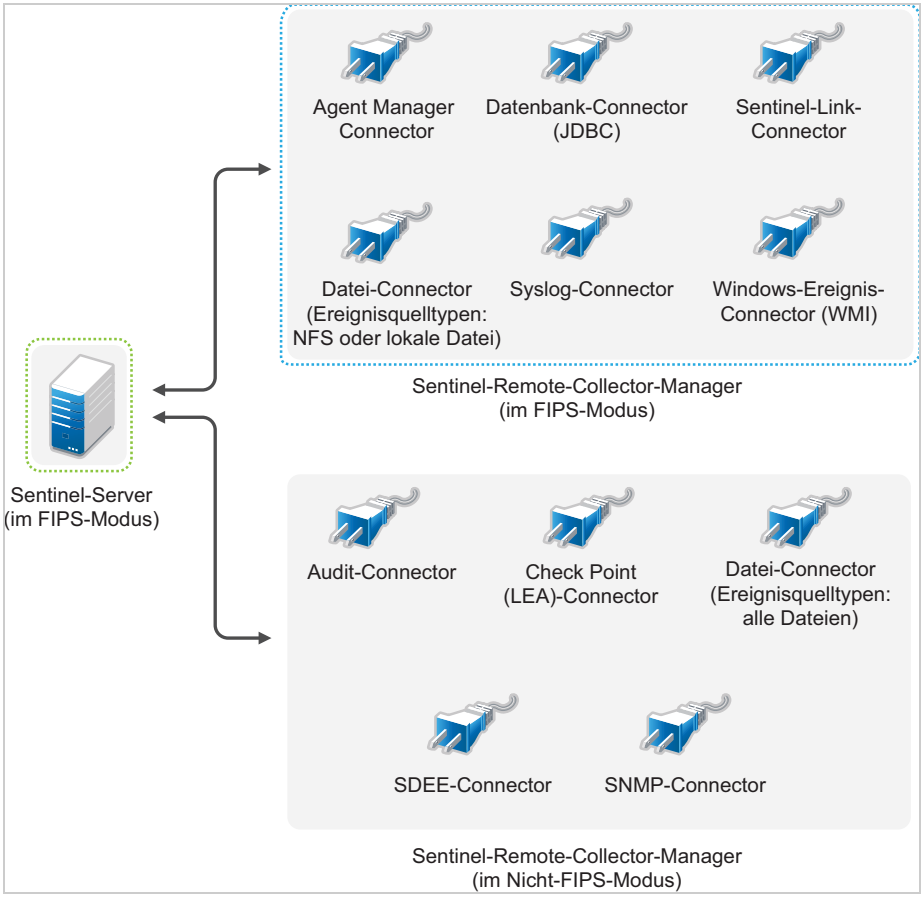
3 Vergewissern Sie sich, dass der FIPS-Server und die Remote-Instanzen von Collector Manager miteinander kommunizieren.

4 Stellen Sie eventuell vorhandene Remote-Instanzen von Correlation Engine auf den FIPS-Modus um. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus auf Remote-Instanzen von Collector Manager und Correlation Engine“, auf Seite 130.

5 Konfigurieren Sie die Sentinel-Plugins zur Ausführung im FIPS 140-2-Modus. Weitere Informationen finden Sie unter „Konfigurieren der Sentinel-Plugins zur Ausführung im FIPS 140-2-Modus“, auf Seite 134.

Szenario 2: Datenerfassung im teilweisen FIPS 140-2-Modus

In diesem Szenario erfolgt die Datenerfassung über Connectors, die den FIPS 140-2-Modus unterstützen, und über Connectors, die den FIPS 140-2-Modus nicht unterstützen. Wir gehen davon aus, dass Daten über eine Remote-Instanz von Collector Manager erfasst werden. Sie können einen oder mehrere Remote-Instanzen von Collector Manager verwenden.



Zur Handhabung der Datenerfassung über Connectors, die den FIPS 140-2-Modus unterstützen, und solche, die dies nicht tun, sollten Sie zwei Remote-Instanzen von Collector Manager verwenden. Die eine wird im FIPS 140-2-Modus ausgeführt für Connectors, die FIPS unterstützen. Die andere wird im Nicht-FIPS-Modus (normalen Modus) ausgeführt für Connectors, die den FIPS 140-2-Modus nicht unterstützen.

Sie müssen wie folgt vorgehen, wenn in Ihrer Umgebung Daten von Ereignisquellen sowohl mit Connectors erfasst werden, die den FIPS 140-2-Modus unterstützen, als auch mit Connectors, die den FIPS 140-2-Modus nicht unterstützen.

1 Sie müssen über einen Sentinel-Server im FIPS 140-2-Modus verfügen.

HINWEIS: Wenn Ihr (neu installierter oder aktualisierter) Sentinel-Server im Nicht-FIPS-Modus ausgeführt wird, müssen sie FIPS am Sentinel-Server aktivieren. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus am Sentinel-Server“, auf Seite 129.

---

2 Stellen Sie sicher, dass eine Remote-Instanz von Collector Manager im FIPS 140-2-Modus und eine andere Remote-Instanz von Collector Manager weiterhin im Nicht-FIPS-Modus ausgeführt wird.

   2a Wenn Sie über keine Remote-Instanz von Collector Manager verfügen, die für den FIPS 140-2-Modus aktiviert wurde, müssen Sie den FIPS-Modus auf einer Remote-Instanz von Collector Manager aktivieren. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus auf Remote-Instanzen von Collector Manager und Correlation Engine“, auf Seite 130.

   2b Aktualisieren Sie das Serverzertifikat auf der Remote-Instanz von Collector Manager im Nicht-FIPS-Modus. Weitere Informationen finden Sie unter „Aktualisieren der Serverzertifikate in Remote-Instanzen von Collector Managern und Correlation Engine“, auf Seite 133.

3 Vergewissern Sie sich, dass die beiden Remote-Instanzen von Collector Manager mit dem FIPS 140-2-fähigen Sentinel-Server kommunizieren.

4 Stellen Sie eventuell vorhandene Remote-Instanzen von Correlation Engine auf den FIPS 140-2-Modus um. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus auf Remote-Instanzen von Collector Manager und Correlation Engine“, auf Seite 130.

5 Konfigurieren Sie die Sentinel-Plugins so, dass sie im FIPS 140-2-Modus ausgeführt werden. Weitere Informationen finden Sie unter „Konfigurieren der Sentinel-Plugins zur Ausführung im FIPS 140-2-Modus“, auf Seite 134.

   5a Stellen Sie Connectors, die den FIPS 140-2-Modus unterstützen, in der Remote-Instanz von Collector Manager bereit, die im FIPS-Modus ausgeführt wird.

   5b Stellen Sie Connectors, die den FIPS 140-2-Modus nicht unterstützen, in der Remote-Instanz von Collector Manager bereit, die nicht im FIPS-Modus ausgeführt wird.

8 Verwendete Ports

Für die externe Kommunikation mit anderen Komponenten verwendet Sentinel verschiedene Ports. Für die Appliance-Installation werden die Ports standardmäßig in der Firewall geöffnet. Für die herkömmliche Installation müssen Sie jedoch das Betriebssystem, auf dem Sie Sentinel installieren, so konfigurieren, dass die entsprechenden Ports in der Firewall geöffnet sind.

Sentinel-Server-Ports

Der Sentinel-Server verwendet die folgenden Ports für die interne und externe Kommunikation.

Lokale Ports

Für die interne Kommunikation mit der Datenbank und mit anderen internen Prozessen verwendet Sentinel folgende Ports:

Ports	Beschreibung
TCP 27017	Wird für die Sicherheitsintelligenz-Konfigurationsdatenbank verwendet.
TCP 28017	Wird für die Webkonsole der Sicherheitsintelligenz-Datenbank verwendet.
TCP 32000	Wird für die interne Kommunikation zwischen dem Wrapper-Prozess und dem Serverprozess verwendet.
TCP 9200	Wird für die REST-Kommunikation mit dem Service für die Warnmeldungsindexierung verwendet.
TCP 9300	Wird für die Kommunikation mit dem Service für die Warnmeldungsindexierung über das native Protokoll verwendet.

Netzwerkports

Stellen Sie sicher, dass folgende Ports in der Firewall geöffnet sind, damit Sentinel ordnungsgemäß funktioniert:

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 5432	Eingehend	Optional. Standardmäßig überwacht dieser Port nur die Loopback-Schnittstelle.	Wird für die PostgreSQL-Datenbank verwendet. Dieser Port muss standardmäßig nicht geöffnet werden. Sie müssen diesen Port jedoch öffnen, wenn Sie Berichte mit dem Sentinel-SDK entwickeln. Weitere Informationen finden Sie im Abschnitt Sentinel-Plugin-SDK.
TCP 1099 und 2000	Eingehend	Erforderlich	Werden gemeinsam von Überwachungswerkzeugen verwendet, um mit Java Management Extensions (JMX) eine Verbindung zum Sentinel-Serverprozess herzustellen.
TCP 1289	Eingehend	Optional	Wird für Audit-Verbindungen verwendet.
UDP 1514	Eingehend	Optional	Wird für Syslog-Meldungen verwendet.
TCP 8443	Eingehend	Erforderlich	Wird für die HTTPS-Kommunikation verwendet.
TCP 1443	Eingehend	Optional	Wird für SSL-verschlüsselte Syslog-Meldungen verwendet.
TCP 61616	Eingehend	Optional	Wird für eingehende Verbindungen von den Collector Manager-Instanzen und den Correlation Engine-Instanzen verwendet.
TCP 10013	Eingehend	Erforderlich	Wird von Sentinel Control Center und Solution Designer verwendet.
TCP 1468	Eingehend	Optional	Wird für Syslog-Meldungen verwendet.
TCP 10014	Eingehend	Optional	Wird von den Remote-Instanzen von Collector Manager verwendet, um über den SSL-Proxy eine Verbindung zum Server herzustellen. Dies ist jedoch ungewöhnlich. Standardmäßig verwenden die Remote-Instanzen von Collector Manager für die Verbindung zum Server den SSL-Port 61616.
TCP 443	Ausgehend	Optional	Wenn Advisor verwendet wird, initiiert der Port über das Internet eine Verbindung zum Advisor-Service der Advisor-Aktualisierungsseite.
TCP 8443	Ausgehend	Optional	Wenn die Datenverbundfunktion verwendet wird, initiiert der Port eine Verbindung zu anderen Sentinel-Systemen, um die verteilte Suche durchzuführen.
TCP 389 oder 636	Ausgehend	Optional	Wenn die LDAP-Authentifizierung verwendet wird, initiiert der Port eine Verbindung zum LDAP-Server.
TCP/UDP 111 und TCP/UDP 2049	Ausgehend	Optional	Wenn der Sekundärspeicher zur Verwendung von NFS konfiguriert ist.
TCP 137, 138, 139, 445	Ausgehend	Optional	Wenn der Sekundärspeicher zur Verwendung von CIFS konfiguriert ist.
TCP JDBC (abhängig von der Datenbank)	Ausgehend	Optional	Wenn die Datensynchronisierung verwendet wird, initiiert der Port über JDBC eine Verbindung zur Zieldatenbank. Der verwendete Port hängt von der Zieldatenbank ab.
TCP 25	Ausgehend	Optional	Initiiert eine Verbindung zum Email-Server.

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 1290	Ausgehend	Optional	Wenn Sentinel Ereignisse an ein anderes Sentinel-System weiterleitet, initiiert dieser Port eine Sentinel-Link-Verbindung zu diesem System.
UDP 162	Ausgehend	Optional	Wenn Sentinel Ereignisse an das System weiterleitet, das SNMP-Traps empfängt, sendet der Port ein Paket an den Empfänger.
UDP 514 oder TCP 1468	Ausgehend	Optional	Dieser Port wird verwendet, wenn Sentinel Ereignisse an das System weiterleitet, das Syslog-Nachrichten empfängt. Wenn der Port ein UDP-Port ist, sendet er ein Paket an den Empfänger. Wenn der Port ein TCP-Port ist, initiiert er eine Verbindung zum Empfänger.
TCP 9443	Eingehend	Optional	Über diesen Port kann ein Sentinel-System Ereignisse von anderen SIEMsoftware-Produkten wie Change Guardian oder Secure Configuration Manager empfangen.

Spezifische Ports für Sentinel Server Appliance

Zusätzlich zu den oben genannten Ports sind die folgenden Ports für Appliances geöffnet.

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 22	Eingehend	Erforderlich	Wird für sicheren Shell-Zugriff auf Sentinel Appliance verwendet.
TCP 4984	Eingehend	Erforderlich	Wird außerdem von Sentinel Appliance für den Aktualisierungsservice verwendet.
TCP 289	Eingehend	Optional	Wird für Audit-Verbindungen an 1289 weitergeleitet.
TCP 443	Eingehend	Optional	Wird für die HTTPS-Kommunikation an 8443 weitergeleitet.
UDP 514	Eingehend	Optional	Wird für Syslog-Meldungen an 1514 weitergeleitet.
TCP 1290	Eingehend	Optional	Sentinel Link-Port, der eine Verbindung über die SuSE-Firewall herstellen darf.
UDP und TCP 40000–41000	Eingehend	Optional	Ports, die bei der Konfiguration von Datenerfassungsservern verwendet werden können, beispielsweise eines Syslog-Servers. Standardmäßig überwacht Sentinel diese Ports nicht.
TCP 443 oder 80	Ausgehend	Erforderlich	Initiiert eine Verbindung zum Repository für Appliance-Software-Aktualisierungen im Internet oder zu einem Dienst für Abonnementverwaltungswerkzeuge in Ihrem Netzwerk.
TCP 80	Ausgehend	Optional	Initiiert eine Verbindung zum Abonnementverwaltungswerkzeug.
TCP 7630	Eingehend	Erforderlich	Wird von High Availability Web Konsole (Hawk) verwendet.

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 9443	Eingehend	Erforderlich	Wird von der Verwaltungskonsole von Sentinel Appliance verwendet.
TCP 1098 und 2000	Eingehend	Erforderlich	Werden gemeinsam von Überwachungswerkzeugen verwendet, um mit Java Management Extensions (JMX) eine Verbindung zum Sentinel-Serverprozess herzustellen.

Collector Manager-Ports

Collector Manager verwendet die folgenden Ports für die Kommunikation mit anderen Komponenten.

Netzwerkports

Damit der Sentinel-Collector Manager ordnungsgemäß funktioniert, stellen Sie sicher, dass folgende Ports in der Firewall geöffnet sind:

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 1289	Eingehend	Optional	Wird für Audit-Verbindungen verwendet.
UDP 1514	Eingehend	Optional	Wird für Syslog-Meldungen verwendet.
TCP 1443	Eingehend	Optional	Wird für SSL-verschlüsselte Syslog-Meldungen verwendet.
TCP 1468	Eingehend	Optional	Wird für Syslog-Meldungen verwendet.
TCP 1099 und 2000	Eingehend	Erforderlich	Werden gemeinsam von Überwachungswerkzeugen verwendet, um mit Java Management Extensions (JMX) eine Verbindung zum Sentinel-Serverprozess herzustellen.
TCP 61616	Ausgehend	Erforderlich	Initiiert eine Verbindung zum Sentinel-Server.
TCP 8443	Ausgehend	Erforderlich	Initiiert eine Verbindung zum Sentinel-Webserverport. Lassen Sie diesen Port bei der Installation und Konfiguration von Collector Manager offen.

Spezifische Ports für Collector Manager Appliance

Zusätzlich zu den oben genannten Ports sind auf Sentinel Collector Manager Appliance auch die folgenden Ports geöffnet.

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 22	Eingehend	Erforderlich	Wird für sicheren Shell-Zugriff auf Sentinel Appliance verwendet.
TCP 4984	Eingehend	Erforderlich	Wird außerdem von Sentinel Appliance für den Aktualisierungsservice verwendet.
TCP 289	Eingehend	Optional	Wird für Audit-Verbindungen an 1289 weitergeleitet.
UDP 514	Eingehend	Optional	Wird für Syslog-Meldungen an 1514 weitergeleitet.
TCP 1290	Eingehend	Optional	Dies ist der Sentinel Link-Port, der eine Verbindung über die SuSE-Firewall erstellen darf.
UDP und TCP 40000–41000	Eingehend	Optional	Wird zur Konfiguration von Datenerfassungsservern wie z. B. syslog verwendet. Standardmäßig überwacht Sentinel diese Ports nicht.
TCP 443	Ausgehend	Erforderlich	Initiiert eine Verbindung zum Repository für Appliance-Software-Aktualisierungen im Internet oder zu einem Dienst für Abonnementverwaltungswerkzeuge in Ihrem Netzwerk.
TCP 80	Ausgehend	Optional	Initiiert eine Verbindung zum Abonnementverwaltungswerkzeug.
TCP 9443	Eingehend	Erforderlich	Wird von der Verwaltungskonsole von Sentinel Appliance verwendet.
TCP 1098 und 2000	Eingehend	Erforderlich	Werden gemeinsam von Überwachungswerkzeugen verwendet, um mit Java Management Extensions (JMX) eine Verbindung zum Sentinel-Serverprozess herzustellen.

Correlation Engine-Ports

Die Correlation Engine verwendet die folgenden Ports für die Kommunikation mit anderen Komponenten.

Netzwerkports

Damit die Sentinel-Correlation Engine ordnungsgemäß funktioniert, stellen Sie sicher, dass folgende Ports in der Firewall geöffnet sind:

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 1099 und 2000	Eingehend	Erforderlich	Werden gemeinsam von Überwachungswerkzeugen verwendet, um mit Java Management Extensions (JMX) eine Verbindung zum Sentinel-Serverprozess herzustellen.
TCP 61616	Ausgehend	Erforderlich	Initiiert eine Verbindung zum Sentinel-Server.

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 8443	Ausgehend	Erforderlich	Initiiert eine Verbindung zum Sentinel-Webserverport. Lassen Sie diesen Port bei der Installation und Konfiguration von Correlation Engine offen.

Spezifische Ports für Correlation Engine Appliance

Zusätzlich zu den oben genannten Ports sind auf Sentinel Correlation Engine Appliance auch die folgenden Ports geöffnet.

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 22	Eingehend	Erforderlich	Wird für sicheren Shell-Zugriff auf Sentinel Appliance verwendet.
TCP 4984	Eingehend	Erforderlich	Wird außerdem von Sentinel Appliance für den Aktualisierungsservice verwendet.
TCP 443	Ausgehend	Erforderlich	Initiiert eine Verbindung zum Repository für Appliance-Software-Aktualisierungen im Internet oder zu einem Dienst für Abonnementverwaltungswerkzeuge in Ihrem Netzwerk.
TCP 80	Ausgehend	Optional	Initiiert eine Verbindung zum Abonnementverwaltungswerkzeug.
TCP 9443	Eingehend	Erforderlich	Wird von der Verwaltungskonsole von Sentinel Appliance verwendet.
TCP 1098 und 2000	Eingehend	Erforderlich	Werden gemeinsam von Überwachungswerkzeugen verwendet, um mit Java Management Extensions (JMX) eine Verbindung zum Sentinel-Serverprozess herzustellen.

Ports für den skalierbaren Speicher

Damit SSDM mit CDH und Elasticsearch kommunizieren kann, müssen neben den für Cloudera erforderlichen Ports und den im Abschnitt Sentinel-Server-Ports aufgeführten Ports auch die Ports in der Firewall offen sein, die Sie bei der Konfiguration des skalierbaren Speichers festlegen.

9 Installationsoptionen

Sie können eine herkömmliche Installation von Sentinel durchführen oder die Appliance installieren. In diesem Kapitel finden Sie Informationen über die beiden Installationsoptionen.

Herkömmliche Installation

Bei der normalen Installation wird Sentinel mit dem Anwendungsinstallationsprogramm auf einem vorhandenen Betriebssystem installiert. Zur Installation von Sentinel können die folgenden Methoden angewendet werden:

- **Interaktiv:** Zum Fortführen der Installation sind Benutzereingaben erforderlich. Während der Installation können Sie die Installationsoptionen (Benutzereingaben oder Standardwerte) in einer Datei aufzeichnen, die später für die automatische Installation verwendet werden kann. Sie können entweder eine Standardinstallation durchführen oder eine benutzerdefinierte Installation.

Standardinstallation	Angepasste Installation
Verwendet die Standardwerte für die Konfiguration. Eine Benutzereingabe ist lediglich für das Passwort erforderlich.	Sie werden aufgefordert, die Werte für das Konfigurations-Setup anzugeben. Sie können die Standardwerte auswählen oder die gewünschten Werte angeben.
Verwendet den standardmäßigen Evaluierungsschlüssel.	Bietet die Möglichkeit, den standardmäßigen Evaluierungslizenzschlüssel oder einen gültigen Lizenzschlüssel zu verwenden.
Bietet die Möglichkeit, das Admin-Passwort anzugeben, und verwendet das Admin-Passwort als standardmäßiges Passwort für die Benutzer „dbauser“ und „appuser“.	Bietet die Möglichkeit, dass Admin-Passwort anzugeben. Für die Benutzer „dbauser“ und „appuser“ können Sie entweder ein neues Passwort angeben oder das Admin-Passwort verwenden.
Installiert für alle Komponenten die Standardports.	Bietet die Möglichkeit, für verschiedene Komponenten Ports anzugeben.
Installiert Sentinel im Nicht-FIPS-Modus.	Ermöglicht die Installation von Sentinel im FIPS 140-2-Modus.
Speichert Rohdaten und Ereignisse in herkömmlichem Speicher.	Bietet die Möglichkeit, Rohdaten und Ereignisse in skalierbarem Speicher abzulegen.
Authentifiziert die Benutzer mit der internen Datenbank.	Bietet die Option zur Einrichtung der LDAP-Authentifizierung für Sentinel zusätzlich zur Datenbankauthentifizierung. Wenn Sie Sentinel für die LDAP-Authentifizierung konfigurieren, können sich Benutzer mit ihren Novell eDirectory- oder Microsoft Active Directory-Anmeldedaten beim Server anmelden.

Weitere Informationen zur interaktiven Installation finden Sie unter „Durchführen der interaktiven Installation“, auf Seite 89.

- **Automatisch:** Wenn Sie mehrere Sentinel-Server in Ihrer Bereitstellung installieren möchten, können Sie die Installationsoptionen während der standardmäßigen oder benutzerdefinierten Installation in einer Konfigurationsdatei aufzeichnen und anhand dieser Datei eine automatische Installation ausführen. Weitere Informationen zur automatischen Installation finden Sie unter „Ausführen einer automatischen Installation“, auf Seite 95.

Appliance-Installation

Bei der Appliance-Installation werden sowohl SLES 12 SP3 (64 Bit) als Betriebssystem als auch Sentinel installiert.

Sentinel Appliance steht in den folgenden Formaten zur Verfügung:

- OVF-Appliance-Image
- ISO-Appliance-Image

Weitere Informationen zu Appliance-Installationen finden Sie in Kapitel 15, „Appliance-Installation“, auf Seite 99.

II Installieren von Sentinel

In diesem Abschnitt finden Sie Informationen zur Installation von Sentinel und den zusätzlichen Komponenten.

10 Installationsüberblick

Bei der standardmäßigen Sentinel-Installation werden die folgenden Komponenten im Sentinel-Server installiert:

- **Prozesse des Sentinel-Servers und -Webservers:** Der Sentinel-Server-Prozess verarbeitet Anforderungen von anderen Komponenten von Sentinel und ermöglicht die nahtlose Funktion des Systems. Der Sentinel-Server-Prozess verarbeitet Anforderungen wie das Filtern von Daten, die Verarbeitung von Suchanfragen und das Verwalten von Administrationsaufgaben einschließlich Benutzerauthentifizierung und -autorisierung.

  Der Sentinel-Webserver ermöglicht eine sichere Verbindung zur Benutzeroberfläche von Sentinel Main.
- **PostgreSQL-Datenbank:** In Sentinel ist eine Datenbank integriert, in der Sentinel-Konfigurationsinformationen, Bestands- und Schwachstellendaten, Identitätsinformationen, der Vorfalls- und Workflowstatus etc. gespeichert werden.
- **MongoDB-Datenbank:** Speichert die Sicherheitsintelligenz- und Warnmeldungsdaten.
- **Elasticsearch:** Indexiert Ereignisse und Warnmeldungen für die Suche und die Anzeige als Grafik.
- **Collector Manager:** Collector Manager stellt eine flexible Datenerfassungsstelle für Sentinel bereit. Das Sentinel-Installationsprogramm installiert während der Installation standardmäßig einen Collector Manager.
- **Elasticsearch:** Optionale Datenspeicherkomponente zum Speichern und Indexieren von Daten. Standardmäßig enthält Sentinel einen Elasticsearch-Knoten. Wenn Sie große EPS über 2.500 erwarten, stellen Sie zusätzliche Elasticsearch-Knoten in einem Cluster bereit.
- **Correlation Engine:** Die Correlation Engine verarbeitet Ereignisse aus dem Echtzeit-Ereignisstrom, um zu ermitteln, ob Korrelationsregeln ausgelöst werden sollen.
- **Advisor:** Advisor von Security Nexus ist ein optionaler Datenabonnement-Service, der eine Korrelation auf Geräteebene zwischen Echtzeitereignissen herstellt, die von der Eindringversuchserkennung und den Präventionssystemen sowie den Ergebnissen der unternehmensweiten Schwachstellenprüfung erfasst werden. Weitere Informationen zu Advisor finden Sie im Abschnitt „Detecting Vulnerabilities and Exploits“ (Erkennen von Schwachstellen und Exploits) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).
- **Sentinel-Plugins:** Sentinel unterstützt eine Reihe von Plugins zur Erweiterung und Optimierung der Systemfunktionalität. Einige dieser Plugins sind bereits vorinstalliert. Sie können weitere Plugins und Aktualisierungen von der Website für Sentinel-Plugins herunterladen. Sentinel-Plugins sind:
  - Collectors
  - Connectors
  - Korrelationsregeln und -aktionen
  - Berichte
  - iTRAC-Workflows
  - Lösungspakete

11 Installations-Checkliste

Vergewissern Sie sich vor Beginn der Installation, dass folgende Aufgaben abgeschlossen sind:

- ❒ Vergewissern Sie sich, dass die Hardware und Software die in Kapitel 5, „Erfüllen der Systemanforderungen“, auf Seite 37 aufgeführten Systemanforderungen erfüllt.
- ❒ Falls Sentinel bereits installiert war, stellen Sie sicher, dass von der vorherigen Installation keine Dateien oder Systemeinstellungen mehr vorhanden sind. Weitere Informationen finden Sie unter Anhang B, „Deinstallation“, auf Seite 233.
- ❒ Wenn Sie die lizenzierte Version installieren möchten, fordern Sie Ihren Lizenzschlüssel vom Kundenservicezentrum an.
- ❒ Vergewissern Sie sich, dass die in Kapitel 8, „Verwendete Ports“, auf Seite 61 aufgeführten Ports in der Firewall geöffnet sind.
- ❒ Damit das Sentinel-Installationsprogramm richtig funktioniert, muss das System den Hostnamen oder die gültige IP-Adresse zurückgeben können. Fügen Sie hierzu in der Datei `/etc/hosts` den Hostnamen zur Zeile mit der IP-Adresse hinzu. Geben Sie dann den Befehl `hostname -f` ein, um sicherzustellen, dass der Hostname ordnungsgemäß angezeigt wird.
- ❒ Synchronisieren Sie die Zeit mit NTP (Network Time Protocol).
- ❒ Wenn Sie Sentinel mit skalierbarem Speicher bereitstellen möchten, müssen Sie CDH und Elasticsearch installieren. Weitere Informationen zur Bereitstellung von Sentinel mit skalierbarem Speicher finden Sie unter „Installation und Einrichtung von skalierbarem Speicher“, auf Seite 85.
- ❒ **Auf RHEL-Systemen:** Um eine optimale Leistung zu ermöglichen, müssen die Speichereinstellungen für die PostgreSQL-Datenbank entsprechend festgelegt werden. Der SHMMAX-Parameter muss mindestens 1073741824 betragen.

  Um den geeigneten Wert festzulegen, fügen Sie in der Datei `/etc/sysctl.conf` folgende Informationen an:

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```

- ❒ **Für herkömmliche Installationen:**

  Das Betriebssystem für den Sentinel-Server muss mindestens die Basisserver-Komponenten des SLES- bzw. RHEL 6-Servers enthalten. Sentinel erfordert die 64-Bit-Versionen folgender RPMs:

  - bash
  - bc
  - coreutils
  - gettext
  - glibc
  - grep
  - libgcc
  - libstdc

- lsof
- net-tools
- openssl
- python-libs
- sed
- zlib

❒ **Für Sentinel mit herkömmlichem Speicher:**

Um Ereignisgrafiken anzuzeigen, legen Sie den virtuellen Arbeitsspeicher fest, indem Sie die Eigenschaft `vm.max_map_count=262144` in der Datei `/etc/sysctl.conf` hinzufügen.

12 Installation und Konfiguration von Elasticsearch

Wenn Sie Ereignisse skalierbar und verteilt indexieren möchten, müssen Sie Elasticsearch im Cluster-Modus installieren. Der für Sentinel installierte Elasticsearch-Cluster darf nur zur Indexierung von Sentinel-Daten verwendet werden.

Voraussetzungen

Vor der Installation von Elasticsearch müssen folgende Voraussetzungen erfüllt sein:

- Stellen Sie Elasticsearch je nach EPS-Rate in einem Clustermodus bereit. Befolgen Sie dabei die Empfehlungen auf der Seite Technical Information for Sentinel (Technische Informationen für Sentinel) in Bezug auf Anzahl der Knoten und Anzahl der Reproduktionen.
- Legen Sie die Dateideskriptoren fest, indem Sie in der Datei `/etc/security/limits.conf` die folgenden Eigenschaften hinzufügen:

  ```
  elasticsearch hard nofile 65536
  elasticsearch soft nofile 65536
  elasticsearch soft as unlimited
  ```

HINWEIS: Nachdem Sie die oben aufgeführten Voraussetzungen erfüllt haben, führen Sie den Befehl `sysctl -p` aus, um die an den Dateien vorgenommenen Änderungen neu zu laden.

Installation und Konfiguration von Elasticsearch

Installieren Sie Elasticsearch und die erforderlichen Plugins auf jedem Knoten des Elasticsearch-Clusters.

So installieren und konfigurieren Sie Elasticsearch:

1. Installieren Sie die von Elasticsearch unterstützte JDK-Version.
2. Laden Sie die zertifizierte Version des Elasticsearch-RPM-Pakets herunter. Weitere Informationen zur zertifizierten Version von Elasticsearch sowie die Download-URL finden Sie auf der Seite Technical Information for Sentinel (Technische Informationen für Sentinel).
3. Installieren Sie Elasticsearch:

   ```
   rpm -i elasticsearch-<Version>.rpm
   ```

4. Führen Sie die Aufgaben wie auf dem Bildschirm mit der RPM-Installations-Nachbereitungsliste angegeben aus.
5. Stellen Sie sicher, dass der Elasticsearch-Benutzer Zugriff auf Java hat.
6. Konfigurieren Sie die Datei `/etc/elasticsearch/elasticsearch.yml`, indem Sie die folgenden Informationen aktualisieren oder ergänzen:

Eigenschaft und Wert	Anmerkungen
cluster.name: <*Elasticsearch-Cluster-Name*>	Der von Ihnen gewählte Cluster-Name muss für alle Knoten derselbe sein.
node.name: <*Knotenname*>	Jeder Knoten muss einen eindeutigen Namen erhalten.
network.host: _<*Netzwerkschnittstelle*>:ipv4_	
discovery.zen.ping.unicast.hosts: [<FQDN des Elasticsearch-Knotens auf dem Sentinel-Server>,<*FQDN des Elasticsearch-Knotens1*>, <*FQDN des Elasticsearch-Knotens2*> usw.]	
thread_pool.bulk.queue_size: 300	
thread_pool.search.queue_size: 10000	Sobald die Suchwarteschlange den Grenzwert erreicht, verwirft Elasticsearch alle in der Warteschlange befindlichen ausstehenden Suchanforderungen. Mittels folgender Methode können Sie berechnen, um wie viel Sie die Suchwarteschlange eventuell verlängern müssen: threadpool.search.queue_size = durchschnittliche Anzahl an Widget-Anfoderungen pro Benutzer für ein Dashboard x Anzahl der Shards (Pro-Tag-Index) x Anzahl der Tage (Suchdauer)
index.codec: best_compression	
path.data: ["/<*es1*>", "/<*es2*>"]	Um die Datenträger-E/A-Latenz zu reduzieren, können Sie Daten auf mehrere voneinander unabhängige Datenträger oder Speicherorte verteilen. Konfigurieren Sie mehrere Pfade zum Speichern von Elasticsearch-Daten, z. B. /es1, /es2 und so weiter. Die besten Ergebnisse bezüglich Leistung und Verwaltbarkeit erhalten Sie, wenn Sie jeden Pfad einem separaten physischen Datenträger (JBOD) zuordnen.

7. Aktualisieren Sie die standardmäßige Heap-Größe für Elasticsearch in der Datei `/etc/elasticsearch/jvm.options`.

Die Heap-Größe muss 50 % des Server-Arbeitsspeichers betragen. Beispiel: In einem 24-GB-Elasticsearch-Knoten bedeutet dies, dass eine Heap-Größe von 12 GB optimale Leistung verspricht.

8 Wiederholen Sie jeden dieser Schritte auf jedem Knoten im Elasticsearch-Cluster.

9 Konfigurieren Sie im Elasticsearch-Knoten des Sentinel-Servers `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` wie folgt:

9a Stellen Sie sicher, dass die Werte von `cluster.name` und `discovery.zen.ping.unicast.hosts` in der Datei `elasticsearch.yml` mit den Werten in der Datei `elasticsearch.yml` im externen Elasticsearch-Knoten übereinstimmen.

9b Geben Sie die Localhost-IP-Adresse, gefolgt von der IP-Adresse des lokalen Elasticsearch-Knotens, wie folgt in der Eigenschaft `network.host` an:

```
network.host: ["127.0.0.1","<IP-Adresse des Elasticsearch-Knotens in Sentinel>"]
```

10 (Bedingt) Für Sentinel mit herkömmlichem Speicher fügen Sie die IP-Adressen der externen Elasticsearch-Knoten zur Eigenschaft `ServerList` in der Datei `/etc/opt/novell/sentinel/config/elasticsearch-index.properties` hinzu.

Beispiel: `ServerList=<Elasticsearch-IP1>:<Port>,<Elasticsearch-IP2>:<Port>`

11 Starten Sie Sentinel neu:

```
rcsentinel restart
```

12 Starten Sie jeden Elasticsearch-Knoten neu:

```
/etc/init.d/elasticsearch start
```

13 Konfigurieren Sie zum Erreichen einer optimalen Leistung und Stabilität des Sentinel-Servers den Elasticsearch-Knoten im Sentinel-Server als dedizierten `master-eligible`-Knoten, damit alle Ereignisgrafikdaten in externen Elasticsearch-Knoten indexiert werden:

13a Melden Sie sich beim Sentinel-Server als der Benutzer „novell“ an.

13b Stellen Sie sicher, dass die vorhandenen Warnmeldungsdaten zu externen Elasticsearch-Knoten verschoben wurden.

13c Öffnen Sie die Datei `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` und fügen Sie die folgenden Informationen hinzu:

```
node.master: true
node.data: false
node.ingest: false
search.remote.connect: false
```

13d Starten Sie Elasticsearch neu:

```
rcsentinel stopSIdb
```

```
rcsentinel startSIdb
```

14 Fahren Sie mit „Sichern von Daten in Elasticsearch“, auf Seite 77 fort.

Sichern von Daten in Elasticsearch

Auf Elasticsearch-Clusterknoten kann mit verschiedenen Clients zugegriffen werden, zum Beispiel:

- Sentinel: Abrufen und Präsentieren von Ereignisdaten im Ereignisgrafik-Dashboard.
- Spark-Aufträge, die in YARN NodeManager-Knoten ausgeführt werden: Massenindexierung der von Kafka empfangenen Ereignisse. (für SSDM)

- Collector Manager: Massenindexierung der Ereignisse in Sentinel mit herkömmlichem Speicher.
- Andere externe Clients: Ausführen benutzerdefinierter Vorgänge wie benutzerdefinierte Analysen.

Sentinel bietet ein Sicherheits-Plugin für Elasticsearch (**elasticsearch-security-plugin**), das den Zugriff auf Elasticsearch authentifiziert und autorisiert.

Das Plugin verwendet zur Validierung entweder ein SAML-Token oder eine weiße Liste, je nachdem, wie die Clients eine Verbindung herstellen:

- Wenn ein Client ein SAML-Token zusammen mit der Anforderung sendet, authentifiziert das Plugin das Token über den Sentinel-Authentifizierungsserver. Nach der erfolgreichen Authentifizierung erlaubt das Plugin den Zugriff nur auf die gefilterten Ereignisse, für die der Client autorisiert ist.

  Beispielsweise werden im Ereignisgrafik-Dashboard (Client) nur die Ereignisse von Elasticsearch angezeigt, für die der Benutzer mit seiner Rolle zum Anzeigen autorisiert ist.

  Informationen über Rollen und Berechtigungen finden Sie in „Creating a Role“ (Erstellen einer Rolle) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).
- Wenn ein Client kein SAML-Token senden kann, überprüft das Plugin seine weiße Liste berechtigter Clients. Nach der erfolgreichen Validierung erlaubt das Plugin ohne Filterung den Zugriff auf alle Ereignisse.
- Wenn ein Client kein gültiges SAML-Token sendet und nicht über die weiße Liste berechtigt ist, betrachtet das Plugin den Client als illegitim und verweigert dem Client den Zugriff.

Dieser Abschnitt enthält Informationen zur Installation und Konfiguration des Elasticsearch-Sicherheits-Plugins:

- „Installieren des Elasticsearch-Sicherheits-Plugins“, auf Seite 78
- „Sicheren Zugriff für zusätzliche Elasticsearch-Clients bereitstellen“, auf Seite 79
- „Elasticsearch-Plugin-Konfiguration aktualisieren“, auf Seite 80

Installieren des Elasticsearch-Sicherheits-Plugins

Sie müssen das Elasticsearch-Sicherheits-Plugin in jedem Knoten des Elasticsearch-Clusters und auch in dem in Sentinel enthaltenen Elasticsearch-Knoten installieren.

So installieren Sie das Elasticsearch-Sicherheits-Plugin im Elasticsearch-Knoten, der in Sentinel enthalten ist:

1. Melden Sie sich am Sentinel Main- oder am SSDM-Server an.
2. Legen Sie den Pfad für die JAVA_HOME-Umgebungsvariable wie folgt fest:

   ```
   export JAVA_HOME=/<Sentinel_installation_path>/opt/novell/sentinel/jdk/
   ```

3. Installieren Sie das Plugin:

   Unter Linux melden Sie sich als der Benutzer an, mit dem Elasticsearch ausgeführt wird, und führen Sie den folgenden Befehl aus:

   ```
   <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/
   elasticsearch-plugin install file://localhost/<Sentinel_installation_path>/
   etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip --
   verbose
   ```

   Wenn Sie zum Fortsetzen der Installation aufgefordert werden, geben Sie `j` ein.

4 (Bedingt) Wenn Elasticsearch nicht den standardmäßigen HTTP-Port (9200) überwacht, aktualisieren Sie die Elasticsearch-Portnummer in jedem Eintrag der Datei `<Sentinel_Installationspfad>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt`.

   Weitere Informationen finden Sie unter „Zugriff für Elasticsearch-Clients über die weiße Liste“, auf Seite 80.

5 Starten Sie mit folgendem Befehl die Indexierungsservices in Sentinel neu:

```
rcsentinel stopSIdb
rcsentinel startSIdb
```

So installieren Sie das Elasticsearch-Sicherheits-Plugin auf externen Elasticsearch-Knoten:

Führen Sie die folgenden Schritte auf jedem Knoten im Elasticsearch-Cluster aus:

1 Melden Sie sich am Sentinel Main- oder am SSDM-Server an.

2 Kopieren Sie die Datei `<Sentinel_Installationspfad>/etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip` an einen temporären Speicherort auf jedem Knoten im Elasticsearch-Cluster.

3 Installieren Sie das Plugin:

   Unter Linux melden Sie sich als der Benutzer an, mit dem Elasticsearch ausgeführt wird, und führen Sie den folgenden Befehl aus:

```
<elasticsearch_install_directory>/bin/elasticsearch-plugin install file://
localhost/<full path of elasticsearch-security-plugin*.zip file> --verbose
```

   Wenn Sie zum Fortsetzen der Installation aufgefordert werden, geben Sie `j` ein.

4 (Bedingt) Wenn Elasticsearch nicht den standardmäßigen HTTP-Port (9200) überwacht, aktualisieren Sie die Elasticsearch-Portnummer in jedem Eintrag der Datei `<Elasticsearch_Installationspfad>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt`.

   Weitere Informationen finden Sie unter „Zugriff für Elasticsearch-Clients über die weiße Liste“, auf Seite 80.

5 Starten Sie Elasticsearch neu.

Sicheren Zugriff für zusätzliche Elasticsearch-Clients bereitstellen

Verbürgte Clients wie der SSDM-Server (für das Ereignisgrafik-Dashboard) und YARN NodeManager-Instanzen, der Sentinel-Server (für das Ereignisgrafik-Dashboard) und RCM haben standardmäßig Zugriff auf Elasticsearch. Wenn Sie zusätzliche Elasticsearch-Clients verwenden möchten, müssen Sie für diese Clients entweder mit einem SAML-Token oder mit einer weißen Liste einen sicheren Zugriff bereitstellen.

Zugriff für Elasticsearch-REST-Clients mit SAML-Token

Wenn Sie zum Zugriff auf Elasticsearch einen REST-Client verwenden, können Sie im Anforderungsheader wie folgt ein SAML-Token einschließen:

1 Rufen Sie vom Sentinel-Authentifizierungsserver ein SAML-Token ab. Weitere Informationen hierzu finden Sie in der REST-API-Dokumentation in Sentinel.

Klicken Sie auf **Hilfe** > **APIs > Tutorial > API-Sicherheit > SAML-Token (Anmeldung) abrufen**.

2. Verwenden Sie das SAML-Token in den nachfolgenden REST-Anforderungen: Schließen Sie das SAML-Token in den Authentifizierungsheader jeder Anforderung des REST-Clients ein. Geben Sie den Headernamen als `Authorization` und den Headerwert als das in Schritt 1 erhaltene <*SAML-Token*> an.

Zugriff für Elasticsearch-Clients über die weiße Liste

Standardmäßig füllt Sentinel automatische eine weiße Liste mit den IP-Adressen verbürgter Elasticsearch-Clients aus, wie SSDM-Server (für das Ereignisgrafik-Dashboard) und YARN NodeManager-Instanzen, Sentinel-Server (für das Ereignisgrafik-Dashboard) und RCM. Das Elasticsearch-Sicherheits-Plugin gewährt allen Clients, die in der weißen Liste aufgeführt sind, Zugriff auf Elasticsearch.

Um zusätzlichen Clients, die kein gültiges Sentinel-Token senden, Zugriff zu gewähren, fügen Sie die IP-Adresse des Clients und die HTTP-Portnummer des Elasticsearch-Servers im Format `IP-Adresse:Port` zur weißen Liste hinzu. Um unberechtigten Zugriff zu vermeiden, müssen Sie sicherstellen, dass die externen Clients, die Sie zur weißen Liste hinzufügen, legitim und vertrauenswürdig sind.

So aktualisieren Sie die weiße Liste:

1. Melden Sie sich am Sentinel-Server oder am Elasticsearch-Knoten als der Benutzer an, mit dem Elasticsearch ausgeführt wird.
2. Fügen Sie den Eintrag <Elasticsearch_Client_IP>:<Ziel_Elasticsearch_HTTP_Port> zur folgenden Datei hinzu:
   - `<sentinel_Installationspfad>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin//elasticsearch-ip-whitelist.txt` für den in Sentinel enthaltenen Elasticsearch-Knoten
   - `<elasticsearch_Installationsverzeichnis>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt` für externe Elasticsearch-Knoten

   Bei mehreren Einträgen fügen Sie jeden Eintrag in einer neuen Zeile ein und speichern Sie die Datei.
3. Wiederholen Sie die oben aufgeführten Schritte auf jedem Knoten im Elasticsearch-Cluster.

Elasticsearch-Plugin-Konfiguration aktualisieren

Falls Sie die IP-Adresse/den Hostnamen und die Portnummer der skalierbaren Speicherkomponente oder die Elasticsearch-Version und Portnummer ändern, müssen Sie die Elasticsearch-Plugin-Konfigurationsdateien entsprechend aktualisieren.

Führen Sie die folgenden Schritte auf jedem Knoten im Elasticsearch-Cluster aus:

1. Melden Sie sich am Elasticsearch-Knoten mit dem Benutzer an, mit dem Elasticsearch ausgeführt wird.
2. (Bedingt) Wenn Sie die YARN NodeManager-IP-Adressen, die SSDM- oder Sentinel-Server-IP-Adressen, die RCM-IP-Adressen oder die Elasticsearch-Portnummer geändert haben, aktualisieren Sie die weiße Liste entsprechend, um sicherzustellen, dass das Elasticsearch-Sicherheits-Plugin den Elasticsearch-Clients Zugriff gewährt.

   Wenn Sie SSDM oder Sentinel im Hochverfügbarkeitsmodus konfigurieren, fügen Sie Einträge für die physische IP-Adresse jedes aktiven Knotens und passiven Knotens des Hochverfügbarkeits-Clusters hinzu.

Wenn Sie die physische IP-Adresse eines beliebigen Knotens im Hochverfügbarkeits-Cluster ändern oder einen neuen Knoten zum Hochverfügbarkeits-Cluster hinzufügen, aktualisieren Sie die weiße Liste mit den physischen IP-Adressen der geänderten bzw. neu hinzugefügten Knoten.

Weitere Informationen finden Sie unter „Zugriff für Elasticsearch-Clients über die weiße Liste“, auf Seite 80.

3 (Bedingt) Wenn Sie die SSDM-IP-Adresse, die Sentinel-Server-IP-Adresse oder die Webserver-Portnummer geändert haben, aktualisieren Sie die Eigenschaften `authServer.host` und `authServer.port` in den folgenden Dateien und starten Sie Elasticsearch neu:

- `<Sentinel_Installationspfad>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-configuration.properties` für den in Sentinel enthaltenen Elasticsearch-Knoten
- `<Elasticsearch_Installationsverzeichnis>/plugins/elasticsearch-security-plugin/plugin-configuration.properties` für externe Elasticsearch-Knoten

Wenn Sie SSDM oder Sentinel im Hochverfügbarkeitsmodus konfigurieren, legen Sie die Eigenschaft `authServer.host` auf die virtuelle IP-Adresse des Hochverfügbarkeits-Clusters fest.

Wenn Sie die virtuelle IP-Adresse des Hochverfügbarkeits-Clusters ändern, aktualisieren Sie die Eigenschaft `authServer.host` auf die geänderte virtuelle IP-Adresse.

4 (Bedingt) Wenn Sie Elasticsearch auf eine neuere Version aufgerüstet haben, aktualisieren Sie die Eigenschaft `elasticsearch.version` in den folgenden Dateien und starten Sie Elasticsearch neu:

- `/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` für den in Sentinel enthaltenen Elasticsearch-Knoten
- `<Elasticsearch_Installationsverzeichnis>/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` für externe Elasticsearch-Knoten

Leistungsoptimierung für Elasticsearch

Sentinel konfiguriert die in der Tabelle unten beschriebenen Elasticsearch-Einstellungen automatisch. Sie können die Elasticsearch-Einstellungen je nach Bedarf anpassen.

So ändern Sie die Standardeinstellungen:

Herkömmlicher Speicher: Öffnen Sie die Datei `/etc/opt/novell/sentinel/config/elasticsearch-index.properties` und aktualisieren Sie die in der Tabelle aufgeführten Eigenschaften je nach Bedarf.

Skalierbarer Speicher: Klicken Sie auf der SSDM-Startseite auf **Speicher** > **Skalierbarer Speicher** > **Erweiterte Eigenschaften** > **Elasticsearch**.

Tabelle 12-1 *Elasticsearch-Eigenschaften*

Eigenschaft	Standardwert	Anmerkungen
elasticsearch.events.lucenefilter (optional)		Legen Sie einen Filter fest, um nur bestimmte Ereignisse zur Indexierung an Elasticsearch zu senden. Beispiel: Wenn Sie den Wert als sev:[3-5] festlegen, werden nur Ereignisse mit einem Schweregradswert zwischen 3 und 5 zu Elasticsearch gesendet.
index.fields	id,dt,rv171,msg,ei,evt,xdastaxname,xdasoutcomename,sev,vul,rv32,rv39,rv159,dhn,dip,rv98,dp,fn,rv199,dun,tufname,rv84,rv158,shn,sip,rv76,sun,iufname,sp,iudep,rv198,rv62,st,tid,srcgeo,destgeo,obsgeo,rv145,estz,estzmonth,estzdiy,estzdim,estzdiw,estzhour,estzmin,rv24,tudep,pn,xdasclass,xdasid,xdasreg,xdasprov,iuident,tuident	Gibt die Ereignisfelder an, die Elasticsearch indexieren soll.
es.num.shards	5	Gibt die Anzahl der primären Shards pro Index an. Sie können diesen Standardwert erhöhen, wenn die Shard-Größe 50 GB überschreitet.
es.num.replicas	1	Gibt die Anzahl der Reproduktions-Shards an, die jeder primäre Shard haben sollte. Zur Berücksichtigung von Failover und Hochverfügbarkeit werden mindestens Zwei-Knoten-Cluster empfohlen.

Elasticsearch-Sicherheits-Plugin neu bereitstellen

In den folgenden Szenarien muss das Elasticsearch-Sicherheits-Plugin neu bereitgestellt, d. h. im in Sentinel enthaltenen Elasticsearch-Knoten und in externen Elasticsearch-Knoten deinstalliert und neu installiert, werden:

- Hinzufügen oder Ändern der Remote-Collector Manager-IP-Adressen.
- Deinstallieren von Remote-Collector Manager-Instanzen.
- Aktivieren des skalierbaren Speichers nach der Installation.

So stellen Sie das Elasticsearch-Sicherheits-Plugin neu bereit:

1. Melden Sie sich am Sentinel-Server oder am Elasticsearch-Knoten als der Benutzer an, mit dem Elasticsearch ausgeführt wird.
2. Deinstallieren Sie das Plugin mit dem folgenden Befehl:
   - Für Elasticsearch in Sentinel: `<Sentinel_Installationspfad>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin remove file://localhost/<Sentinel_Installationspfad>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
   - Für externe Elasticsearch-Knoten: `<Elasticsearch_Installationsverzeichnis> remove file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
3. Installieren Sie das Plugin neu:
   - Für Elasticsearch in Sentinel: `<Sentinel_Installationspfad>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin install file://localhost/<Sentinel_Installationspfad>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
   - Für externe Elasticsearch-Knoten: `<Elasticsearch_Installationsverzeichnis>/bin/elasticsearch-plugin install file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
4. Starten Sie Elasticsearch mit dem folgenden Befehl neu:
   - Für den in Sentinel enthaltenen Elasticsearch-Knoten:

     ```
     rcsentinel stopSIdb
     rcsentinel startSIdb
     ```

   - Für externe Elasticsearch-Knoten:

     ```
     sudo systemctl restart elasticsearch.service
     ```

13 Installation und Einrichtung von skalierbarem Speicher

In der folgenden Tabelle finden Sie die Voraussetzungen, die erfüllt sein müssen, um skalierbaren Speicher als Datenspeicheroption für Sentinel einzurichten:

Tabelle 13-1 *Voraussetzungen für die Aktivierung skalierbaren Speichers*

❒	Aufgaben	Erklärt in
❒	Bestimmen Sie anhand der EPS-Rate und der Anzahl der benötigten Reproduktionen die Anzahl der zu konfigurierenden Clusterknoten für die Hadoop-Distribution und Elasticsearch. Bestimmen Sie die zertifizierte Version von CDH und Elasticsearch.	Technical Information for Sentinel (Technische Informationen für Sentinel).
❒	Für CDH, Elasticsearch und Sentinel gibt es jeweils eine eigene Übersicht für den Plattform-Support. Diese Übersichten helfen Ihnen, die für Sie geeignete Plattform auszuwählen. Für Elasticsearch wird die RPM-Installation empfohlen, weil das RPM das Init-Skript enthält. So wird Elasticsearch als Service installiert und festgelegt, dass dieser bei Reboots und Aufrüstungen automatisch stoppt und startet, die Konfigurationsdateien aber nicht überschreibt. SLES 11 unterstützt die RPM-Installation von Elasticsearch nicht. Wählen Sie daher eine geeignete Plattform für Elasticsearch aus.	Support-Übersicht für CDH in der Cloudera-Dokumentation. Support-Übersicht für Elasticsearch in der Elasticsearch-Dokumenation. Support-Übersicht für Sentinel.
❒	Installieren und konfigurieren Sie CDH im Cluster-Modus.	„Installation und Konfiguration von CDH“, auf Seite 86.
❒	Installieren und konfigurieren Sie Elasticsearch im Cluster-Modus.	„Installation und Konfiguration von Elasticsearch“, auf Seite 75.
❒	Aktivieren Sie in Sentinel den skalierbaren Speicher.	„Aktivierung des skalierbaren Speichers“, auf Seite 88

Installation und Konfiguration von CDH

In diesem Abschnitt werden die speziellen Sentinel-Einstellungen für die Installation und Konfiguration von CDH erläutert. Ausführliche Informationen zur Installation und Konfiguration von CDH finden Sie in der zertifizierten Version der Cloudera-Dokumentation.

Sentinel ist mit Cloudera Express, der kostenlosen CDH-Version, kompatibel. Das ebenfalls kompatible Cloudera Enterprise enthält zahlreiche Funktionen, die in Cloudera Express nicht verfügbar sind, allerdings erfordert es den Kauf einer entsprechenden Lizenz. Wenn Sie bei der Arbeit mit Cloudera Express feststellen, dass Sie auf die Funktionen von Cloudera Enterprise nicht verzichten möchten, können Sie mit dem Erwerb einer entsprechenden Cloudera-Lizenz das Cluster aufrüsten.

Voraussetzungen

Vor der Installation von CDH müssen Sie die Hosts nach den folgenden Vorgaben einrichten:

- Erfüllen Sie alle Bedingungen, die in der Cloudera-Dokumentation aufgeführt sind.
- Nutzen Sie das ext4- oder XFS-Dateisystem zur Leistungssteigerung.
- CDH erfordert einige Betriebssystempakete, die nicht standardmäßig installiert werden. Legen Sie daher die entsprechende Betriebssystem-DVD ein. In der Cloudera-Installationsanleitung finden Sie Informationen zu den Paketen, die zu installieren sind.
- CDH erfordert für SLES-Betriebssysteme das Paket `python-psycopg2`. Installieren Sie das Paket `python-psycopg2`. Weitere Informationen finden Sie in der openSUSE-Dokumentation.
- Sollten Sie virtuelle Maschinen nutzen, reservieren Sie im Dateisystem den nötigen Speicherplatz, wenn Sie VM-Knoten erstellen. Im Fall von VMware können Sie beispielweise Thick Provisioning wählen.
- Stellen Sie sicher, dass Sentinel und die CDH-Clusterknoten in der gleichen Zeitzone liegen.
- Legen Sie den „Swappiness“-Parameter aller Hosts in der Datei `/etc/sysctl.conf` mit „1“ fest. Machen Sie dazu den folgenden Eintrag:

  ```
  vm.swappiness=1
  ```

  Führen Sie dann diesen Befehl aus, um die Einstellung umgehend anzuwenden:

  ```
  sysctl -p
  ```

- Die JDK-Version in CDH muss dieselbe JDK-Version (oder höher) sein, die in Sentinel verwendet wird. Wenn die in CDH verfügbare JDK-Version älter ist als die in Sentinel, installieren Sie das JDK gemäß der Anleitung manuell, aber nicht das JDK, das im CDH-Repository verfügbar ist.

  Installieren Sie das JDK mithilfe der Archiv-Binärdatei (`.tar.gz`), denn wenn Sie es per RPM installieren, kann dies Probleme verursachen, wenn Sie versuchen, Spark-Jobs unter YARN mithilfe des Skripts `manage_spark_jobs.sh` abzusenden.

  Die in Sentinel verwendete JDK-Version finden Sie in den Versionshinweisen zu Sentinel.

Installation und Konfiguration von CDH

Installieren Sie die zertifizierte Version von CDH. Weitere Informationen zur zertifizierten CDH-Version finden Sie auf der Seite Technical Information for Sentinel (Technische Informationen für Sentinel). Eine Installationsanleitung finden Sie in der zertifizierten Version der Cloudera-Dokumentation.

Achten Sie bei der CDH-Installation auf Folgendes:

- (Bedingt) Wenn die Installation während der Installation der eingebetteten PostgreSQL-Datenbank fehlschlägt, führen Sie die folgenden Schritte aus:

  ```
  mkdir -p /var/run/postgresql
  ```

  ```
  sudo chown cloudera-scm:cloudera-scm /var/run/postgresql
  ```

- Aktivieren Sie bei der Auswahl des Software-Installationstyps im Fenster **Select Repository** (Repository auswählen) die Optionen **Use Parcels** (Pakete verwenden) und „Kafka“ in **Additional Parcels** (Weitere Pakete).
- Aktivieren Sie beim Hinzufügen von Services die folgenden:
  - Cloudera Manager
  - ZooKeeper
  - HDFS
  - HBase
  - YARN
  - Spark
  - Kafka

  HINWEIS: Installieren Sie Spark History Server und HDFS NameNode in demselben Knoten, um die Systemstabilität zu gewährleisten. Informationen zur Architektur des skalierbaren Speichers finden Sie in „Planen des skalierbaren Speichers“, auf Seite 44.

  Beim Aktivieren der oben genannten Services muss für folgende Elemente Hochverfügbarkeit konfiguriert werden:
  - HBase HMaster
  - HDFS NameNode
  - YARN ResourceManager
- (Bedingt) Wenn das Installationsprogramm die Client-Konfiguration wegen eines fehlenden Java-Pfads nicht bereitstellt, starten Sie eine neue Browsersitzung und aktualisieren Sie den Java-Pfad manuell wie folgt:

  Klicken Sie auf **Hosts** > **All Hosts** > **Configuration** (Host > Alle Hosts > Konfiguration) und geben Sie im Feld **Java Home Directory** (Java-Basisverzeichnis) den korrekten Pfad an.

Aktivierung des skalierbaren Speichers

Sie können den skalierbaren Speicher sowohl während als auch nach der Installation von Sentinel aktivieren. Bei der Aktivierung des skalierbaren Speichers während der Installation konfiguriert Sentinel CDH-Komponenten mit Standardwerten. Einige dieser Konfigurationen sind permanent, d. h., sie können nicht geändert werden. So ist zum Beispiel unveränderlich, dass für Kafka-Themen standardmäßig 9 Partitionen zur Verfügung stehen.

Um die Standardwerte zu ändern, müssen Sie nach der Installation von Sentinel den skalierbaren Speicher aktivieren und dann die gewünschten Einstellungen für CDH-Komponenten vornehmen.

Bei herkömmlichen Installationen lässt sich der skalierbare Speicher entweder während oder nach der Sentinel-Installation aktivieren. Bei Appliance-Installationen lässt sich der skalierbare Speicher nur nach der Installation aktivieren.

In Aufrüstungsinstallationen können Sie den skalierbaren Speicher erst nach der Aufrüstung von Sentinel aktivieren.

Bevor Sie mit der Aktivierung des skalierbaren Speichers beginnen, halten Sie die Liste der IP-Adressen bzw. Hostnamen und Portnummern für Kafka-, HDFS NameNode-, YARN NodeManager-, ZooKeeper- und Elasticsearch-Knoten griffbereit. Sie benötigen diese Informationen für den Aktivierungsvorgang.

Eine Anleitung zur Aktivierung des skalierbaren Speichers während der Sentinel-Installation finden Sie im Abschnitt „Angepasste Sentinel-Serverinstallation“, auf Seite 90.

Eine Anleitung zur Aktivierung des skalierbaren Speichers nach der Sentinel-Installation oder -Aufrüstung finden Sie im Abschnitt „Enabling Scalable Storage Post-Installation“ (Aktivierung des skalierbaren Speichers nach der Installation) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

14 Herkömmliche Installation

In diesem Kapitel finden Sie Informationen über die verschiedenen Methoden zur Installation von Sentinel.

Durchführen der interaktiven Installation

In diesem Abschnitt finden Sie Informationen über die Standardinstallation und die benutzerdefinierte Installation.

Standardmäßige Sentinel-Serverinstallation

Gehen Sie folgendermaßen vor, um eine Standardinstallation durchzuführen:

1. Laden Sie die Installationsdatei von der Downloads-Website herunter.
2. Geben Sie in der Befehlszeile den folgenden Befehl ein, um die Installationsdatei zu extrahieren.

   ```
   tar zxvf <install_filename>
   ```

   Ersetzen Sie *<install_filename>* durch den tatsächlichen Namen der Installationsdatei.
3. Wechseln Sie in das Verzeichnis, in das Sie das Installationsprogramm extrahiert haben:

   ```
   cd <directory_name>
   ```

4. Geben Sie folgenden Befehl ein, um Sentinel zu installieren:

   ```
   ./install-sentinel
   ```

   Alternativ:

   Wenn Sie Sentinel auf mehr als einem Server installieren möchten, können Sie die Installationsoptionen in einer Datei aufzeichnen. Diese Datei können Sie für die unbeaufsichtigte Installation von Sentinel auf anderen Systemen verwenden. Geben Sie zum Aufzeichnen Ihrer Installationsoptionen den folgenden Befehl an:

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

5. Geben Sie die entsprechende Zahl für die Sprache an, die für die Installation verwendet werden soll. Drücken Sie dann die Eingabetaste.

   Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.
6. Drücken Sie die Leertaste, um die Lizenzvereinbarung durchzulesen.

7 Geben Sie `yes` (ja) bzw. `y` ein, um die Lizenz zu akzeptieren und mit der Installation fortzufahren.

   Das Laden der Installationspakete kann einige Sekunden in Anspruch nehmen. Anschließend werden Sie zur Eingabe des Konfigurationstyps aufgefordert.

8 Geben Sie bei der Eingabeaufforderung `1` an, um mit der Standardkonfiguration fortzufahren.

   Der Installationsvorgang wird mit dem standardmäßigen Evaluierungslizenzschlüssel, der im Installationsprogramm enthalten ist, fortgesetzt. Sie können die Evaluierungslizenz zu jedem beliebigen Zeitpunkt während des Testzeitraums oder danach durch einen gekauften Lizenzschlüssel ersetzen.

9 Geben Sie das Passwort für den Administratorbenutzer `admin` an.

10 Bestätigen Sie das Passwort.

   Die Benutzer `admin`, `dbauser` und `appuser` verwenden dieses Passwort.

   Die Installation von Sentinel wird beendet und der Server gestartet. Nach der Installation nimmt das Starten der Services möglicherweise einige Minuten in Anspruch, da das System eine einmalige Initialisierung ausführt. Warten Sie, bis die Installation abgeschlossen ist, bevor Sie sich am Server anmelden.

Geben Sie in einem Webbrowser folgende URL ein, um auf die Benutzeroberfläche von Sentinel Main zuzugreifen:

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

IP_AddressOrDNS_Sentinel_server ist die IP-Adresse oder der DNS-Name des Sentinel-Servers und *8443* ist der Standardport für den Sentinel-Server.

Angepasste Sentinel-Serverinstallation

Bei einer benutzerdefinierten Installation von Sentinel können Sie Anpassungen vornehmen, z. B. Ihren Lizenzschlüssel angeben, das Passwort ändern, andere Ports festlegen usw.

1 Soll der skalierbare Speicher aktiviert werden, müssen zunächst die in Kapitel 13, „Installation und Einrichtung von skalierbarem Speicher“, auf Seite 85 aufgeführten Voraussetzungen erfüllt sein.

2 Laden Sie die Installationsdatei von der Downloads-Website herunter.

3 Geben Sie in der Befehlszeile den folgenden Befehl ein, um die Installationsdatei zu extrahieren.

   ```
   tar zxvf <install_filename>
   ```

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

4 Geben Sie im Stamm des extrahierten Verzeichnisses den folgenden Befehl ein, um Sentinel zu installieren:

   ```
   ./install-sentinel
   ```

   Alternativ:

   Wenn Sie diese benutzerdefinierte Konfiguration dazu verwenden möchten, Sentinel auf mehr als einem Server zu installieren, können Sie die Installationsoptionen in einer Datei aufzeichnen. Diese Datei können Sie für die unbeaufsichtigte Installation von Sentinel auf anderen Systemen verwenden. Geben Sie zum Aufzeichnen Ihrer Installationsoptionen den folgenden Befehl an:

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

5 Geben Sie die entsprechende Zahl für die Sprache an, die für die Installation verwendet werden soll. Drücken Sie dann die Eingabetaste.

Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.

6 Drücken Sie die Leertaste, um die Lizenzvereinbarung durchzulesen.

7 Geben Sie `yes` bzw. `y` ein, um die Lizenzvereinbarung zu akzeptieren und mit der Installation fortzufahren.

Das Laden der Installationspakete kann einige Sekunden in Anspruch nehmen. Anschließend werden Sie zur Eingabe des Konfigurationstyps aufgefordert.

8 Geben Sie `2` ein, um Sentinel benutzerdefiniert zu konfigurieren.

9 Geben Sie `1` ein, um den standardmäßigen Evaluierungslizenzschlüssel zu verwenden.

Alternativ:

Geben Sie `2` ein, um einen erworbenen Lizenzschlüssel für Sentinel einzugeben.

10 Geben Sie das Passwort für den Administratorbenutzer `admin` ein und bestätigen Sie das Passwort.

11 Geben Sie das Passwort für den Datenbankbenutzer `dbauser` ein und bestätigen Sie das Passwort.

Das `dbauser`-Konto wird von Sentinel zur Interaktion mit der Datenbank verwendet. Das hier eingegebene Passwort kann zum Ausführen von Datenbankwartungsaufgaben verwendet werden, unter anderem zum Zurücksetzen des Administratorpassworts, falls dieses vergessen wird bzw. nicht mehr auffindbar ist.

12 Geben Sie das Passwort für den Anwendungsbenutzer `appuser` ein und bestätigen Sie das Passwort.

13 Ändern Sie die Portzuweisungen für die Sentinel-Services, indem Sie die entsprechende Nummer und dann die neue Portnummer angeben.

14 Geben Sie nach dem Ändern der Ports `7` ein, um den Änderungsvorgang abzuschließen.

15 Geben Sie `1` ein, um Benutzer nur über die interne Datenbank zu authentifizieren.

Alternativ:

Wenn in der Domäne ein LDAP-Verzeichnis konfiguriert ist, geben Sie `2` ein, um Benutzer über das LDAP-Verzeichnis zu authentifizieren.

Der Standardwert ist `1`.

16 ***Wenn Sie Sentinel im FIPS 140-2-Modus aktivieren möchten***, geben Sie `y` ein.

16a Geben Sie ein starkes Passwort für die Keystore-Datenbank an und wiederholen Sie das Passwort.

HINWEIS: Das Passwort muss mindestens sieben Zeichen lang sein. Das Passwort muss mindestens drei der folgenden Zeichenklassen enthalten: Ziffern, ASCII-Kleinbuchstaben, ASCII-Großbuchstaben, nicht alphanumerische ASCII-Zeichen und Nicht-ASCII-Zeichen.

Wenn ein ASCII-Großbuchstabe das erste Zeichen ist oder eine Ziffer das letzte Zeichen, werden diese nicht gezählt.

16b Wenn Sie externe Zertifikate zur Verbürgung in die Keystore-Datenbank einfügen möchten, drücken Sie `j` und geben Sie den Pfad für die Zertifikatsdatei an. Drücken Sie andernfalls `n`.

16c Konfigurieren Sie den FIPS 140-2-Modus, indem Sie die unter Kapitel 24, „Ausführen von Sentinel im FIPS 140-2-Modus“, auf Seite 131 genannten Aufgaben ausführen.

17 ***Aktivieren Sie den skalierbaren Speicher***, indem Sie `yes` (ja) oder `y` eingeben.

WICHTIG: Die Konfiguration mit skalierbarem Speicher lässt sich nicht rückgängig machen, allerdings können Sie bei einer Neuinstallation von Sentinel eine andere Entscheidung treffen.

17a Geben Sie die IP-Adressen bzw. Hostnamen und Portnummern der Komponenten für skalierbaren Speicher an.

17b (Bedingt) Wenn Sie die Aktivierung des skalierbaren Speichers abbrechen und mit der Sentinel-Installation fortfahren möchten, geben Sie `no` (nein) oder `n` ein.

17c Schließen Sie nach erledigter Sentinel-Installation die Konfiguration des skalierbaren Speichers wie im Abschnitt „Konfiguration für den skalierbaren Speicher nach der Installation“, auf Seite 92 beschrieben ab.

Die Installation von Sentinel wird beendet und der Server wird gestartet. Nach der Installation nimmt das Starten der Services möglicherweise einige Minuten in Anspruch, da das System eine einmalige Initialisierung ausführt. Warten Sie, bis die Installation abgeschlossen ist, bevor Sie sich am Server anmelden.

Geben Sie in einem Webbrowser folgende URL ein, um auf die Benutzeroberfläche von Sentinel Main zuzugreifen:

`https://`*`IP_AddressOrDNS_Sentinel_server`*`:8443/sentinel/views/main.html`

<*IP_AddressOrDNS_Sentinel_server*> ist die IP-Adresse oder der DNS-Name des Sentinel-Servers und *8443* ist der Standardport für den Sentinel-Server.

Konfiguration für den skalierbaren Speicher nach der Installation

1. Melden Sie sich beim SSDM-Server an.
2. Löschen Sie den Browser-Cache, um die installierte Sentinel-Version anzuzeigen.
3. Um Ereignisse und Warnmeldungen anzuzeigen, fügen Sie den in SSDM enthaltenen Elasticsearch-Knoten zum Elasticsearch-Cluster hinzu, den Sie für den skalierbaren Speicher eingerichtet haben:

   Öffnen Sie im lokalen Elasticsearch-Knoten die Datei `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` und fügen Sie die folgenden Informationen hinzu:

   - cluster.name: <*Elasticsearch-Cluster-Name*>
   - node.name: <*Knotenname*>
   - discovery.zen.ping.unicast.hosts: ["<*FQDN des Elasticsearch-Knotens 1*>", "<*FQDN des Elasticsearch-Knotens 2*>" und so weiter"]

   Öffnen Sie in allen externen Elasticsearch-Knoten `/etc/elasticsearch/elasticsearch.yml` und aktualisieren Sie

   discovery.zen.ping.unicast.hosts: ["<*FQDN des Elasticsearch-Knotens 1*>", "<*FQDN des Elasticsearch-Knotens 2*>" und so weiter"]

   HINWEIS: Stellen Sie sicher, dass die Werte der Parameter in der lokalen Datei `elasticsearch.yml` und in der Datei `elasticsearch.yml` in den externen Elasticsearch-Knoten übereinstimmen. Die einzigen Ausnahmen sind die Werte für `network.host` und `node.name`; diese Werte sind für den jeweiligen Knoten eindeutig.

4. Starten Sie mit folgendem Befehl die Indexierungsservices neu:

   ```
   rcsentinel stopSIdb
   rcsentinel startSIdb
   ```

5 Schließen Sie die Konfiguration des skalierbaren Speichers wie in den folgenden Abschnitten beschrieben ab:

- „Sichern von Daten in Elasticsearch“, auf Seite 77
- Performance Tuning Guidelines (Leitfaden für die Leistungsoptimierung) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch)
- Processing Data (Datenverarbeitung) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch)

Collector Manager- und Correlation Engine-Installation

Standardmäßig installiert Sentinel einen Collector Manager und eine Correlation Engine. Für Produktionsumgebungen richten Sie eine verteilte Bereitstellung ein, da hierbei die Datenerfassungskomponenten auf einem separaten Computer isoliert werden. Dies ist für die Bewältigung von Spitzenlasten und anderen Anomalien mit größtmöglicher Systemstabilität wichtig. Weitere Informationen zu den Vorteilen der Installation zusätzlicher Komponenten finden Sie unter „Vorteile von verteilten Bereitstellungen“, auf Seite 47.

WICHTIG: Sie müssen den zusätzlichen Collector Manager oder die Correlation Engine auf unterschiedlichen Systemen installieren. Der Collector Manager oder die Correlation Engine darf sich nicht auf dem System befinden, auf dem der Sentinel-Server installiert ist.

Installations-Checkliste: Vergewissern Sie sich vor dem Beginn der Installation, dass folgende Aufgaben abgeschlossen sind:

- Stellen Sie sicher, dass die Hardware und die Software den Mindestanforderungen entsprechen. Weitere Informationen finden Sie unter Kapitel 5, „Erfüllen der Systemanforderungen“, auf Seite 37.
- Synchronisieren Sie die Zeit mit NTP (Network Time Protocol).
- Ein Collector Manager erfordert Netzwerkkonnektivität zum Port für den Nachrichtenbus (61616) auf dem Sentinel-Server. Stellen Sie vor der Installation des Collector Managers sicher, dass alle Firewall- und Netzwerkeinstellungen über diesen Port kommunizieren dürfen.

Gehen Sie wie folgt vor, um den Collector Manager und die Correlation Engine zu installieren:

1 Starten Sie die Benutzeroberfläche von Sentinel Main, indem Sie in einem Webbrowser folgende URL eingeben:

```
https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html
```

<*IP_AddressOrDNS_Sentinel_server*> ist die IP-Adresse oder der DNS-Name des Sentinel-Servers und *8443* ist der Standardport für den Sentinel-Server.

Melden Sie sich mit dem bei der Installation des Sentinel-Servers angegebenen Benutzernamen und Passwort an.

2 Klicken Sie in der Symbolleiste auf **Downloads**.

3 Klicken Sie unter der gewünschten Installation auf **Installationsprogramm herunterladen**.

4 Klicken Sie auf **Datei speichern**, um das Installationsprogramm am gewünschten Standort zu speichern.

5 Geben Sie zum Extrahieren der Installationsdatei folgenden Befehl ein.

```
tar zxvf <install_filename>
```

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

6 Wechseln Sie in das Verzeichnis, in das Sie das Installationsprogramm extrahiert haben.

7 Geben Sie den folgenden Befehl ein, um den Collector Manager oder die Correlation Engine zu installieren:

Für den Collector Manager:

```
./install-cm
```

Für die Correlation Engine:

```
./install-ce
```

Alternativ:

Wenn Sie den Collector Manager oder die Correlation Engine auf mehr als einem System installieren möchten, können Sie die Installationsoptionen in einer Datei aufzeichnen. Diese Datei können Sie für die unbeaufsichtigte Installation von auf anderen Systemen verwenden. Geben Sie zum Aufzeichnen Ihrer Installationsoptionen den folgenden Befehl an:

Für den Collector Manager:

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

Für die Correlation Engine:

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

8 Geben Sie die Nummer der Sprache an, die Sie für die Installation verwenden möchten.

Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.

9 Drücken Sie die Leertaste, um die Lizenzvereinbarung durchzulesen.

10 Geben Sie `yes` bzw. `y` ein, um die Lizenzvereinbarung zu akzeptieren und mit der Installation fortzufahren.

Das Laden der Installationspakete kann einige Sekunden in Anspruch nehmen. Anschließend werden Sie zur Eingabe des Konfigurationstyps aufgefordert.

11 Geben Sie bei Aufforderung die entsprechende Option an, um mit der standardmäßigen oder benutzerdefinierten Konfiguration fortzufahren.

12 Geben Sie den Hostnamen des standardmäßigen Kommunikationsservers oder die IP-Adresse des Computers ein, auf dem Sentinel installiert ist.

13 (Bedingt) Geben Sie bei einer benutzerdefinierten Konfiguration Folgendes an:

13a Portnummer des Kommunikationskanals für den Sentinel-Server

13b Portnummer des Sentinel-Webservers

14 Führen Sie zur Überprüfung des Zertifikats folgenden Befehl auf dem Sentinel-Server aus, wenn Sie zur Annahme des Zertifikats aufgefordert werden:

Für FIPS-Modus:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.activemqkeystore.jks
```

Für Nicht-FIPS-Modus:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/nonfips_backup/.activemqkeystore.jks
```

Vergleichen Sie die Zertifikatausgabe mit dem in Schritt 12 angezeigten Sentinel-Serverzertifikat.

HINWEIS: Stimmt das Zertifikat nicht überein, wird die Installation angehalten. Führen Sie die Installation erneut aus und überprüfen Sie die Zertifikate.

15 Akzeptieren Sie das Zertifikat, wenn die Zertifikatausgabe mit dem Sentinel-Serverzertifikat übereinstimmt.

16 Geben Sie den Berechtigungsnachweis für jeden Benutzer mit einer Verwalterfunktion an. Dieser besteht aus einem Benutzernamen und Passwort.

17 (Bedingt) Geben Sie bei einer benutzerdefinierten Konfiguration `yes` oder `y` ein, um den FIPS 140-2-Modus in Sentinel zu aktivieren und mit der FIPS-Konfiguration fortzufahren.

18 (Bedingt) Wenn die Umgebung eine Mehr-Faktor-Authentifizierung oder starke Authentifizierung verwendet, müssen Sie die Sentinel-Client-ID und das Sentinel-Clientgeheimnis angeben. Weitere Informationen zu Authentifizierungsmethoden finden Sie unter „Authentication Methods“ (Authentifizierungsmethoden) im *Sentinel Administrator Guide* (Sentinel-Administrationshandbuch).

Öffnen Sie die folgende URL, um die Sentinel-Client-ID und das Sentinel-Clientgeheimnis abzurufen:

`https://Hostname:Port/SentinelAuthServices/oauth/clients`

Hierbei gilt:

- *Hostname* ist der Hostname des Sentinel-Servers.
- *Port* ist der von Sentinel verwendete Port (üblicherweise 8443).

Die angegebene URL verwendet zum Abrufen der Sentinel-Client-ID und des Sentinel-Clientgeheimnisses Ihre aktuelle Sentinel-Sitzung.

19 (Bedingt) Wenn Sie die Ereignisgrafikfunktion aktiviert haben, müssen Sie Collector Manager zur weißen Liste in Elasticsearch hinzufügen. Weitere Informationen finden Sie unter „Zugriff für Elasticsearch-Clients über die weiße Liste“, auf Seite 80.

20 Fahren Sie wie aufgefordert mit der Installation fort, bis sie abgeschlossen ist.

Ausführen einer automatischen Installation

Die automatische oder unbeaufsichtigte Installation ist nützlich, wenn Sie mehrere Sentinel-Server, Collector Manager- oder Correlation Engine-Instanzen in Ihrer Bereitstellung installieren möchten. In diesem Fall können Sie die Installationsparameter während der interaktiven Installation aufzeichnen und die aufgezeichnete Datei auf allen anderen Servern ausführen.

Wenn Sie eine automatische Installation ausführen möchten, vergewissern Sie sich, dass Sie die Installationsparameter in einer Datei aufgezeichnet haben. Weitere Informationen zum Erstellen der Antwortdatei finden Sie in „Standardmäßige Sentinel-Serverinstallation“, auf Seite 89 oder „Angepasste Sentinel-Serverinstallation“, auf Seite 90 und „Collector Manager- und Correlation Engine-Installation“, auf Seite 93.

Zur Aktivierung des FIPS 140-2-Modus müssen Sie sicherstellen, dass die Antwortdatei die folgenden Parameter enthält:

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

Gehen Sie folgendermaßen vor, um eine automatische Installation durchzuführen:

1 Laden Sie die Installationsdateien von der Downloads-Website herunter.

2 Melden Sie sich als `root`-Benutzer beim Server an, wenn Sie Sentinel, einen Collector Manager oder eine Correlation Engine installieren möchten.

3 Geben Sie den folgenden Befehl an, um die Installationsdateien aus der TAR-Datei zu extrahieren:

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

Ersetzen Sie *<install_filename>* mit dem tatsächlichen Namen der Installationsdatei.

4 Geben Sie folgenden Befehl ein, um Sentinel im Automatikmodus zu installieren:

Für den Sentinel-Server:

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

Für den Collector Manager:

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

Für die Correlation Engine:

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

Die Installation wird mit den Werten fortgesetzt, die in der Antwortdatei gespeichert sind.

Nach der Installation eines Sentinel-Servers nimmt das Starten der Services möglicherweise einige Minuten in Anspruch, da das System eine einmalige Initialisierung ausführt. Warten Sie, bis die Installation abgeschlossen ist, bevor Sie sich am Server anmelden.

5 **(Bedingt) Wenn Sie den FIPS 140-2-Modus für den Sentinel-Server aktivieren möchten,**

konfigurieren Sie den FIPS 140-2-Modus, indem Sie die unter Kapitel 24, „Ausführen von Sentinel im FIPS 140-2-Modus“, auf Seite 131 genannten Aufgaben ausführen.

Installieren von Sentinel mit einem Nicht-root-Benutzer

Wenn die Richtlinien in Ihrem Unternehmen nicht zulassen, dass die vollständige Installation von Sentinel mit dem Benutzer `root` ausgeführt wird, können Sie Sentinel auch mit einem `Nicht-Root`-Benutzer installieren, d. h. mit dem Benutzer `novell`. Bei dieser Installationsart werden einige wenige Schritte mit dem Benutzer `root` ausgeführt. Anschließend stellen Sie die Sentinel-Installation mit dem Benutzer `novell` fertig, der mit dem Benutzer `root` erstellt wurde. Danach wird die Installation mit dem Benutzer `root` fertig gestellt.

Wenn Sie Sentinel als `Nicht-Root`-Benutzer ausführen, sollten Sie es mit dem Benutzer „novell“ installieren. Installation mit einem anderen Nicht-Root-Benutzer als der Benutzer „novell“ werden nicht unterstützt, auch wenn die Installation erfolgreich fortschreitet.

HINWEIS: Bei der Installation von Sentinel in einem bereits bestehenden, nicht standardmäßigen Verzeichnis müssen Sie sicherstellen, dass der Benutzer „novell“ über Eigentumsberechtigungen für das Verzeichnis verfügt. Führen Sie folgenden Befehl aus, um Eigentumsberechtigungen zuzuweisen:

```
chown novell:novell <non-default installation directory>
```

---

1 Laden Sie die Installationsdateien von der Downloads-Website herunter.

2 Geben Sie in der Befehlszeile den folgenden Befehl ein, um die Installationsdateien aus der TAR-Datei zu extrahieren:

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

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

3 Melden Sie sich als `root` an dem Server an, auf dem Sie Sentinel als `root` installieren möchten.

4 Geben Sie folgenden Befehl ein:

```
./bin/root_install_prepare
```

Es wird eine Liste der Befehle angezeigt, die mit root-Berechtigungen ausgeführt werden. Wenn die mit dem Nicht-root-Benutzer ausgeführte Sentinel-Installation an einem anderen als dem Standardinstallationsort erfolgen soll, geben Sie zusammen mit dem Befehl die Option „--location“ an. Beispiel:

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

Der Wert, den Sie an die Option `--location` weiterreichen, `foo`, wird den Verzeichnispfaden vorangestellt.

Es wird außerdem eine Gruppe mit dem Namen `novell` und ein Benutzer mit dem Namen `novell` erstellt, sofern noch nicht vorhanden.

5 Akzeptieren Sie die Liste der Befehle.

Die angezeigten Befehle werden ausgeführt.

6 Geben Sie den folgenden Befehl ein, um zur Anmeldung als der neu erstellte Nicht-Root-Benutzer `novell` zu wechseln:

```
su novell
```

7 (Bedingt) So führen Sie eine interaktive Installation aus:

7a Geben Sie je nach zu installierender Komponente den entsprechenden Befehl ein:

Komponente	Befehl
Sentinel-Server	**Standardstandort:** `./install-sentinel`
	Anderer Standort: `./install-sentinel --location=/foo`
Collector Manager	**Standardstandort:** `./install-cm`
	Anderer Standort: `./install-cm --location=/foo`
Correlation Engine	**Standardstandort:** `./install-ce`
	Anderer Standort: `./install-cm --location=/foo`

7b Fahren Sie mit Schritt 9 fort.

8 (Bedingt) Wenn Sie eine automatische Installation ausführen möchten, vergewissern Sie sich, dass Sie die Installationsparameter in einer Datei aufgezeichnet haben. Weitere Informationen zum Erstellen der Antwortdatei finden Sie in „Standardmäßige Sentinel-Serverinstallation“, auf Seite 89 oder „Angepasste Sentinel-Serverinstallation“, auf Seite 90.

So führen Sie eine automatische Installation aus:

8a Geben Sie je nach zu installierender Komponente den entsprechenden Befehl ein:

Komponente	Befehl
Sentinel-Server	**Standardstandort:** `./install-sentinel -u <Antwortdatei>`
	Anderer Standort: `./install-sentinel --location=/foo -u <Antwortdatei>`
Collector Manager	**Standardstandort:** `./install-cm -u <Antwortdatei>`
	Anderer Standort: `./install-cm --location=/foo -u <Antwortdatei>`
Correlation Engine	**Standardstandort:** `./install-ce -u <Antwortdatei>`
	Anderer Standort: `./install-ce --location=/foo -u <Antwortdatei>`

Die Installation wird mit den Werten fortgesetzt, die in der Antwortdatei gespeichert sind.

8b Fahren Sie mit Schritt 12 fort.

9 Geben Sie die Nummer der Sprache an, die Sie für die Installation verwenden möchten.

Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.

10 Lesen Sie die Endbenutzer-Lizenzvereinbarung und geben Sie `yes` oder `y` ein, um die Lizenzbedingungen zu akzeptieren und die Installation fortzusetzen.

Die Installation wird gestartet. Zunächst werden alle RPM-Pakete installiert. Diese Installation kann einige Sekunden dauern.

11 Sie werden aufgefordert, den Installationsmodus anzugeben.

- Wenn Sie die Standardkonfiguration auswählen, fahren Sie fort mit Schritt 8 bis Schritt 10 in „Standardmäßige Sentinel-Serverinstallation“, auf Seite 89.
- Wenn Sie die benutzerdefinierte Konfiguration auswählen, fahren Sie fort mit Schritt 8 bis Schritt 15 in „Angepasste Sentinel-Serverinstallation“, auf Seite 90.

12 Melden Sie sich als `root`-Benutzer an und geben Sie folgenden Befehl ein, um die Installation abzuschließen:

```
./bin/root_install_finish
```

Die Installation von Sentinel wird beendet und der Server gestartet. Nach der Installation nimmt das Starten der Services möglicherweise einige Minuten in Anspruch, da das System eine einmalige Initialisierung ausführt. Warten Sie, bis die Installation abgeschlossen ist, bevor Sie sich am Server anmelden.

Geben Sie in einem Webbrowser folgende URL ein, um auf die Benutzeroberfläche von Sentinel Main zuzugreifen:

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

IP_AddressOrDNS_Sentinel_server ist die IP-Adresse oder der DNS-Name des Sentinel-Servers und *8443* ist der Standardport für den Sentinel-Server.

15 Appliance-Installation

Sentinel Appliance ist eine ausführungsbereite Software-Appliance, die auf Micro Focus Common Appliance Framework basiert. Die Appliance vereint ein verstärktes SLES 12 SP3-Betriebssystem und den in die Sentinel-Software integrierten Aktualisierungsservice. Sie bietet eine einfache und nahtlose Benutzererfahrung und ermöglicht Ihnen, vorhandene Investitionen besser zu nutzen. Sentinel Appliance bietet eine Weboberfläche zur Konfiguration und Überwachung der Appliance.

Das Sentinel Appliance-Image ist als ISO- oder OVF-Paket für die Bereitstellung in virtuellen Umgebungen verfügbar. Weitere Informationen zu den unterstützten Virtualisierungsplattformen finden Sie auf der Website Sentinel Technical Information (Technische Informationen für Sentinel).

Voraussetzungen

Die Umgebung, in der Sie Sentinel Appliance als ISO-Paket installieren, muss die folgenden Voraussetzungen erfüllen:

- Lesen Sie vor der Installation von Sentinel Appliance die Versionshinweise des zertifizierten SLES, um sich über die neuen Funktionen und bekannten Probleme zu informieren.
- (Bedingt) Wenn Sie die Sentinel Appliance mit dem ISO-Image auf Bare-Metal-Hardware installieren, laden Sie sich das ISO-Datenträger-Image der Appliance von der Support-Website herunter und erstellen Sie eine DVD.
- Vergewissern Sie sich, dass auf der Festplatte mindestens 50 GB freier Speicherplatz zur Verfügung steht, damit das Installationsprogramm einen automatischen Partitionierungsvorschlag erstellen kann.
- Stellen Sie sicher, dass das System über mindestens 4 GB Arbeitsspeicher zum Abschließen der Installation verfügt. Wenn weniger als 4 GB Arbeitsspeicher verfügbar sind, tritt bei der Installation ein Fehler auf. Bei mehr als 4 GB, jedoch weniger als den empfohlenen 24 GB Arbeitsspeicher meldet die Installation, dass weniger Arbeitsspeicher als empfohlen zur Verfügung steht.

Installieren der Sentinel-ISO-Appliance

In diesem Abschnitt wird erklärt, wie Sie Sentinel, Collector Manager und Correlation Engine mithilfe des ISO-Appliance-Images installieren. Dieses Image-Format erlaubt die Generierung eines vollständigen Datenträger-Images in Form eines bootfähigen ISO-DVD-Images, das direkt auf der Hardware bereitgestellt wird. Dabei kann es sich um physische Bare-Metal-Hardware oder virtuelle Hardware (nicht installierte virtuelle Maschine in einem Hypervisor) handeln.

Installieren von Sentinel

So installieren Sie Sentinel Appliance mit dem ISO-Image:

1. Laden Sie das virtuelle ISO-Appliance-Image von der Download-Website herunter.
2. (Bedingt) Wenn Sie einen Hypervisor verwenden, gehen Sie wie folgt vor:

   Richten Sie die virtuelle Maschine mithilfe des virtuellen ISO-Appliance-Images ein und schalten Sie sie ein.

   Alternativ:

   Brennen Sie das ISO-Image auf eine DVD, richten Sie die virtuelle Maschine mit der DVD ein und schalten Sie sie ein.
3. (Bedingt) Wenn Sie Sentinel Appliance auf Bare-Metal-Hardware installieren, gehen Sie wie folgt vor:
   - **3a** Booten Sie den physischen Computer über die DVD im DVD-Laufwerk.
   - **3b** Befolgen Sie die Bildschirmanweisungen des Installationsassistenten.
   - **3c** Wählen Sie **Sentinel-Server <*version*>** installieren aus.
4. Wählen Sie die gewünschte Sprache aus.
5. Wählen Sie das Tastaturlayout aus.
6. Klicken Sie auf **Weiter**.
7. Lesen und akzeptieren Sie die SUSE Enterprise Server Software-Lizenzvereinbarung. Klicken Sie auf **Weiter**
8. Lesen und akzeptieren Sie die Lizenzvereinbarung für Sentinel Server Appliance. Klicken Sie auf **Weiter**
9. Legen Sie die Passwörter, die NTP-Konfiguration und die Zeitzone für Sentinel Appliance fest.

   Legen Sie die `vaadmin`-Anmeldedaten zur Anmeldung bei der Verwaltungskonsole von Sentinel Appliance fest.

   HINWEIS: Nach der Installation können Sie die NTP-Konfiguration und die Zeitzone auf eine der folgenden Weisen ändern:

   - Geben Sie in der Befehlszeile `yast->Network Services->NTP Configuration` ein.
   - Klicken Sie in der Verwaltungskonsole von Sentinel Appliance auf **Uhrzeit**.

   Wenn die Zeit unmittelbar nach der Installation nicht synchronisiert erscheint, führen Sie den folgenden Befehl aus, um NTP neu zu starten:

   ```
   rcntp restart
   ```

   ---
10. Geben Sie auf der Seite zu den Netzwerkeinstellungen für Sentinel Server Appliance den Hostnamen und die Domäne an. Wählen Sie entweder **Statische IP-Adresse** oder **DHCP-IP-Adresse** aus.
11. Klicken Sie auf **Weiter**.
12. (Bedingt) Wenn Sie in Schritt 10 **Statische IP-Adresse** ausgewählt haben, geben Sie die Netzwerkverbindungseinstellungen an.
13. Klicken Sie auf **Weiter**.
14. Legen Sie das Passwort für den Benutzer `admin` fest und klicken Sie dann auf **Weiter**.

    Die Appliance wird installiert.
15. Notieren Sie sich die IP-Adresse der Appliance, die in der Konsole angezeigt wird.

16 Melden Sie sich als `root`-Benutzer bei der Konsole an, um sich bei der Appliance anzumelden.

   Geben Sie den Benutzernamen `root` ein und geben Sie das in Schritt 9 festgelegte Passwort ein.

17 Fahren Sie mit „Konfiguration der Appliance im Anschluss an die Installation“, auf Seite 104 fort.

Installieren von Collector Manager- und Correlation Engine-Instanzen

Die Vorgehensweise zur Installation von Collector Manager oder Correlation Engine ähnelt der Vorgehensweise zur Installation von Sentinel und unterscheidet sich nur dadurch, dass Sie die entsprechende ISO-Appliance-Datei von der Download-Website herunterladen müssen.

1 Führen Sie die Schritte 1 bis 13 aus, die unter „Installieren von Sentinel“, auf Seite 100 aufgeführt sind.

   Das Installationsskript prüft, ob genügend Arbeitsspeicher und Plattenspeicherplatz zur Verfügung stehen. Bei weniger als 1 GB verfügbarem Arbeitsspeicher wird die Installation nicht fortgeführt. Die Schaltfläche **Weiter** ist in diesem Fall nicht verfügbar.

2 Legen Sie die folgende Konfiguration für den Collector Manager oder die Correlation Engine fest:

   - **Sentinel Server Hostname or IP Address (Hostname oder IP-Adresse des Sentinel-Servers):** Geben Sie den Hostnamen/die IP-Adresse des Sentinel-Servers an, mit dem der Collector Manager oder die Correlation Engine eine Verbindung herstellen soll.
   - **Sentinel-Kommunikationskanalport:** Geben Sie die Portnummer des Kommunikationskanals für den Sentinel-Server an. Die Standardportnummer ist `61616`.
   - **Sentinel-Webserver-Port:** Geben Sie den Sentinel-Webserver-Port an. Der Standardport ist 8443.
   - **Benutzername mit Verwalterfunktion:** Geben Sie den Benutzernamen eines beliebigen Benutzers mit Verwalterfunktion an.
   - **Passwort für Benutzer mit Verwalterfunktion:** Geben Sie das Passwort für den im obigen Feld·angegebenen Benutzernamen an.

3 (Bedingt) Wenn die Umgebung eine Mehr-Faktor-Authentifizierung oder starke Authentifizierung verwendet, müssen Sie die Sentinel-Client-ID und das Sentinel-Clientgeheimnis angeben. Weitere Informationen zu Authentifizierungsmethoden finden Sie unter „Authentication Methods“ (Authentifizierungsmethoden) im *Sentinel Administrator Guide* (Sentinel-Administrationshandbuch).

   Öffnen Sie die folgende URL, um die Sentinel-Client-ID und das Sentinel-Clientgeheimnis abzurufen:

   `https://`*`Hostname`*`:`*`Port`*`/SentinelAuthServices/oauth/clients`

   Hierbei gilt:

   - *Hostname* ist der Hostname des Sentinel-Servers.
   - *Port* ist der von Sentinel verwendete Port (üblicherweise 8443).

   Die angegebene URL verwendet zum Abrufen der Sentinel-Client-ID und des Sentinel-Clientgeheimnisses Ihre aktuelle Sentinel-Sitzung.

4 Klicken Sie auf **Weiter**.

5 Akzeptieren Sie das Zertifikat, wenn Sie dazu aufgefordert werden.

6 Notieren Sie sich die IP-Adresse der Appliance, die in der Konsole angezeigt wird.

Die IP-Adresse wird angezeigt sowie eine Meldung, die besagt, dass diese Appliance abhängig davon, was Sie installieren, der Sentinel-Collector Manager oder die Sentinel-Correlation Engine ist. Die Konsole zeigt auch die IP-Adresse der Sentinel-Server-Benutzeroberfläche an.

7 Führen Sie Schritt 16 bis Schritt 17 in „Installieren von Sentinel“, auf Seite 100 aus.

Installieren von Sentinel Appliance mit OVF-Image

In diesem Abschnitt finden Sie Informationen zur Installation von Sentinel, Collector Manager und Correlation Engine als OVF-Appliance-Image.

OVF ist das Standardformat für virtuelle Maschinen und wird von den meisten Hypervisoren unterstützt – entweder direkt oder nach einer einfachen Konvertierung. Für das OVF-Image von Sentinel Appliance sind zwei Hypervisoren zertifiziert, aber sie kann auch mit anderen Hypervisoren verwendet werden.

Installieren von Sentinel

So installieren Sie Sentinel Appliance mit dem OVF-Image:

1 Laden Sie das virtuelle OVF-Appliance-Image von der Download-Website herunter.

2 Importieren Sie in der Verwaltungskonsole Ihres Hypervisors die OVF-Image-Datei als neue virtuelle Maschine. Lassen Sie den Hypervisor das OVF-Image in sein natives Format konvertieren, wenn Sie dazu aufgefordert werden.

3 Stellen Sie sicher, dass die virtuellen Hardware-Ressourcen, die Ihrer neuen virtuellen Maschine zugeordnet sind, die Anforderungen von Sentinel erfüllen.

4 Schalten Sie die virtuelle Maschine ein.

5 Wählen Sie die gewünschte Sprache aus.

6 Wählen Sie das Tastaturlayout aus.

7 Klicken Sie auf **Weiter**.

8 Lesen und akzeptieren Sie die SUSE Enterprise Server Software-Lizenzvereinbarung. Klicken Sie auf **Weiter**.

9 Lesen und akzeptieren Sie die Lizenzvereinbarung für Sentinel Server Appliance. Klicken Sie auf **Weiter**.

10 Legen Sie die Passwörter, die NTP-Konfiguration und die Zeitzone für Sentinel Appliance fest.

Legen Sie die `vaadmin`-Anmeldedaten zur Anmeldung bei der Verwaltungskonsole von Sentinel Appliance fest.

HINWEIS: Nach der Installation können Sie die NTP-Konfiguration und die Zeitzone auf eine der folgenden Weisen ändern:

- Geben Sie in der Befehlszeile `yast->Network Services->NTP Configuration` ein.
- Klicken Sie in der Verwaltungskonsole von Sentinel Appliance auf **Uhrzeit**.

Wenn die Zeit unmittelbar nach der Installation nicht synchronisiert erscheint, führen Sie den folgenden Befehl aus, um NTP neu zu starten:

```
rcntp restart
```

---

11 Geben Sie auf der Seite zu den Netzwerkeinstellungen für Sentinel Server Appliance den Hostnamen und die Domäne an. Wählen Sie entweder **Statische IP-Adresse** oder **DHCP-IP-Adresse** aus.

12 Klicken Sie auf **Weiter**.

13 (Bedingt) Wenn Sie in Schritt 11 **Statische IP-Adresse** ausgewählt haben, geben Sie die Netzwerkverbindungseinstellungen an.

14 Klicken Sie auf **Weiter**.

15 Legen Sie das Sentinel-admin-Passwort fest und klicken Sie auf **Weiter**.

   Nach der Installation nimmt das Starten der Services möglicherweise einige Minuten in Anspruch, da das System eine einmalige Initialisierung ausführt. Warten Sie, bis die Installation abgeschlossen ist, bevor Sie sich am Server anmelden.

16 Notieren Sie sich die IP-Adresse der Appliance, die in der Konsole angezeigt wird. Greifen Sie über diese IP-Adresse auf die Benutzeroberfläche von Sentinel Main zu.

Installieren von Collector Manager- und Correlation Engine-Instanzen

So installieren Sie einen Collector Manager oder eine Correlation Engine als OVF-Appliance-Image auf einem VMware ESX-Server:

1 Führen Sie die Schritte 1 bis 14 aus, die unter „Installieren von Sentinel“, auf Seite 102 aufgeführt sind.

   Das Installationsskript prüft, ob genügend Arbeitsspeicher und Plattenspeicherplatz zur Verfügung stehen. Bei weniger als 1 GB verfügbarem Arbeitsspeicher wird die Installation nicht fortgeführt. Die Schaltfläche **Weiter** ist in diesem Fall nicht verfügbar.

2 Geben Sie den Hostnamen/die IP-Adresse des Sentinel-Servers an, mit dem der Collector Manager eine Verbindung herstellen soll.

3 Geben Sie die Portnummer des Communication Server an. Der Standardport ist `61616`.

4 Geben Sie den Berechtigungsnachweis für jeden Benutzer mit einer Verwalterfunktion an. Dieser besteht aus einem Benutzernamen und Passwort.

5 (Bedingt) Wenn die Umgebung eine Mehr-Faktor-Authentifizierung oder starke Authentifizierung verwendet, müssen Sie die Sentinel-Client-ID und das Sentinel-Clientgeheimnis angeben. Weitere Informationen zu Authentifizierungsmethoden finden Sie unter „Authentication Methods“ (Authentifizierungsmethoden) im *Sentinel Administrator Guide* (Sentinel-Administrationshandbuch).

   Öffnen Sie die folgende URL, um die Sentinel-Client-ID und das Sentinel-Clientgeheimnis abzurufen:

   `https://`*`Hostname`*`:`*`Port`*`/SentinelAuthServices/oauth/clients`

   Hierbei gilt:

   - *Hostname* ist der Hostname des Sentinel-Servers.
   - *Port* ist der von Sentinel verwendete Port (üblicherweise 8443).

   Die angegebene URL verwendet zum Abrufen der Sentinel-Client-ID und des Sentinel-Clientgeheimnisses Ihre aktuelle Sentinel-Sitzung.

6 Klicken Sie auf **Weiter**.

7 Akzeptieren Sie das Zertifikat.

8 Klicken Sie auf **Weiter**, um die Installation abzuschließen.

   Nach Abschluss der Installation wird im Installationsprogramm die IP-Adresse angezeigt sowie eine Meldung, die besagt, dass diese Appliance abhängig davon, was Sie installieren, Sentinel Collector Manager oder Sentinel Correlation Engine ist. Sie zeigt auch die IP-Adresse der Sentinel-Server-Benutzeroberfläche an.

Konfiguration der Appliance im Anschluss an die Installation

Nach der Installation von Sentinel müssen Sie weitere Konfigurationsschritte ausführen, damit die Appliance ordnungsgemäß funktioniert.

- „Registrieren für Aktualisierungen“, auf Seite 104
- „Erstellen von Partitionen für herkömmlichen Speicher“, auf Seite 105
- „Konfigurieren des skalierbaren Speichers“, auf Seite 106
- „Konfigurieren der Appliance mit SMT“, auf Seite 106

Registrieren für Aktualisierungen

Registrieren Sie Sentinel Appliance beim Appliance-Aktualisierungskanal, um Aktualisierungen für Sentinel und die neuesten Betriebssystemaktualisierungen zu erhalten. Zur Registrierung der Appliance müssen Sie zunächst den Appliance-Registrierungscode oder den Appliance-Aktivierungsschlüssel vom Kundenservicezentrum abrufen.

Registrieren mit der Verwaltungskonsole von Sentinel Appliance

Wenn Sie SLES 12 SP3 verwenden, können Sie sich mit der Verwaltungskonsole von Sentinel Appliance zum Erhalt von Aktualisierungen registrieren.

1 Starten Sie Sentinel Appliance auf eine der folgenden Weisen:
   - Melden Sie sich bei Sentinel an und klicken Sie auf **Sentinel Main** > **Appliance**.
   - Geben Sie im Webbrowser die folgende URL an: `https://<IP_Adresse>:9443`.
2 Melden Sie sich mit dem Benutzer `vaadmin` oder `root` an.
3 Klicken Sie auf **Onlineaktualisierung** > **Jetzt registrieren**.
4 Geben Sie im Feld **Email** die Email-ID an, unter der Sie Aktualisierungen empfangen möchten.
5 Geben Sie im Feld **Aktivierungsschlüssel** den Registrierungscode ein.
6 Klicken Sie auf **Registrieren**, um die Registrierung abzuschließen.

Registrierung mit Befehlen

Wenn Sie SLES 11 SP4 oder SLES 12 SP3 verwenden, können Sie die Registrierung über Befehle ausführen.

So registrieren Sie sich zum Erhalt von Aktualisierungen

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

2 Geben Sie die folgenden Befehle an:

- Geben Sie zum Registrieren des Servers Folgendes ein: `suse_register -a regcode-sentinel="<Registrierungscode>" -a email="<Email_ID>"`
- Geben Sie zum Registrieren von Collector Manager Folgendes ein: `suse_register -a regcode-sentinel-collector="<Registrierungscode>" -a email="<Email_ID>"`
- Geben Sie zum Registrieren von Correlation Engine Folgendes ein: `suse_register -a regcode-sentinel-correlation ="<Registrierungscode>" -a email="<Email_ID>"`
- Um Sentinel im Hochverfügbarkeitsmodus zu registrieren, geben Sie Folgendes ein: `suse_register -a regcode-sentinel-ha ="<Registrierungscode>" -a email="<Email_ID>"`

Geben Sie für den Email-Parameter die Email-ID an, unter der Sie Aktualisierungen empfangen möchten.

Erstellen von Partitionen für herkömmlichen Speicher

Die Informationen in diesem Abschnitt beziehen sich nur auf den Fall, dass Sie zur Datenspeicherung herkömmlichen Speicher verwenden möchten.

Es empfiehlt sich, separate Partitionen anzulegen, damit die Sentinel-Daten auf einer anderen Partition gespeichert werden als die ausführbaren Dateien, die Konfigurations- und die Betriebssystemdateien. Das separate Speichern von Variablendaten bietet den Vorteil einer einfacheren Sicherung von Dateisätzen, einer einfacheren Wiederherstellung im Falle einer Beschädigung und einer besseren Stabilität, falls die Datenträgerpartition aufgefüllt ist. Weitere Informationen zum Planen der Partitionen finden Sie unter „Planen des herkömmlichen Speichers“, auf Seite 41. Sie können mit dem YaST-Tool eine Partition in der Appliance hinzufügen und ein Verzeichnis in die neue Partition verschieben.

Gehen Sie folgendermaßen vor, um eine neue Partition zu erstellen und die Datendateien aus ihrem Verzeichnis zur neu erstellten Partition zu verschieben:

1 Melden Sie sich mit dem Benutzer `root` bei Sentinel an.

2 Führen Sie folgenden Befehl aus, um Sentinel auf der Appliance zu stoppen:

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

3 Geben Sie den folgenden Befehl ein, um zum Benutzer `novell` zu wechseln:

```
su -novell
```

4 Verschieben Sie den Inhalt des Verzeichnisses `/var/opt/novell/sentinel/` an einen temporären Standort.

5 Wechseln Sie zum `root`-Benutzer.

6 Geben Sie folgenden Befehl ein, um auf das YaST2 Control Center zuzugreifen:

```
yast
```

7 Wählen Sie **System > Partitioner (Partitionierer)** aus.

8 Lesen Sie die Warnmeldung und wählen Sie **Yes (Ja)** aus, um die neue, ungenutzte Partition hinzufügen.

Weitere Informationen zum Erstellen von Partitionen finden Sie unter Using the YaST Partitioner (Verwenden des YaST-Partitionierungsprogramms) in der *SLES 11-Dokumentation*.

9 Hängen Sie die neue Partition unter `/var/opt/novell/sentinel/` ein.

10 Geben Sie den folgenden Befehl ein, um zum Benutzer `novell` zu wechseln:

```
su -novell
```

11 Verschieben Sie den Inhalt des Datenverzeichnisses vom temporären Standort (wo Sie es in Schritt 4 gespeichert haben) zurück in das Verzeichnis `/var/opt/novell/sentinel/` in der neuen Partition.

12 Führen Sie den folgenden Befehl aus, um Sentinel Appliance neu zu starten:

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

Konfigurieren des skalierbaren Speichers

Anleitungen zur Aktivierung und Konfiguration des optionalen skalierbaren Datenspeichers finden Sie im Abschnitt „Configuring Scalable Storage“ (Konfigurieren des skalierbaren Speichers) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuchs).

Konfigurieren der Appliance mit SMT

In sicheren Umgebungen, wo die Appliance ohne direkten Internetzugriff ausgeführt werden muss, können Sie die Appliance mit dem Subscription Management Tool (SMT) konfigurieren, mit dem Sie die Appliance auf die neuesten verfügbaren Versionen von Sentinel aufrüsten können. SMT ist ein Proxy-System-Paket, das ins Customer Center integriert ist und Kernfunktionen des Customer Centers zur Verfügung stellt.

- „Voraussetzungen“, auf Seite 106
- „Konfigurieren der Appliance“, auf Seite 107
- „Aufrüsten der Appliance“, auf Seite 107

Voraussetzungen

Ehe Sie die Appliance mit SMT konfigurieren können, müssen die folgenden Voraussetzungen erfüllt sein:

- Fordern Sie beim Kundenservicezentrum die Anmeldedaten zum Abrufen von Sentinel-Aktualisierungen an. Weitere Informationen zum Erhalt der Anmeldedaten hält der Technische Support bereit.
- Stellen Sie sicher, dass SLES 11 SP3 mit den folgenden Paketen auf dem Computer, auf dem SMT installiert werden soll, installiert wurde:
  - htmldoc
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - perl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - yum-metadata-parser
  - createrepo
  - perl-DBI
  - apache2-prefork
  - libapr1
  - perl-Data-ShowTable
  - perl-Net-Daemon

- perl-Tie-IxHash
- fltk
- libapr-util1
- perl-PIRPC
- apache2-mod_perl
- apache2-utils
- apache2
- perl-DBD-mysql

- Installieren Sie SMT und konfigurieren Sie den SMT-Server. Weitere Informationen finden Sie in folgenden Abschnitten der SMT-Dokumentation:
  - SMT Installation (SMT-Installation)
  - SMT Server Configuration (SMT-Serverkonfiguration)
  - Mirroring Installation and Update Repositories with SMT (Spiegelung von Installations- und Aktualisierungs-Repositorys mit SMT)
- Installieren Sie das Dienstprogramm `wget` auf dem Appliance-Computer.

Konfigurieren der Appliance

Führen Sie diese Schritte aus, um die Appliance mit SMT zu konfigurieren:

1. Führen Sie auf dem SMT-Server die folgenden Befehle aus, um die Appliance-Repositorys zu aktivieren:

   ```
   smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64
   ```

   ```
   smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64
   ```

   ```
   smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64
   ```

2. Zur Konfiguration der Appliance mit SMT befolgen Sie die Anleitung im Abschnitt „Configuring Clients to Use SMT“ (Konfigurieren von Clients zur Verwendung von SMT) in der SMT-Dokumentation.

Aufrüsten der Appliance

Informationen zur Aufrüstung der Appliance finden Sie unter „Aufrüsten von Sentinel“, auf Seite 159.

16 Installieren von zusätzlichen Collectors und Connectors

Standardmäßig werden alle herausgegebenen Collectors und Connectors bei der Installation von Sentinel installiert. In den folgenden Abschnitten finden Sie Informationen zur Installation eines neuen Collectors oder Connectors, der nach der Veröffentlichung von Sentinel freigegeben wurde.

Installieren eines Collectors

Gehen Sie folgendermaßen vor, um einen Collector zu installieren:

1. Laden Sie den gewünschten Collector von der Website für Sentinel-Plugins herunter.
2. Klicken Sie in **Sentinel Main** auf die Dropdownliste **admin** und klicken Sie dann auf **Anwendungen**.
3. Klicken Sie auf **Control Center starten**, um das Sentinel Control Center zu starten.
4. Klicken Sie in der Symbolleiste auf **Ereignisquellenmanagement** > **Live-Ansicht**. Klicken Sie dann auf **Werkzeuge** > **Plugin importieren**.
5. Suchen Sie die Collector-Datei, die Sie in Schritt 1 heruntergeladen haben, und klicken Sie dann auf **Weiter**.
6. Befolgen Sie die verbleibenden Aufforderungen und klicken Sie dann auf **Fertig stellen**.

Informationen zur Konfiguration des Collectors finden Sie in der Dokumentation für den jeweiligen Collector auf der Website für Sentinel-Plugins.

Installieren eines Connectors

Gehen Sie folgendermaßen vor, um einen Connector zu installieren:

1. Laden Sie den gewünschten Connector von der Website für Sentinel-Plugins herunter.
2. Klicken Sie in **Sentinel Main** auf die Dropdownliste **admin** und klicken Sie dann auf **Anwendungen**.
3. Klicken Sie auf **Control Center starten**, um das Sentinel Control Center zu starten.
4. Klicken Sie in der Symbolleiste auf **Ereignisquellenmanagement** > **Live-Ansicht**. Klicken Sie dann auf **Werkzeuge** > **Plugin importieren**.
5. Suchen Sie die Connector-Datei, die Sie in Schritt 1 heruntergeladen haben, und klicken Sie dann auf **Weiter**.
6. Befolgen Sie die verbleibenden Aufforderungen und klicken Sie dann auf **Fertig stellen**.

Informationen zur Konfiguration des Connectors finden Sie in der Dokumentation für den jeweiligen Connector auf der Website für Sentinel-Plugins.

17 Überprüfen der Installation

Sie können erkennen, ob die Installation erfolgreich war, wenn Sie einen der folgenden Schritte ausführen:

- Überprüfen Sie die Sentinel-Version:

  ```
  /etc/init.d/sentinel version
  ```

- Überprüfen Sie, ob die Sentinel-Services im FIPS- oder Nicht-FIPS-Modus einwandfrei funktionieren:

  ```
  /etc/init.d/sentinel status
  ```

- Überprüfen Sie, ob die Webdienste aktiv sind:

  ```
  netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  Die Standard-Portnummer lautet 8443.

- Starten Sie Sentinel:

  1. Starten Sie einen unterstützten Webbrowser.
  2. Geben Sie die URL von Sentinel an:

     ```
     https://IP_AddressOrDNS_Sentinel_server:8443
     ```

     IP_AddressOrDNS_Sentinel_server ist die IP-Adresse oder der DNS-Name des Sentinel-Servers und *8443* ist der Standardport für den Sentinel-Server.
  3. Melden Sie sich mit dem Administratornamen und -passwort an, die Sie während der Installation angegeben haben. Der Standard-Benutzername lautet „admin“.

IV Konfigurieren von Sentinel

In diesem Abschnitt finden Sie Informationen zur Konfiguration von Sentinel und den einsatzbereiten Plugins.

18 Konfigurieren der Zeit

Die Uhrzeit eines Ereignisses ist für seine Verarbeitung in Sentinel von ausgesprochen großer Bedeutung. Sie spielt für Berichterstellung und Revision sowie für die Echtzeitverarbeitung eine wichtige Rolle. In diesem Abschnitt finden Sie Informationen über das Verständnis von Zeit in Sentinel, über die Konfiguration der Zeit und der Behandlung von Zeitzonen.

Zeit in Sentinel

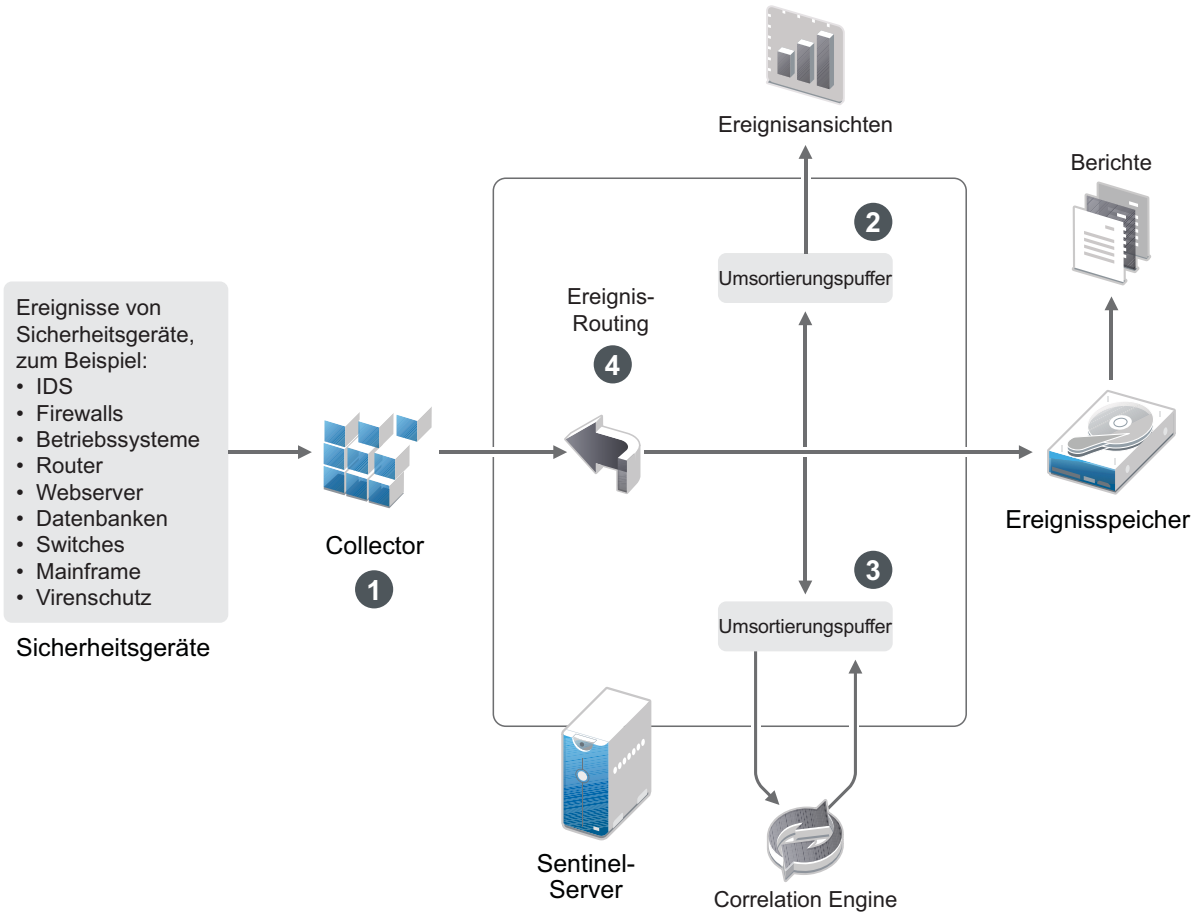
Sentinel ist ein verteiltes System, das aus verschiedenen Prozessen besteht, die im Netzwerk verteilt sind. Zudem kann es durch die Ereignisquelle zu einer gewissen Verzögerung kommen. Aus diesem Grund ordnen die Sentinel-Vorgänge die Ereignisse vor der Verarbeitung nach der Uhrzeit neu an.

Jedes Ereignis verfügt über drei Zeitfelder:

- **Ereigniszeit:** Dies ist die Ereigniszeit, die von allen Analyse-Engines, Suchen, Berichten usw. verwendet wird.
- **Sentinel-Verarbeitungszeit:** Die Zeit, zu der Sentinel die Daten vom Gerät erfasst hat. Sie wird von der Zeit des Collector Manager-Systems bestimmt.
- **Observer-Ereigniszeit:** Der Zeitstempel, den das Gerät den Daten zugewiesen hat. Diese Angabe ist nicht immer ein verlässlicher Zeitstempel und kann erheblich von der Sentinel-Verarbeitungszeit abweichen. Dies ist beispielsweise der Fall, wenn das Gerät Daten gesammelt liefert.

Die folgende Abbildung zeigt dieses Vorgehen in einem Sentinel-System mit herkömmlichem Speicher:

Abbildung 18-1 *Sentinel-Zeit*



1. Standardmäßig wird die Ereigniszeit auf die Sentinel-Verarbeitungszeit festgelegt. Im Idealfall stimmt jedoch die Ereigniszeit mit der Observer-Ereigniszeit überein, wenn diese verfügbar und zuverlässig ist. Wenn die Gerätezeit verfügbar und genau ist und vom Collector richtig analysiert wird, ist es am besten, die Datenerfassung mit **verbürgter Ereignisquellenzeit** zu konfigurieren. Der Collector stimmt die Ereigniszeit mit der Observer-Ereigniszeit ab.
2. Ereignisse mit einer Ereigniszeit, die um weniger als 5 Minuten von der Serverzeit abweicht, werden normal von „Event Views“ (Ereignisansichten) verarbeitet. Ereignisse, deren Ereigniszeit mehr als 5 Minuten in der Zukunft liegen, werden in den „Event Views“ (Ereignisansichten) nicht angezeigt, sondern in den Ereignisspeicher eingefügt. Ereignisse, deren Ereigniszeit über 5 Minuten in der Zukunft oder weniger als 24 Stunden in der Vergangenheit liegt, werden in den Diagrammen angezeigt, jedoch nicht in den Ereignisdaten dieser Diagramme. Zum Abrufen dieser Ereignisse aus dem Ereignisspeicher ist eine Detailanalyse erforderlich.
3. Die Ereignisse werden in 30-Sekunden-Intervallen sortiert, damit die Correlation Engine sie in chronologischer Reihenfolge verarbeiten kann. Liegt die Ereigniszeit mehr als 30 Sekunden vor der Serverzeit, verarbeitet die Correlation Engine das Ereignis nicht.
4. Liegt die Ereigniszeit mehr als 5 Minuten vor der Collector Manager-Systemzeit, leitet Sentinel das Ereignis direkt an den Ereignisspeicher und umgeht dabei die Echtzeitsysteme wie Correlation Engine und Sicherheitsintelligenz.

Konfigurieren der Zeit in Sentinel

Die Correlation Engine verarbeitet nach Uhrzeit geordnete Ereignisdatenströme und erkennt Muster in Ereignissen sowie Zeitmuster im Datenstrom. Das Gerät, das das Ereignis generiert, schließt die Zeit jedoch manchmal nicht in die Protokollnachricht ein.

Es stehen zwei Möglichkeiten zur Verfügung, die Zeit für ein ordnungsgemäßes Arbeiten von Sentinel zu konfigurieren:

- Konfigurieren Sie NTP auf dem Collector Manager und deaktivieren Sie **Verbürgte Ereignisquelle Uhrzeit** auf der Ereignisquelle im Ereignisquellen-Manager. Sentinel verwendet den Collector Manager als Zeitquelle für die Ereignisse.
- Wählen Sie **Verbürgte Ereignisquelle Uhrzeit** auf der Ereignisquelle im Ereignisquellen-Manager aus. Sentinel verwendet die Uhrzeit aus der Protokollnachricht als richtige Zeit.

So ändern Sie diese Einstellung auf der Ereignisquelle:

1. Melden Sie sich an der Ereignisquellenverwaltung an.

   Weitere Informationen finden Sie unter „Zugriff auf die Ereignisquellenverwaltung“ im *Sentinel - Administrationshandbuch*.
2. Klicken Sie mit der rechten Maustaste auf die Ereignisquelle, für die Sie die Zeiteinstellung ändern möchten, und wählen Sie **Bearbeiten** aus.
3. Aktivieren oder deaktivieren Sie die Option **Verbürgte Ereignisquelle** unten in der Registerkarte **Allgemein**.
4. Klicken Sie zum Speichern der Änderungen auf **OK**.

Konfigurieren der maximalen Verzögerungszeit für Ereignisse

Wenn Sentinel Ereignisse von Ereignisquellen empfängt, kann eine Verzögerung zwischen dem Zeitpunkt, an dem das Ereignis erzeugt wurde, und der Verarbeitung dieses Ereignisses in Sentinel eintreten. Sentinel speichert die Ereignisse mit großen Verzögerungen in separaten Partitionen. Falls zahlreiche Ereignisse über einen längeren Zeitraum verzögert sind, kann dies darauf hinweisen, dass die Ereignisquelle nicht ordnungsgemäß konfiguriert ist. Damit kann auch die Leistung von Sentinel beeinträchtigt werden, wenn Sentinel versucht, die verzögerten Ereignisse zu verarbeiten. Da die verzögerten Ereignisse aus einer fehlerhaften Konfiguration stammen können und daher ggf. nicht gespeichert werden sollen, können Sie in Sentinel die zulässige maximale Verzögerung für eingehende Ereignisse festlegen. Alle Ereignisse, die die maximale Verzögerung überschreiten, werden durch den Ereignisrouter verworfen. Legen Sie die maximale Verzögerung in der Datei `configuration.properties` in der folgenden Eigenschaft fest:

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

Außerdem ist es möglich, in regelmäßigen Abständen eine Liste in der Sentinel-Serverprotokolldatei festzuhalten, aus der die Ereignisquellen, von denen die übermäßig verzögerten Ereignisse empfangen werden, hervorgehen. Zum Protokollieren dieser Daten legen Sie den Höchstwert in der Datei `configuration.properties` in der folgenden Eigenschaft fest:

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

Zeitzonen

In einer verteilten Umgebung kann die Berücksichtigung der Zeitzonen sehr komplex werden. Beispielsweise können sich die Ereignisquelle, der Collector Manager, der Backend-Sentinel-Server und der Client, auf dem die Daten angezeigt werden, in jeweils unterschiedlichen Zeitzonen befinden. Zusätzliche Aspekte wie die Sommerzeit oder Ereignisquellen, die nicht melden, auf welche Zeitzone sie festgelegt sind (z. B. alle Syslog-Quellen), führen zu einer Vielzahl möglicher Probleme, die zu bewältigen sind. Sentinel bietet flexible Lösungen, damit Sie stets korrekt darstellen können, wann ein Ereignis aufgetreten ist, und diese Ereignisse mit Ereignissen von anderen Quellen in der gleichen oder in unterschiedlichen Zeitzonen vergleichen können.

Im Allgemeinen gibt es drei verschiedene Möglichkeiten, wie Ereignisquellen die Zeitstempel melden:

- Die Ereignisquelle meldet die Uhrzeit als koordinierte Weltzeit (UTC). Beispielsweise werden alle Standardereignisse des Windows-Ereignisprotokolls mit der UTC-Zeit gemeldet.
- Die Ereignisquelle meldet die örtliche Zeit und schließt dabei stets die Zeitzone in den Zeitstempel ein. Beispielsweise schließen Ereignisquellen, die für die Strukturierung des Zeitstempels RFC 3339 befolgen, die Zeitzone als Abweichung ein; andere Quellen verwenden lange Zeitzonen-IDs wie „Americas/New York“ oder kurze IDs wie „EST“. Dies kann aufgrund von Konflikten und unangemessenen Auflösungen zu Problemen führen.
- Die Ereignisquelle berichtet die Ortszeit, gibt jedoch keine Zeitzone an. Unglücklicherweise nutzt das sehr weit verbreitete Syslog-Format dieses Modell.

Im ersten Fall kann stets die UTC-Zeit errechnet werden, zu der das Ereignis aufgetreten ist (sofern ein Zeitsynchronisierungsprotokoll verwendet wird). Die Ereigniszeit kann daher sehr einfach mit anderen Ereignisquellen an einem beliebigen Standort verglichen werden. Die Ortszeit, zu der das Ereignis aufgetreten ist, kann jedoch nicht automatisch ermittelt werden. Aus diesem Grund kann die Zeitzone einer Ereignisquelle in Sentinel manuell festgelegt werden, indem der Ereignisquellenknoten im Ereignisquellen-Manager bearbeitet und die entsprechende Zeitzone angegeben wird. Diese Angabe hat keinen Einfluss auf die Berechnung der Parameter „DeviceEventTime“ und „EventTime“. Sie wird lediglich im ObserverTZ-Feld hinterlegt und zur Berechnung der verschiedenen ObserverTZ-Felder verwendet, z. B. „ObserverTZHour“. Diese Felder sind stets als Ortszeit ausgedrückt.

Wenn im zweiten Fall die Zeitzone im langen Format oder als Abweichung angegeben wird, kann die Zeit in UTC-Zeit umgerechnet werden (in „DeviceEventTime“ gespeichert). Sie können jedoch auch die Ortszeit für die ObserverTZ-Felder berechnen. Bei der Verwendung von kurzen Zeitzonen-IDs können gegebenenfalls Konflikte auftreten.

Beim dritten Szenario muss der Administrator die Ereignisquellenzeitzone manuell für alle betroffenen Quellen festlegen, damit Sentinel ordnungsgemäß die UTC-Zeit berechnen kann. Wird die Zeitzone nicht richtig durch Bearbeiten des Ereignisquellenknotens im Ereignisquellen-Manager festgelegt, ist möglicherweise die Geräteereigniszeit „DeviceEventTime“ (und ggf. die Ereigniszeit „EventTime“) falsch. Auch „ObserverTZ“ und die verbundenen Felder können in diesem Fall falsch sein.

Der Collector für eine bestimmte Ereignisquellenart (z. B. Microsoft Windows) verfügt üblicherweise über Informationen dazu, wie eine Ereignisquelle Zeitstempel darstellt, und nimmt die erforderlichen Anpassungen vor. Es empfiehlt sich, die Zeitzonen aller Ereignisquellenknoten im Ereignisquellen-Manager stets manuell festzulegen, es sei denn, Sie sind sich sicher, dass die Ereignisquelle in der Ortszeit berichtet und die Zeitzone immer in den Zeitstempel einschließt.

Die Ereignisquellendarstellung des Zeitstempels wird im Collector und im Collector Manager verarbeitet. Die Geräteereigniszeit „DeviceEventTime“ und die Ereigniszeit „EventTime“ werden im UTC-Format gespeichert. Die ObserverTZ-Felder werden als Zeichenkette gespeichert, deren Wert die Ortszeit der Ereignisquelle darstellt. Diese Informationen werden vom Collector Manager an den

Sentinel-Server gesendet und im Ereignisspeicher gespeichert. Die Zeitzonen des Collector Managers und des Sentinel-Servers dürfen diesen Vorgang und die gespeicherten Daten nicht beeinflussen. Wenn das Ereignis jedoch auf einem Client im Webbrowser angezeigt wird, wird die UTC-Ereigniszeit gemäß dem Webbrowser in die Ortszeit umgewandelt, sodass alle Ereignisse in der Ortszeit des Clients dargestellt werden. Über die Details in den ObserverTZ-Feldern kann der Benutzer die Ortszeit der Quelle anzeigen.

19 Sichern von Daten in Elasticsearch

Sentinel nutzt Kibana, ein browserbasiertes Analyse- und Such-Dashboard, mit dem Sie Ereignisse und Warnmeldungen in Dashboards grafisch darstellen können. Sentinel speichert und indexiert Warnmeldungen in Elasticsearch. Sie können Sentinel so konfigurieren, dass auch die Ereignisse in Elasticsearch gespeichert und indexiert werden, um die Ereignisgrafikfunktion voll auszunutzen. Sentinel-Dashboards greifen auf Daten von Elasticsearch zu, um Ereignisse und Warnmeldungen in Dashboards zu präsentieren. Um sicherzustellen, dass in den Dashboards nur Daten angezeigt werden, zu deren Anzeige die Rolle des Benutzers berechtigt ist, und um den unbefugten Zugriff auf Daten in Elasticsearch zu vermeiden, müssen Sie das Elasticsearch-Sicherheits-Plugin installieren. Weitere Informationen finden Sie unter „Sichern von Daten in Elasticsearch“, auf Seite 77.

20 Ereignisgrafik aktivieren

In einer Einrichtung mit skalierbarem Speicher sind die Ereignisgrafiken standardmäßig verfügbar. Bei einer Einrichtung mit herkömmlichem Speicher sind die Ereignisgrafiken nur verfügbar, wenn Sie den Grafikdatenspeicher (Elasticsearch) zum Speichern und Indexieren von Daten aktiviert haben.

Voraussetzung

Für die skalierbare und verteilte Indexierung von Ereignissen in Produktionsumgebungen müssen Sie zusätzliche Elasticsearch-Knoten in einem Clustermodus einrichten. Informationen zur Installation und Konfiguration von Elasticsearch in einem Clustermodus finden Sie in „Installation und Konfiguration von Elasticsearch“, auf Seite 75.

Ereignisgrafik aktivieren

So aktivieren Sie die Ereignisgrafiken:

1. Melden Sie sich beim Sentinel-Server als der Benutzer „novell“ an.
2. Öffnen Sie die Datei `/etc/opt/novell/sentinel/config/configuration.properties`.
3. Legen Sie `eventvisualization.traditionalstorage.enabled` auf `true` fest.
4. Aktualisieren Sie nach einigen Minuten die Benutzeroberfläche, um die Ereignisgrafiken anzuzeigen.

   Nun sollten alle Dashboards sichtbar sein, die in der Benutzeroberfläche **Mein Sentinel** aktiviert sind. Starten Sie ein beliebiges Dashboard, zum Beispiel das Bedrohungssuche-Dashboard, und klicken Sie auf **Suche**. Das Dashboard zeigt alle Ereignisse an, die in der letzten Stunde generiert wurden.
5. (Optional) In den Ereignisgrafik-Dashboards werden nur die Ereignisse angezeigt, die nach der Aktivierung der Ereignisgrafik verarbeitet wurden. Um die im dateibasierten Speicher vorhandenen Ereignisse anzuzeigen, migrieren Sie die Daten von einem dateibasierten Speicher zu Elasticsearch. Weitere Informationen finden Sie unter Kapitel 33, „Migrieren von Daten zu Elasticsearch“, auf Seite 183.

HINWEIS: Das Aktivieren und Deaktivieren der Ereignisgrafik erzeugt eine Ausnahme, während die Sentinel-Indexierungsservices neu gestartet werden. Diese Ausnahme wird erwartet und kann ignoriert werden.

---

21 Ändern der Konfiguration nach der Installation

Wenn Sie nach der Installation von Sentinel einen gültigen Lizenzschlüssel eingeben möchten oder das Passwort oder die zugewiesenen Ports ändern möchten, können Sie hierzu das Skript `configure.sh` ausführen. Das Skript befindet sich im Ordner `/opt/novell/sentinel/setup`.

1. Fahren Sie Sentinel mit dem folgenden Befehl herunter:

   ```
   rcsentinel stop
   ```

2. Geben Sie in der Befehlszeile folgenden Befehl ein, um das Skript `configure.sh` auszuführen:

   ```
   ./configure.sh
   ```

3. Geben Sie `1` ein, um die Standardkonfiguration durchzuführen, oder `2`, um Sentinel benutzerdefiniert zu konfigurieren.
4. Drücken Sie die Leertaste, um die Lizenzvereinbarung durchzulesen.
5. Geben Sie `yes` bzw. `y` ein, um die Lizenzvereinbarung zu akzeptieren und mit der Installation fortzufahren.

   Das Laden der Installationspakete kann einige Sekunden in Anspruch nehmen.
6. Geben Sie `1` ein, um den standardmäßigen Evaluierungslizenzschlüssel zu verwenden.

   Alternativ:

   Geben Sie `2` ein, um einen erworbenen Lizenzschlüssel für Sentinel einzugeben.
7. Wählen Sie aus, ob Sie das vorhandene Passwort für den Administratorbenutzer `admin` beibehalten möchten.
   - Wenn Sie das vorhandene Passwort beibehalten möchten, geben Sie `1` ein und fahren Sie fort mit Schritt 8.
   - Wenn Sie das Passwort ändern möchten, geben Sie `2` ein. Geben Sie dann das neue Passwort an, bestätigen Sie das Passwort und fahren Sie fort mit Schritt Schritt 8.

     Der `admin`-Benutzer wird zum Ausführen von Verwaltungsaufgaben über die Benutzeroberfläche von Sentinel Main verwendet. Dies umfasst auch die Erstellung weiterer Benutzerkonten.
8. Wählen Sie aus, ob Sie das vorhandene Passwort für den Datenbankbenutzer `dbauser` beibehalten möchten.
   - Wenn Sie das vorhandene Passwort beibehalten möchten, geben Sie `1` ein und fahren Sie fort mit Schritt 9.
   - Wenn Sie das Passwort ändern möchten, geben Sie `2` ein. Geben Sie dann das neue Passwort an, bestätigen Sie das Passwort und fahren Sie fort mit Schritt Schritt 9.

   Das `dbauser`-Konto wird von Sentinel zur Interaktion mit der Datenbank verwendet. Das hier eingegebene Passwort kann zum Ausführen von Datenbankwartungsaufgaben verwendet werden, unter anderem zum Zurücksetzen des Administratorpassworts, falls dieses vergessen wird bzw. nicht mehr auffindbar ist.

9 Wählen Sie aus, ob Sie das vorhandene Passwort für den Anwendungsbenutzer `appuser` beibehalten möchten.

- Wenn Sie das vorhandene Passwort beibehalten möchten, geben Sie `1` ein und fahren Sie fort mit Schritt 10.
- Wenn Sie das Passwort ändern möchten, geben Sie `2` ein. Geben Sie dann das neue Passwort an, bestätigen Sie das Passwort und fahren Sie fort mit Schritt Schritt 10.

  Das `appuser`-Konto ist eine interne Identität, mit der der Java-Prozess von Sentinel eine Verbindung zur Datenbank herstellt und mit ihr interagiert. Das hier eingegebene Passwort wird zum Ausführen von Datenbankaufgaben verwendet.

10 Ändern Sie die Portzuweisungen für die Sentinel-Services, indem Sie die entsprechende Nummer und dann die neue Portnummer angeben.

11 Geben Sie nach dem Ändern der Ports `7` ein, um den Änderungsvorgang abzuschließen.

12 Geben Sie `1` ein, um Benutzer nur über die interne Datenbank zu authentifizieren.

Alternativ:

Wenn in der Domäne ein LDAP-Verzeichnis konfiguriert ist, geben Sie `2` ein, um Benutzer über das LDAP-Verzeichnis zu authentifizieren.

Der Standardwert ist `1`.

22 Konfigurieren von einsatzbereiten Plugins

Sentinel wird mit den standardmäßigen Sentinel-Plugins vorinstalliert, die zum Zeitpunkt der Veröffentlichung von Sentinel verfügbar waren.

In diesem Abschnitt finden Sie Informationen zur Konfiguration der einsatzbereiten Plugins.

Anzeigen der vorinstallierten Plugins

Sie können die Liste der in Sentinel vorinstallierten Plugins anzeigen. Außerdem können Sie die Versionen und andere Metadaten der Plugins anzeigen, um einfacher ermitteln zu können, ob die jeweils neueste Version eines Plugins installiert ist.

So zeigen Sie die auf dem Sentinel-Server installierten Plugins an:

1. Melden Sie sich als Administrator unter `https://<IP-Adresse>:8443` bei der Benutzeroberfläche von Sentinel Main an. 8443 ist der Standardport für den Sentinel-Server.
2. Klicken Sie auf **Plugins** > **Katalog**.

Konfigurieren der Datenerfassung

Informationen zur Konfiguration von Sentinel für die Datenerfassung finden Sie unter „Collecting and Routing Event Data“ (Erfassen und Routing von Ereignisdaten) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Konfigurieren von Lösungspaketen

Sentinel enthält eine Vielzahl nützlicher, einsatzbereiter Inhalte, die Sie sofort anwenden können, um verschiedenste Analyseanforderungen zu erfüllen. Viele dieser Inhalte stammen aus dem vorinstallierten Sentinel Core Solution Pack und dem Lösungspaket für die ISO 27000-Reihe. Weitere Informationen finden Sie im Abschnitt „Using Solution Packs“ (Verwenden von Lösungspaketen) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).

Lösungspakete ermöglichen das Einteilen und Gruppieren von Inhalten in Steuerelemente oder Richtliniensätze, die als Einheit behandelt werden. Die Steuerelemente der Lösungspakete sind vorinstalliert, um Ihnen einsatzbereite Inhalte zur Verfügung zu stellen. Sie müssen diese Steuerelemente jedoch formal implementieren bzw. über die Benutzeroberfläche von Sentinel Main testen.

Wenn Sie das ordnungsgemäße Funktionieren der Sentinel-Bereitstellung etwas strenger überprüfen möchten, können Sie hierzu den formellen Beglaubigungsvorgang nutzen, der in den Lösungspaketen enthalten ist. Der Beglaubigungsvorgang implementiert die Steuerelemente der Lösungspakete und testet sie, genau wie Sie dies mit Steuerelementen anderer Lösungspakete tun würden. Als Teil dieses Vorgangs bescheinigt die beauftragte Person, dass alle entsprechenden Aufgaben ausgeführt wurden. Diese Bescheinigungen werden dann Bestandteil einer Revisionsliste, die überprüft werden kann, um die ordnungsgemäße Implementierung jedes bestimmten Steuerelements zu bezeugen.

Sie können den Beglaubigungsvorgang über den Solution Manager ausführen. Weitere Informationen zur Implementierung und zum Testen der Steuerelemente finden Sie unter „Installieren und Verwalten von Lösungspaketen“ im *Sentinel -Administrationshandbuch*.

Konfigurieren von Aktionen und Integratoren

Informationen zur Konfiguration der einsatzbereiten Plugins finden Sie in der Dokumentation zum jeweiligen Plugin auf der Website für Sentinel-Plugins.

23 Aktivieren des FIPS 140-2-Modus in einer vorhandenen Sentinel-Installation

In diesem Kapitel finden Sie Informationen zur Aktivierung des FIPS 140-2-Modus in einer vorhandenen Installation von Sentinel.

HINWEIS: Bei diesen Anweisungen wird angenommen, dass Sentinel im Verzeichnis `/opt/novell/sentinel` installiert ist. Die Befehle müssen als `novell`-Benutzer ausgeführt werden.

Aktivieren des FIPS 140-2-Modus am Sentinel-Server

So aktivieren Sie den FIPS 140-2-Modus am Sentinel-Server:

1. Melden Sie sich beim Sentinel-Server an.
2. Wechseln Sie zum `novell`-Benutzer (`su novell`).
3. Wechseln Sie zum Sentinel-Verzeichnis „bin“.
4. Führen Sie das Skript `convert_to_fips.sh` aus und folgen Sie den Anweisungen am Bildschirm.
5. (Bedingt) Wenn Ihre Umgebung eine Mehr-Faktor-Authentifizierung oder starke Authentifizierung verwendet, führen Sie das Skript `create_mfa_fips_keys.sh` aus und befolgen Sie die Bildschirmanweisungen.

   HINWEIS: Das Skript benötigt während der Ausführung das Passwort für die NSS-Datenbank.

   ---

6. (Bedingt) Wenn die Umgebung eine Mehr-Faktor-Authentifizierung oder starke Authentifizierung verwendet, müssen Sie die Sentinel-Client-ID und das Sentinel-Clientgeheimnis angeben. Weitere Informationen zu Authentifizierungsmethoden finden Sie unter „Authentication Methods“ (Authentifizierungsmethoden) im *Sentinel Administrator Guide* (Sentinel-Administrationshandbuch).

   Öffnen Sie die folgende URL, um die Sentinel-Client-ID und das Sentinel-Clientgeheimnis abzurufen:

   `https://`*`Hostname`*`:`*`Port`*`/SentinelAuthServices/oauth/clients`

   Hierbei gilt:

   - *Hostname* ist der Hostname des Sentinel-Servers.
   - *Port* ist der von Sentinel verwendete Port (üblicherweise 8443).

   Die angegebene URL verwendet zum Abrufen der Sentinel-Client-ID und des Sentinel-Clientgeheimnisses Ihre aktuelle Sentinel-Sitzung.

7 Starten Sie den Sentinel-Server neu.

8 Konfigurieren Sie den FIPS 140-2-Modus, indem Sie die unter Kapitel 24, „Ausführen von Sentinel im FIPS 140-2-Modus“, auf Seite 131 genannten Aufgaben ausführen.

Aktivieren des FIPS 140-2-Modus auf Remote-Instanzen von Collector Manager und Correlation Engine

Sie müssen den FIPS 140-2-Modus auf der Remote-Instanz von Collector Manager und der Remote-Instanz von Correlation Engine aktivieren, wenn Sie die FIPS-zugelassene Kommunikation mit dem Sentinel-Server verwenden möchten, der im FIPS 140-2-Modus ausgeführt wird.

So aktivieren Sie eine Remote-Instanz von Collector Manager oder Correlation Engine für den FIPS 140-2-Modus:

1 Melden Sie sich bei der Remote-Instanz von Collector Manager oder Correlation Engine an.

2 Wechseln Sie zum `novell`-Benutzer (`su novell`).

3 Wechseln Sie zum Verzeichnis „bin“: Der Standardspeicherort lautet `/opt/novell/sentinel/bin`.

4 Führen Sie das Skript `convert_to_fips.sh` aus und folgen Sie den Anweisungen am Bildschirm.

5 Starten Sie Collector Manager oder Correlation Engine neu.

6 Konfigurieren Sie den FIPS 140-2-Modus, indem Sie die unter Kapitel 24, „Ausführen von Sentinel im FIPS 140-2-Modus“, auf Seite 131 genannten Aufgaben ausführen.

24 Ausführen von Sentinel im FIPS 140-2-Modus

In diesem Kapitel finden Sie Informationen über die Konfiguration und den Betrieb von Sentinel im FIPS 140-2-Modus.

Konfigurieren des Advisor-Service im FIPS 140-2-Modus

Der Advisor-Service verwendet eine sichere HTTPS-Verbindung, um seinen Feed vom Advisor-Server herunterzuladen. Das Zertifikat, das vom Server für die sichere Kommunikation verwendet wird, muss der Sentinel-FIPS-Keystore-Datenbank hinzugefügt werden.

So überprüfen Sie die erfolgreiche Registrierung bei der Ressourcenverwaltungs-Datenbank:

1. Laden Sie das Zertifikat vom Advisor-Server herunter und speichern Sie die Datei unter `advisor.cer`.
2. Importieren Sie das Advisor-Serverzertifikat in den Sentinel-FIPS-Keystore.

   Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

Konfigurieren der verteilten Suche im FIPS 140-2-Modus

Dieser Abschnitt enthält Informationen zur Konfiguration der verteilten Suche im FIPS 140-2-Modus.

Szenario 1: Die Quell- und Zielserver von Sentinel werden im FIPS 140-2-Modus ausgeführt.

Um eine verteilte Suche über mehrere im FIPS 140-2-Modus ausgeführte Sentinel-Server ausführen zu können, müssen die Zertifikate für die sichere Verbindung zum FIPS-Keystore hinzugefügt werden.

1. Melden Sie sich beim Quellcomputer für die verteilte Suche an.
2. Wechseln Sie zum Zertifikatsverzeichnis:

   ```
   cd <sentinel_install_directory>/config
   ```

3 Kopieren Sie das Quellzertifikat (`sentinel.cer`) an einen temporären Speicherort am Zielcomputer.

4 Importieren Sie das Quellzertifikat in den Sentinel-FIPS-Keystore des Zielcomputers.

   Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

5 Melden Sie sich beim Zielcomputer für die verteilte Suche an.

6 Wechseln Sie zum Zertifikatsverzeichnis:

```
cd /etc/opt/novell/sentinel/config
```

7 Kopieren Sie das Zielzertifikat (`sentinel.cer`) an einen temporären Speicherort auf dem Quellcomputer.

8 Importieren Sie das Zertifikat des Zielsystems in den Sentinel-FIPS-Keystore des Quellcomputers.

9 Starten Sie die Sentinel-Dienste neu, und zwar sowohl auf dem Quell- als auch auf dem Zielcomputer.

Szenario 2: Der Sentinel-Quellserver wird im Nicht-FIPS-Modus und der Sentinel-Zielserver im FIPS 140-2-Modus ausgeführt.

In diesem Fall müssen Sie den Webserver-Keystore auf dem Quellcomputer in das Zertifikatformat konvertieren und dann das Zertifikat zum Zielcomputer exportieren.

1 Melden Sie sich beim Quellcomputer für die verteilte Suche an.

2 Erstellen Sie den Webserver-Keystore im Zertifikatformat (`.cer`):

```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
password -file <certificate_name.cer>
```

3 Kopieren Sie das Quellzertifikat (`sentinel.cer`) der verteilten Suche an einen temporären Speicherort am Zielcomputer der verteilten Suche.

4 Melden Sie sich beim Zielcomputer für die verteilte Suche an.

5 Importieren Sie das Quellzertifikat in den Sentinel-FIPS-Keystore des Zielcomputers.

   Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

6 Starten Sie die Sentinel-Services auf dem Zielcomputer neu.

Szenario 3: Der Sentinel-Quellserver wird im FIPS-Modus und der Sentinel-Zielserver im Nicht-FIPS-Modus ausgeführt.

1 Melden Sie sich beim Zielcomputer für die verteilte Suche an.

2 Erstellen Sie den Webserver-Keystore im Zertifikatformat (.cer):

```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
password -file <certificate_name.cer>
```

3 Kopieren Sie das Zertifikat an einen temporären Standort des Quellcomputers der verteilten Suche.

4 Importieren Sie das Zielzertifikat in den Sentinel-FIPS-Keystore des Quellcomputers.

Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

5 Starten Sie die Sentinel-Services auf dem Quellcomputer neu.

Konfigurieren der LDAP-Authentifizierung im FIPS 140-2-Modus

So konfigurieren Sie die LDAP-Authentifizierung für Sentinel-Server, die im FIPS 140-2-Modus ausgeführt werden:

1 Rufen Sie das LDAP-Serverzertifikat vom LDAP-Administrator ab. Sie können auch einen Befehl verwenden. Beispiel:

```
openssl s_client -connect <LDAP server IP>:636
```

Kopieren Sie anschließend den zurückgegeben Text (zwischen den Zeilen BEGIN und END, doch ohne diese Zeilen) in eine Datei.

2 Importieren Sie das LDAP-Serverzertifikat in den Sentinel-FIPS-Keystore.

Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

3 Navigieren Sie als Benutzer mit Verwalterfunktion zur Benutzeroberfläche von **Sentinel Main** und fahren Sie mit der Konfiguration der LDAP-Authentifizierung fort.

Weitere Informationen finden Sie unter „LDAP Authentication Against a Single LDAP Server Or Domain“ (LDAP-Authentifizierung über einen einzelnen LDAP-Server bzw. eine einzelne LDAP-Domäne) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).

HINWEIS: Sie können auch die LDAP-Authentifizierung für einen Sentinel-Server konfigurieren, der im FIPS 140-2-Modus ausgeführt wird. Führen Sie dazu das Skript `ldap_auth_config.sh` im Verzeichnis `/opt/novell/sentinel/setup` aus.

Aktualisieren der Serverzertifikate in Remote-Instanzen von Collector Managern und Correlation Engine

Zur Konfiguration von vorhandenen Remote-Instanzen von Collector Manager und Correlation Engine für die Kommunikation mit einem Sentinel-Server, der im FIPS 140-2-Modus ausgeführt wird, können Sie entweder das Remote-System in den FIPS 140-2-Modus versetzen oder Sie können das Sentinel-Serverzertifikat auf das Remote-System aktualisieren und den Collector Manager und die

Correlation Engine im Nicht-FIPS-Modus belassen. Remote-Instanzen von Collector Manager im FIPS-Modus funktionieren möglicherweise nicht mit Ereignisquellen, die FIPS nicht unterstützen oder die einen der Sentinel-Connectors im normalen Modus benötigen.

Wenn Sie den FIPS 140-2-Modus auf der Remote-Instanz von Collector Manager oder Correlation Engine nicht aktivieren möchten, müssen Sie das neueste Sentinel-Serverzertifikat in das Remote-System kopieren, damit der Collector Manager oder die Correlation Engine mit dem Sentinel-Server kommunizieren kann.

So aktualisieren Sie das Sentinel-Serverzertifikat in der Remote-Instanz von Collector Manager oder Correlation Engine:

1. Melden Sie sich beim Computer der Remote-Instanz von Collector Manager oder Correlation Engine an.
2. Wechseln Sie zum `novell`-Benutzer (`su novell`).
3. Wechseln Sie zum Verzeichnis „bin“: Der Standardspeicherort lautet `/opt/novell/sentinel/bin`.
4. Führen Sie das Skript `updateServerCert.sh` aus und befolgen Sie die Anweisungen am Bildschirm.

Konfigurieren der Sentinel-Plugins zur Ausführung im FIPS 140-2-Modus

In diesem Abschnitt finden Sie Informationen zur Konfiguration verschiedener Sentinel-Plugins für die Ausführung im FIPS 140-2-Modus.

HINWEIS: Voraussetzung für die erfolgreiche Umsetzung dieser Anleitungen ist die Installation von Sentinel im Verzeichnis `/opt/novell/sentinel`. Führen Sie alle Befehle als `novell`-Benutzer aus.

Agent Manager Connector

Die folgende Prozedur sollten Sie nur durchführen, wenn Sie vorher bei der Konfiguration der Netzwerkeinstellungen des Agent Manager-Ereignisquellenservers die Option **Verschlüsselt (HTTPS)** ausgewählt haben.

So konfigurieren Sie Agent Manager Connector für die Ausführung im FIPS 140-2-Modus:

1. Fügen Sie den Agent Manager-Ereignisquellenserver hinzu oder bearbeiten Sie ihn. Fahren Sie mit der Bearbeitung in den Konfigurationsbildschirmen fort, bis das Fenster „Sicherheit“ angezeigt wird. Weitere Informationen finden Sie im *Agent Manager Connector-Handbuch*.
2. Wählen Sie eine der Optionen aus dem Feld *Client-Authentifizierungstyp* aus. Der Client-Authentifizierungstyp bestimmt, wie streng der SSL Agent Manager-Ereignisquellenserver die Identität der Agent Manager-Ereignisquellen überprüft, die versuchen, Daten zu senden.
   - **Offen:** Lässt alle SSL-Verbindungen zu, die von den Agent Manager-Agenten kommen. Führt keine Validierung oder Authentifizierung des Client-Zertifikats durch.
   - **Streng:** Validiert das Zertifikat als gültiges X.509-Zertifikat und überprüft außerdem, ob der Ereignisquellenserver dem Client-Zertifikat vertraut. Neue Quellen müssen explizit zu Sentinel hinzugefügt werden (wodurch verhindert wird, dass fremde Quellen nicht autorisierte Daten senden).

     Für die Option **Streng** müssen Sie das Zertifikat jedes neuen Agent Manager-Clients in den Sentinel-FIPS-Keystore importieren. Wenn Sentinel im FIPS 140-2-Modus ausgeführt wird, können Sie das Client-Zertifikat nicht über die Oberfläche der Ereignisquellenverwaltung (Event Source Management, ESM) importieren.

     Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

HINWEIS: Im FIPS 140-2-Modus verwendet der Agent Manager-Ereignisquellenserver das Sentinel-Server-Schlüsselpaar. Es ist nicht erforderlich, das Schlüsselpaar zu importieren.

---

3. Wenn die Serverauthentifizierung in den Agenten aktiviert ist, müssen die Agenten zusätzlich so konfiguriert werden, dass sie das Zertifikat des Sentinel-Servers oder der Remote-Instanz von Collector Manager (je nachdem, wo der Connector bereitgestellt ist) als verbürgt betrachten.

   Speicherort des Sentinel-Serverzertifikats: `/etc/opt/novell/sentinel/config/sentinel.cer`

   Speicherort des Zertifikats für die Remote-Instanz von Collector Manager: `/etc/opt/novell/sentinel/config/rcm.cer`

HINWEIS: Wenn benutzerdefinierte Zertifikate verwendet werden, die digital von einer Zertifizierungsstelle unterzeichnet wurden, muss der Agent Manager-Agent der entsprechenden Zertifikatsdatei vertrauen.

Database (JDBC) Connector (Datenbank-Connector)

Die folgende Prozedur sollten Sie nur durchführen, wenn Sie vorher bei der Konfiguration der Datenbankverbindung die Option *SSL* ausgewählt haben.

So konfigurieren Sie den Database Connector für die Ausführung im FIPS 140-2-Modus:

1. Laden Sie vor der Konfiguration des Connectors das Zertifikat vom Datenbankserver herunter und speichern Sie es als Datei `database.cert` in das Verzeichnis `/etc/opt/novell/sentinel/config` am Sentinel-Server.

   Weitere Informationen hierzu finden Sie in der jeweiligen Datenbankdokumentation.
2. Importieren Sie das Zertifikat in den Sentinel-FIPS-Keystore.

   Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.
3. Fahren Sie mit der Konfiguration des Connectors fort.

Sentinel-Link-Connector

Sie sollten die folgende Prozedur nur durchführen, wenn Sie vorher bei der Konfiguration der Netzwerkeinstellungen des Sentinel-Link-Ereignisquellenservers die Option **Verschlüsselt (HTTPS)** ausgewählt haben.

So konfigurieren Sie den Sentinel Link Connector für die Ausführung im FIPS 140-2-Modus:

1. Fügen Sie den Sentinel-Link-Ereignisquellenserver hinzu oder bearbeiten Sie ihn. Fahren Sie mit der Bearbeitung in den Konfigurationsbildschirmen fort, bis das Fenster „Sicherheit“ angezeigt wird. Weitere Informationen finden Sie im *Sentinel Link Connector Guide* (Sentinel Link Connector-Handbuch).
2. Wählen Sie eine der Optionen aus dem Feld *Client-Authentifizierungstyp* aus. Der Client-Authentifizierungstyp bestimmt, wie streng der SSL Sentinel-Link-Ereignisquellenserver die Identität der Sentinel-Link-Ereignisquellen überprüft, die versuchen, Daten zu senden.
   - **Offen:** Lässt alle SSL-Verbindungen zu, die von den Clients (Sentinel-Link-Integratoren) kommen. Führt keine Validierung oder Authentifizierung des Integratorzertifikats durch.
   - **Streng:** Validiert das Integratorzertifikat als gültiges X.509-Zertifikat und überprüft außerdem, ob der Ereignisquellenserver dem Integratorzertifikat vertraut. Weitere Informationen hierzu finden Sie in der jeweiligen Datenbankdokumentation.

     Für die Option **Streng**:

     - Wenn sich der Sentinel-Link-Integrator im FIPS 140-2-Modus befindet, müssen Sie die Datei `/etc/opt/novell/sentinel/config/sentinel.cer` vom sendenden Sentinel-Computer zum empfangenden Sentinel-Computer kopieren. Importieren Sie das Zertifikat in den Sentinel-FIPS-Keystore des Empfängers.

       HINWEIS: Wenn Sie benutzerdefinierte Zertifikate verwenden, die von einer Zertifizierungsstelle (certificate authority, CA) digital unterzeichnet wurden, müssen Sie die entsprechende benutzerdefinierte Zertifikatsdatei importieren.

     - Wenn sich der Sentinel-Link-Integrator nicht im FIPS-Modus befindet, müssen Sie das benutzerdefinierte Integratorzertifikat in den Sentinel-FIPS-Keystore des Empfängers importieren.

       HINWEIS: Wenn der Empfänger ein Sentinel Log Manager (nicht im FIPS-Modus) und der Empfänger ein Sentinel-System im FIPS 140-2-Modus ist, ist das Serverzertifikat, das am Empfänger importiert werden muss, die Datei `/etc/opt/novell/sentinel/config/sentinel.cer` auf dem empfangenden Sentinel-Computer.

     Wenn Sentinel im FIPS 140-2-Modus ausgeführt wird, können Sie das Client-Zertifikat nicht über die Oberfläche der Ereignisquellenverwaltung (Event Source Management, ESM) importieren. Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

HINWEIS: Im FIPS 140-2-Modus verwendet der Sentinel-Link-Ereignisquellenserver das Sentinel-Server-Schlüsselpaar. Es ist nicht erforderlich, das Server-Schlüsselpaar zu importieren.

Syslog-Connector

Die folgende Prozedur sollten Sie nur durchführen, wenn Sie bei der Konfiguration der Netzwerkeinstellungen am Syslog-Ereignisquellenserver das Protokoll **SSL** ausgewählt haben.

So konfigurieren Sie den Syslog-Connector für den FIPS 140-2-Modus:

1. Fügen Sie den Syslog-Ereignisquellenserver hinzu oder bearbeiten Sie ihn. Fahren Sie mit der Bearbeitung in den Konfigurationsbildschirmen fort, bis das Fenster „Netzwerk“ angezeigt wird. Weitere Informationen finden Sie im *Syslog-Connector-Handbuch*.
2. Klicken Sie auf **Einstellungen**.
3. Wählen Sie eine der Optionen aus dem Feld *Client-Authentifizierungstyp* aus. Der Client-Authentifizierungstyp bestimmt, wie streng der SSL-Syslog-Ereignisquellenserver die Identität der Syslog-Ereignisquellen überprüft, die versuchen, Daten zu senden.
   - **Offen:** Lässt alle SSL-Verbindungen zu, die von den Clients (Ereignisquellen) kommen. Führt keine Validierung oder Authentifizierung des Client-Zertifikats durch.
   - **Streng:** Validiert das Zertifikat als gültiges X.509-Zertifikat und überprüft außerdem, ob der Ereignisquellenserver dem Client-Zertifikat vertraut. Neue Quellen müssen explizit zu Sentinel hinzugefügt werden (wodurch verhindert wird, dass fremde Quellen nicht autorisierte Daten an Sentinel senden).

     Für die Option **Streng** müssen Sie das Zertifikat des Syslog-Clients in den Sentinel-FIPS-Keystore importieren.

     Wenn Sentinel im FIPS 140-2-Modus ausgeführt wird, können Sie das Client-Zertifikat nicht über die Oberfläche der Ereignisquellenverwaltung (Event Source Management, ESM) importieren.

     Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

HINWEIS: Im FIPS 140-2-Modus verwendet der Syslog-Ereignisquellenserver das Sentinel-Server-Schlüsselpaar. Es ist nicht erforderlich, das Server-Schlüsselpaar zu importieren.

---

4. Wenn die Serverauthentifizierung im Syslog-Client aktiviert ist, muss der Client das Zertifikat des Sentinel-Servers oder der Remote-Instanz von Collector Manager (je nachdem, wo der Connector bereitgestellt ist) als verbürgt betrachten.

   Die Zertifikatsdatei des Sentinel-Servers befindet sich unter `/etc/opt/novell/sentinel/config/sentinel.cer`.

   Die Zertifikatsdatei des Remote-Collector-Mangers befindet sich unter `/etc/opt/novell/sentinel/config/rcm.cer`.

HINWEIS: Wenn Sie benutzerdefinierte Zertifikate verwenden, die von einer Zertifizierungsstelle digital unterzeichnet wurden, muss der Client der entsprechenden Zertifikatsdatei vertrauen.

Windows Event (WMI) Connector

So konfigurieren Sie den Windows Event (WMI) Connector für die Ausführung im FIPS 140-2-Modus:

1. Fügen Sie den Windows-Event-Connector hinzu oder bearbeiten Sie ihn. Fahren Sie mit der Bearbeitung in den Konfigurationsbildschirmen fort, bis das Fenster „Sicherheit“ angezeigt wird. Weitere Informationen finden Sie im *Windows Event (WMI) Connector Guide* (Windows Event (WMI) Connector-Handbuch).
2. Klicken Sie auf **Einstellungen**.

3 Wählen Sie eine der Optionen aus dem Feld *Client-Authentifizierungstyp* aus. Der Client-Authentifizierungstyp bestimmt, wie streng der Windows-Event-Connector die Identität der Windows-Ereigniserfassungsdienste (WECS) überprüft, die versuchen, Daten zu senden.

- **Offen:** Lässt alle SSL-Verbindungen zu, die von den Client-WECS kommen. Führt keine Validierung oder Authentifizierung des Client-Zertifikats durch.
- **Streng:** Validiert das Zertifikat als gültiges X.509-Zertifikat und überprüft außerdem, ob das Client-WECS-Zertifikat von der Zertifizierungsstelle unterzeichnet wurde. Neue Quellen müssen explizit hinzugefügt werden (wodurch verhindert wird, dass fremde Quellen Daten an Sentinel senden).

  Für die Option **Streng** müssen Sie das Zertifikat des Client-WECSs in den Sentinel-FIPS-Keystore importieren. Wenn Sentinel im FIPS 140-2-Modus ausgeführt wird, können Sie das Client-Zertifikat nicht über die Oberfläche der Ereignisquellenverwaltung (Event Source Management, ESM) importieren.

  Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

HINWEIS: Im FIPS 140-2-Modus verwendet der Windows-Ereignisquellenserver das Sentinel-Server-Schlüsselpaar. Es ist nicht erforderlich, das Server-Schlüsselpaar zu importieren.

---

4 Wenn die Serverauthentifizierung im Windows-Client aktiviert ist, muss der Client das Zertifikat des Sentinel-Servers oder der Remote-Instanz von Collector Manager (je nachdem, wo der Connector bereitgestellt ist) als verbürgt betrachten.

Die Zertifikatsdatei des Sentinel-Servers befindet sich unter `/etc/opt/novell/sentinel/config/sentinel.cer`.

Die Zertifikatsdatei der Remote-Instanz von Collector Manager befindet sich unter `/etc/opt/novell/sentinel/config/rcm.cer`.

HINWEIS: Wenn Sie benutzerdefinierte Zertifikate verwenden, die von einer Zertifizierungsstelle digital unterzeichnet wurden, muss der Client der entsprechenden Zertifikatsdatei vertrauen.

---

5 Wenn Sie die Ereignisquellen automatisch synchronisieren möchten oder die Liste der Ereignisquellen über eine Active Directory-Verbindung ausgefüllt werden soll, müssen Sie das Active Directory-Serverzertifikat in den Sentinel-FIPS-Keystore importieren.

Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

Sentinel Link Integrator

Die folgende Prozedur sollten Sie nur durchführen, wenn Sie vorher bei der Konfiguration der Netzwerkeinstellungen des Sentinel-Link-Integrators die Option **Verschlüsselt (HTTPS)** ausgewählt haben.

So konfigurieren Sie den Sentinel-Link-Integrator für den FIPS 140-2-Modus:

1 Wenn sich der Sentinel-Link-Integrator im FIPS 140-2-Modus befindet, ist die Serverauthentifizierung obligatorisch. Importieren Sie vor der Konfiguration der Integratorinstanz das Zertifikat des Sentinel-Link-Servers in den Sentinel-FIPS-Keystore:

- **Wenn der Sentinel-Link-Connector im FIPS 140-2-Modus ausgeführt wird**:

  Wenn der Connector auf dem Sentinel-Server bereitgestellt ist, kopieren Sie die Datei `/etc/opt/novell/sentinel/config/sentinel.cer` vom empfangenden Sentinel-Computer zum sendenden Sentinel-Computer.

Wenn der Connector auf einer Collector Manager-Remote-Instanz bereitgestellt ist, kopieren Sie die Datei `/etc/opt/novell/sentinel/config/rcm.cer` vom empfangenden Collector Manager-Remote-Computer zum empfangenden Sentinel-Computer.

Importieren Sie dieses Zertifikat in den FIPS-Keystore des Sentinel-Senders.

HINWEIS: Wenn Sie benutzerdefinierte Zertifikate verwenden, die von einer Zertifizierungsstelle (certificate authority, CA) digital unterzeichnet wurden, müssen Sie die entsprechende benutzerdefinierte Zertifikatsdatei importieren.

- Wenn der Sentinel-Link-Connector im Nicht-FIPS-Modus ausgeführt wird:

  Importieren Sie das benutzerdefinierte Zertifikat des Sentinel-Link-Servers in den sendenden Sentinel-FIPS-Keystore.

HINWEIS: Wenn sich der Sentinel-Link-Integrator im FIPS 140-2-Modus befindet und der Sentinel-Link-Connector im Nicht-FIPS-Modus, müssen Sie das benutzerdefinierte Schlüsselpaar am Connector verwenden. Verwenden Sie nicht das interne Server-Schlüsselpaar.

Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

2 Fahren Sie mit der Konfiguration der Integratorinstanz fort.

HINWEIS: Im FIPS 140-2-Modus verwendet der Sentinel-Link-Integrator das Sentinel-Server-Schlüsselpaar. Es ist nicht erforderlich, das Integrator-Schlüsselpaar zu importieren.

LDAP Integrator

So konfigurieren Sie den LDAP Integrator für den FIPS 140-2-Modus:

1 Laden Sie vor der Konfiguration der Integratorinstanz das Zertifikat vom LDAP-Server herunter und speichern Sie es als Datei `ldap.cert` im Verzeichnis `/etc/opt/novell/sentinel/config` am Sentinel-Server.

Verwenden Sie beispielsweise

```
openssl s_client -connect <LDAP server IP>:636
```

Kopieren Sie anschließend den zurückgegeben Text (zwischen den Zeilen BEGIN und END, doch ohne diese Zeilen) in eine Datei.

2 Importieren Sie das Zertifikat in den Sentinel-FIPS-Keystore.

Informationen zum Importieren des Zertifikats finden Sie im Abschnitt „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 141.

3 Fahren Sie mit der Konfiguration der Integratorinstanz fort.

SMTP Integrator

Der SMTP-Integrator unterstützt FIPS 140-2 ab Version 2011.1r2. Es sind keine Änderungen an der Konfiguration erforderlich.

Syslog-Integrator

Führen Sie die folgende Prozedur nur durch, wenn Sie vorher bei der Konfiguration der Netzwerkeinstellungen des Syslog-Integrators die Option „Encrypted (SSL)“ (Verschlüsselt [SSL]) ausgewählt haben.

So konfigurieren Sie den Syslog-Integrator für den FIPS 140-2-Modus:

1. Wenn sich der Syslog-Integrator im FIPS 140-2-Modus befindet, ist die Serverauthentifizierung obligatorisch. Importieren Sie vor der Konfiguration der Integratorinstanz das Zertifikat des Syslog-Servers in den Sentinel-FIPS-Keystore:

   - **Wenn der Syslog-Connector im FIPS 140-2-Modus ausgeführt wird:** Wenn der Connector auf dem Sentinel-Server bereitgestellt ist, kopieren Sie die Datei `/etc/opt/novell/sentinel/config/sentinel.cer` vom empfangenden Sentinel-Server zum sendenden Sentinel-Server.

     Wenn der Connector auf einer Collector Manager-Remote-Instanz bereitgestellt ist, kopieren Sie die Datei `/etc/opt/novell/sentinel/config/rcm.cer` vom empfangenden Collector Manager-Remote-Computer zum empfangenden Sentinel-Computer.

     Importieren Sie dieses Zertifikat in den FIPS-Keystore des Sentinel-Senders.

     HINWEIS: Wenn Sie benutzerdefinierte Zertifikate verwenden, die von einer Zertifizierungsstelle (certificate authority, CA) digital unterzeichnet wurden, müssen Sie die entsprechende benutzerdefinierte Zertifikatsdatei importieren.

   - **Wenn der Syslog-Connector im Nicht-FIPS-Modus ausgeführt wird:** Importieren Sie das benutzerdefinierte Syslog-Serverzertifikat in den Sentinel-FIPS-Keystore des Senders.

     HINWEIS: Wenn sich der Syslog-Integrator im FIPS 140-2-Modus befindet und der Syslog-Connector im Nicht-FIPS-Modus, müssen Sie das benutzerdefinierte Server-Schlüsselpaar am Connector verwenden. Verwenden Sie nicht das interne Server-Schlüsselpaar.

   So importieren Sie Zertifikate in die FIPS-Keystore-Datenbank:

   1. Kopieren Sie die Zertifikatsdatei an einen temporären Speicherort am Sentinel-Server oder an der Remote-Instanz von Collector Manager.
   2. Navigieren Sie zum Verzeichnis `/opt/novell/sentinel/bin`.
   3. Führen Sie den folgenden Befehl aus, um das Zertifikat in die FIPS-Keystore-Datenbank zu importieren, und befolgen Sie dann die angezeigte Anleitung:

      ```
      ./convert_to_fips.sh -i <certificate file path>
      ```

   4. Geben Sie `yes` (ja) oder `y` ein, wenn Sie aufgefordert werden, den Sentinel-Server oder die Remote-Instanz von Collector Manager neu zu starten.

2. Fahren Sie mit der Konfiguration der Integratorinstanz fort.

HINWEIS: Im FIPS 140-2-Modus verwendet der Syslog-Integrator das Sentinel-Server-Schlüsselpaar. Ein Import des Integrator-Schlüsselpaars ist nicht nötig.

Verwenden von Connectors im Nicht-FIPS-Modus mit Sentinel im FIPS 140-2-Modus

In diesem Abschnitt finden Sie Informationen zur Verwendung von Connectors im Nicht-FIPS-Modus mit einem Sentinel-Server im FIPS 140-2-Modus. Wir empfehlen Ihnen diese Variante, wenn Sie über Quellen verfügen, die FIPS nicht unterstützen oder wenn Sie Ereignisse von Nicht-FIPS-Connectors in Ihrer Umgebung erfassen möchten.

So verwenden Sie Nicht-FIPS-Connectors mit Sentinel im FIPS 140-2-Modus:

1. Installieren Sie einen Collector Manager im Nicht-FIPS-Modus, um eine Verbindung zum Sentinel-Server im FIPS 140-2-Modus herzustellen.

   Weitere Informationen finden Sie unter Teil III, „Installieren von Sentinel“, auf Seite 69.
2. Stellen Sie die Nicht-FIPS-Connectors explizit für die Remote-Instanz von Collector Manager bereit, die sich im Nicht-FIPS-Modus befindet.

HINWEIS: Es sind einige Probleme bekannt, die bei der Bereitstellung von Nicht-FIPS-Connectors wie Audit Connector und File Connector auf einer Nicht-FIPS-Remote-Instanz von Collector Manager, die mit einem Sentinel -Server im FIPS 140-2-Modus verbunden ist, auftreten können. Weitere Informationen zu diesen bekannten Problemen finden Sie in den Versionshinweisen zu Sentinel.

Importieren von Zertifikaten in die FIPS-Keystore-Datenbank

Sie müssen Zertifikate in die Sentinel-FIPS-Keystore-Datenbank einfügen, um zwischen den Komponenten, denen diese Zertifikate gehören, und Sentinel eine sichere (SSL-) Kommunikation aufzubauen. Sie können Zertifikate nicht über die Sentinel-Benutzeroberfläche hochladen, wenn der FIPS 140-2-Modus aktiviert ist. Sie müssen die Zertifikate manuell in die FIPS-Keystore-Datenbank importieren.

Für Ereignisquellen, die Connectors verwenden, die für eine Remote-Instanz von Collector Manager bereitgestellt wurden, müssen Sie die Zertifikate in der FIPS-Keystore-Datenbank der Remote-Instanz von Collector Manager und nicht des zentralen Sentinel-Servers importieren.

So importieren Sie Zertifikate in die FIPS-Keystore-Datenbank:

1. Kopieren Sie die Zertifikatsdatei an einen temporären Speicherort am Sentinel-Server oder an der Remote-Instanz von Collector Manager.
2. Wechseln Sie zum Sentinel-Verzeichnis „bin“. Der Standardspeicherort lautet `/opt/novell/sentinel/bin`.
3. Führen Sie den folgenden Befehl aus, um das Zertifikat in die FIPS-Keystore-Datenbank zu importieren, und befolgen Sie die Anweisungen am Bildschirm:

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```
4. Geben Sie `yes` (ja) oder `y` ein, wenn Sie aufgefordert werden, den Sentinel-Server oder die Remote-Instanz von Collector Manager neu zu starten.

Zurücksetzen von Sentinel in den Nicht-FIPS-Modus

In diesem Abschnitt finden Sie Informationen zum Zurücksetzen von Sentinel und dessen Komponenten in den Nicht-FIPS-Modus.

Zurücksetzen des Sentinel-Servers in den Nicht-FIPS-Modus

Sie können einen Sentinel-Server, der im FIPS 140-2-Modus ausgeführt wird, nur dann in den Nicht-FIPS-Modus zurücksetzen, wenn Sie eine Sicherung des Sentinel-Servers erstellt haben, bevor Sie ihn auf den FIPS140-2-Modus umgestellt haben.

HINWEIS: Wenn Sie einen Sentinel-Server in den Nicht-FIPS-Modus zurücksetzen, gehen die Ereignisse, Vorfalldaten und Konfigurationsänderungen verloren, die an Ihrem Sentinel-Server erfasst oder vorgenommen wurden, nachdem Sie ihn auf den FIPS 140-2-Modus umgestellt haben. Das Sentinel-System wird am letzten Wiederherstellungspunkt des Nicht-FIPS-Modus wiederhergestellt. Sie sollten für die Zukunft eine Sicherung des aktuellen Systems erstellen, bevor Sie es auf den Nicht-FIPS-Modus zurücksetzen.

So setzen Sie Ihren Sentinel-Server in den Nicht-FIPS-Modus zurück:

1. Melden Sie sich beim Sentinel-Server als `root`-Benutzer an.
2. Wechseln Sie zum Benutzer `novell`.
3. Wechseln Sie zum Sentinel-Verzeichnis „bin“. Der Standardspeicherort lautet `/opt/novell/sentinel/bin`.
4. Führen Sie den folgenden Befehl aus, um Ihren Sentinel-Server in den Nicht-FIPS-Modus zurückzusetzen, und befolgen Sie die Anweisungen am Bildschirm:

   ```
   ./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'
   ```

   Wenn die Sicherungsdatei beispielsweise `non-fips20130124191111359034887.tar.gz` lautet, führen Sie den folgenden Befehl aus:

   ```
   ./backup_util.sh -f non-fips20130124191111359034887.tar.gz -m 'restore'
   ```

5. Starten Sie den Sentinel-Server neu.

Zurücksetzen von Remote-Instanzen von Collector Manager oder Correlation Engine in den Nicht-FIPS-Modus

Sie können Remote-Instanzen von Collector Manager oder Correlation Engines in den Nicht-FIPS-Modus zurücksetzen.

So setzen Sie eine Remote-Instanz von Collector Manager oder Correlation Engine in den Nicht-FIPS-Modus zurück:

1. Melden Sie sich beim System der Remote-Instanz von Collector Manager oder Correlation Engine an.

2 Wechseln Sie zum `novell`-Benutzer (`su novell`).

3 Wechseln Sie zum Verzeichnis „bin“: Der Standardspeicherort lautet `/opt/novell/sentinel/bin`.

4 Führen Sie das Skript `revert_to_nonfips.sh` aus und folgen Sie den Anweisungen am Bildschirm.

5 Starten Sie die Remote-Instanz von Collector Manager oder Correlation Engine neu.

25 Banner zum Einholen einer Zustimmung hinzufügen

Sentinel bietet die Möglichkeit, vor der Anmeldung ein Banner zum Einholen einer Zustimmung anzuzeigen. Sie können den Inhalt des Banners je nach Anforderung festlegen. Nachdem Sie das Banner zum Einholen der Zustimmung hinzugefügt haben, müssen bei jeder Anmeldung bei Sentinel die im Banner genannten Bedingungen akzeptiert werden.

So fügen Sie ein Banner zum Einholen der Zustimmung hinzu:

1. Melden Sie sich beim Sentinel-Server als der Benutzer `novell` an.
2. Wechseln Sie zu `/<Sentinel_Installationspfad>/var/opt/novell/sentinel/3rdparty/jetty/webapps/ROOT/siemdownloads`.
3. Fügen Sie eine Textdatei mit dem Namen `USER_AGREEMENT.txt` hinzu.
4. Geben Sie den Text der Benutzerzustimmung ein.
5. Speichern Sie die Datei.
6. Starten Sie Sentinel, um das Banner zum Einholen der Zustimmung anzuzeigen.

Sentinel zeigt nun im Anmeldebildschirm das Banner zum Einholen der Zustimmung an.

HINWEIS: Vor der Aufrüstung von Sentinel muss die Datei `USER_AGREEMENT.txt` manuell gesichert werden.

V Aufrüsten von Sentinel

In diesem Abschnitt finden Sie Informationen zur Aufrüstung von Sentinel und anderen Komponenten.

26 Implementierungs-Checkliste

Überprüfen Sie vor einer Aufrüstung von Sentinel die folgende Checkliste, um eine erfolgreiche Aufrüstung zu gewährleisten:

Tabelle 26-1 *Implementierungs-Checkliste*

❒	Aufgaben	Erklärt in
❒	Stellen Sie sicher, dass die Computer, auf denen Sentinel und dessen Komponenten installiert werden sollen, den angegebenen Anforderungen entsprechen.	Website Sentinel Technical Information (Technische Informationen für Sentinel)
❒	Lesen Sie die Versionshinweise der unterstützten Betriebssysteme, um sich über die bekannten Problemen zu informieren.	SUSE-Versionshinweise
❒	Lesen Sie die Sentinel-Versionshinweise, um sich über die neuen Funktionen und bekannten Probleme zu informieren.	Sentinel-Versionshinweise
❒	Führen Sie die in den Voraussetzungen aufgeführten Aufgaben aus.	Kapitel 27, „Voraussetzungen“, auf Seite 151

27 Voraussetzungen

Speichern von Informationen zu benutzerdefinierten Konfigurationen

Einstellungen der Datei „server.conf“ speichern

Wenn Sie benutzerdefinierte Parameterwerte für die Konfiguration in der Datei `server.conf` festgelegt haben, speichern Sie diese Werte vor der Aufrüstung in getrennten Dateien.

So speichern Sie benutzerdefinierte Konfigurationsinformationen:

1. Melden Sie sich am Sentinel-Server als der Benutzer `novell` an und wechseln Sie zum Verzeichnis `/etc/opt/novell/sentinel/config/`.
2. Erstellen Sie eine Konfigurationsdatei mit dem Namen `server-custom.conf` und fügen Sie die benutzerdefinierten Konfigurationsparameter in dieser Datei hinzu.

Sentinel wendet die in diesen Konfigurationsdateien gespeicherte benutzerdefinierte Konfiguration während der Aufrüstung an.

Einstellungen der Datei „jetty-ssl“ speichern

Sentinel 8.1 enthält eine aktualisierte Version von Jetty. Die aktualisierte Jetty-Version enthält Änderungen an ihrer Dateistruktur.

Wenn Sie die Datei `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml` in früheren Versionen von Sentinel geändert haben, beispielsweise durch Ausschließen von Ciphern, speichern Sie diese Änderungen vor der Aufrüstung von Sentinel in einer separaten Datei.

Kopieren Sie diese Änderungen nach dem Abschluss der Sentinel-Aufrüstung in die Datei `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl-context.xml` und starten Sie Sentinel neu.

Verlängern des Beibehaltungszeitraums für Ereignisverknüpfungsdaten

Ab Sentinel 7.4.4 beträgt der standardmäßige Beibehaltungszeitraum für Ereignisverknüpfungen 14 Tage. Wenn Sie von einer Sentinel-Version unter 7.4.4 aufrüsten, wird der Beibehaltungszeitraum, den Sie für Ereignisverknüpfungsdaten festgelegt hatten, nach der Aufrüstung auf 14 Tage festgelegt. Um dies zu verhindern, können Sie den Beibehaltungszeitraum durch Hinzufügen einer Eigenschaft in die Datei `configuration.properties` auf einen gewünschten Wert festlegen.

Weitere Informationen finden Sie unter „Configuring the Retention Period for the Event Associations Data“ (Konfigurieren des Beibehaltungszeitraums für Ereignisverknüpfungsdaten) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Konfiguration für SSDM vor der Aufrüstung

Während der Aufrüstung werden mit Spark-Anwendungen verknüpfte Dateien aktualisiert. Um die aktualisierten Dateien zu verwenden, muss der Spark-Auftrag neu gestartet und müssen alle Spark-Checkpoints auf Kafka-Themen zurückgesetzt werden. Um einen durch das Zurücksetzen des Kafka-Themen-Checkpoints verursachten Datenverlust zu verhindern, muss das Weiterleiten von Daten von den Collector Manager-Instanzen zu Kafka vor der Aufrüstung von SSDM angehalten werden. Während das Weiterleiten der Daten angehalten ist, werden die Daten in Collector Manager gespeichert, bis das Weiterleiten der Daten fortgesetzt wird. Nachdem die Spark-Anwendung die Daten verarbeitet hat, die vor dem Anhalten des Weiterleitens an Kafka weitergeleitet wurden, kann der Checkpoint ohne Datenverlust zurückgesetzt werden.

So halten Sie die Ereignisweiterleitung von Collector Manager zu Kafka an:

1. Klicken Sie in Sentinel Main auf **Speicher** > **Skalierbarer Speicher** > **Erweiterte Konfiguration** > **Kafka**.
2. Fügen Sie folgende Eigenschaft hinzu und legen Sie sie auf „true“ fest:

   ```
   pause.events.tokafka
   ```
3. Klicken Sie auf **Speichern**.

Change Guardian-Integration

Sentinel ist mit Change Guardian 4.2 und höher kompatibel. Um Ereignisse von Change Guardian empfangen zu können, müssen Sie zunächst den Change Guardian-Server sowie seine Agenten und den Richtlinieneditor auf Version 4.2 oder höher aufrüsten, damit Sentinel auch nach der Aufrüstung weiterhin Ereignisse von Change Guardian empfängt.

28 Aufrüsten einer herkömmlichen Sentinel-Installation

Aufrüsten von Sentinel

Gehen Sie folgendermaßen vor, um den Sentinel-Server aufzurüsten:

1. Sichern Sie die Konfiguration, und erstellen Sie einen ESM-Export.

   Weitere Informationen zum Sichern von Daten finden Sie im Abschnitt „Backing Up and Restoring Data (Sichern und Wiederherstellen von Daten)“ im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).
2. (Bedingt) Wenn Sie die Konfigurationseinstellungen in den Dateien `server.xml`, `collector_mgr.xml` oder `correlation_engine.xml` angepasst haben, müssen Sie auch entsprechende Eigenschaftendateien mit der „obj-component id“ im Namen erstellen, damit die Änderungen auch nach der Aufrüstung wirksam sind. Weitere Informationen finden Sie unter „Maintaining Custom Settings in XML Files“ (Pflegen benutzerdefinierter Einstellungen in XML-Dateien) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).
3. Laden Sie das aktuellste Installationsprogramm von der Download-Website herunter.
4. Melden Sie sich am Server, auf dem Sentinel aufgerüstet werden soll, als `root` an.
5. Geben Sie den folgenden Befehl an, um die Installationsdateien aus der TAR-Datei zu extrahieren:

   ```
   tar xfz <install_filename>
   ```

   Ersetzen Sie *<install_filename>* mit dem tatsächlichen Namen der Installationsdatei.
6. Wechseln Sie in das Verzeichnis, in das die Installationsdatei extrahiert wurde.
7. Geben Sie folgenden Befehl ein, um Sentinel aufzurüsten:

   ```
   ./install-sentinel
   ```
8. Um mit einer Sprache Ihrer Wahl fortzufahren, wählen Sie die neben der gewünschten Sprache angegebene Nummer aus.

   Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.
9. Lesen Sie die Endbenutzer-Lizenzvereinbarung, geben Sie `yes` oder `y` ein, um die Lizenzbedingungen zu akzeptieren, und setzen Sie die Installation fort.
10. Das Installationsskript erkennt, dass bereits eine ältere Produktversion vorhanden ist, und fordert Sie auf, anzugeben, ob Sie das Produkt aufrüsten möchten. Zum Fortsetzen der Aufrüstung drücken Sie „j“.

    Die Installation wird gestartet. Zunächst werden alle RPM-Pakete installiert. Diese Installation kann einige Sekunden dauern.

11 Löschen Sie den Webbrowser-Cache, um die neueste Version von Sentinel anzeigen zu lassen.

12 Löschen Sie den Java Web Start-Cache auf den Clientcomputern, um die neueste Version der Sentinel-Anwendungen zu verwenden.

   Sie können den Java Web Start-Cache mit dem Befehl `javaws -clearcache` oder über das Java Control Center löschen. Weitere Informationen finden Sie unter http://www.java.com/en/download/help/plugin_cache.xml.

13 (Bedingt) Falls die PostgreSQL-Datenbank auf eine höhere Hauptversion aufgerüstet wurde (beispielsweise von 8.0 auf 9.0 oder von 9.0 auf 9.1), löschen Sie die alten PostgreSQL-Dateien aus der PostgreSQL-Datenbank. Weitere Informationen darüber, ob die PostgreSQL-Datenbank aufgerüstet wurde, finden Sie in den Sentinel-Versionshinweisen.

   13a Wechseln Sie zum Benutzer novell.

   ```
   su novell
   ```

   13b Wechseln Sie zum Ordner `bin`:

   ```
   cd /opt/novell/sentinel/3rdparty/postgresql/bin
   ```

   13c Löschen Sie mit folgendem Befehl alle alten PostgreSQL-Dateien:

   ```
   ./delete_old_cluster.sh
   ```

14 Informationen zur Aufrüstung von Collector Manager- und Correlation Engine-Systemen finden Sie unter „Aufrüsten von Collector Manager oder Correlation Engine“, auf Seite 156.

15 (Bedingt) Wenn Sie die Kerberos-Authentifizierung verwenden, aktivieren Sie AES256 in der Java-Laufzeitumgebung, weil der Ordner `java` während der Aufrüstung durch Standarddateien ersetzt wird. Führen Sie die folgenden Schritte aus, um AES256 in der Java-Laufzeitumgebung zu aktivieren:

   15a Laden Sie Java Cryptography Extension (JCE) 8 von der folgenden Adresse herunter: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

   15b Extrahieren Sie die beiden `JAR`-Dateien und kopieren Sie sie in das Verzeichnis `/opt/novell/sentinel/jdk/jre/lib/security`.

   15c (Bedingt) Wenn Sie Sentinel in einer Hochverfügbarkeitsumgebung ausführen, wiederholen Sie diese Schritte für alle Knoten im Cluster.

   15d Starten Sie Sentinel neu.

Aufrüsten von Sentinel mit einem Nicht-root-Benutzer

Wenn Ihre Unternehmensrichtlinie nicht zulässt, dass Sie die gesamte Sentinel-Aufrüstung mit dem Benutzer `root` ausführen, können Sie Sentinel mit einem anderen Benutzer aufrüsten. Bei dieser Aufrüstungsart werden einige wenige Schritte mit dem Benutzer `root` ausgeführt. Anschließend stellen Sie die Sentinel-Aufrüstung mit einem anderen Benutzer fertig, der mit dem Benutzer `root` erstellt wurde.

1 Sichern Sie die Konfiguration, und erstellen Sie einen ESM-Export.

   Weitere Informationen zum Sichern von Daten finden Sie im Abschnitt „Backing Up and Restoring Data“ (Sichern und Wiederherstellen von Daten) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

2 (Bedingt) Wenn Sie die Konfigurationseinstellungen in den Dateien `server.xml`, `collector_mgr.xml` oder `correlation_engine.xml` angepasst haben, müssen Sie auch entsprechende Eigenschaftendateien mit der „obj-component id“ im Namen erstellen, damit die Änderungen auch nach der Aufrüstung wirksam sind. Weitere Informationen finden Sie im Abschnitt „Sichern und Wiederherstellen von Daten“ im *Sentinel -Administrationshandbuch*.

3 Laden Sie die Installationsdateien von der Downloads-Website herunter.

4 Geben Sie in der Befehlszeile den folgenden Befehl ein, um die Installationsdateien aus der TAR-Datei zu extrahieren:

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

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

5 Melden Sie sich am Server, auf dem Sentinel aufgerüstet werden soll, als `root` an.

6 Extrahieren Sie den `squashfs`-RPM aus den Sentinel-Installationsdateien.

7 Installieren Sie `squashfs` auf dem Sentinel-Server.

```
rpm -Uvh <install_filename>
```

8 Geben Sie den folgenden Befehl ein, um zur Anmeldung als der neu erstellte Nicht-Root-Benutzer `novell` zu wechseln: `novell`:

```
su novell
```

9 (Bedingt) So führen Sie eine interaktive Aufrüstung aus:

9a Geben Sie folgenden Befehl ein:

```
./install-sentinel
```

Um Sentinel an einem anderen als dem Standardstandort aufzurüsten, geben Sie zusammen mit dem Befehl die Option „--location“ an. Beispiel:.

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

9b Fahren Sie mit Schritt 11 fort.

10 (Bedingt) Geben Sie folgenden Befehl ein, um eine automatische Aufrüstung auszuführen:

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

Die Installation wird mit den Werten fortgesetzt, die in der Antwortdatei gespeichert sind. Die Sentinel-Aufrüstung ist abgeschlossen.

11 Geben Sie die Nummer der Sprache an, die Sie für die Aufrüstung verwenden möchten.

Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.

12 Lesen Sie die Endbenutzer-Lizenzvereinbarung und geben Sie `yes` oder `y` ein, um die Lizenzbedingungen zu akzeptieren und die Aufrüstung fortzusetzen.

Die Aufrüstung wird gestartet. Zunächst werden alle RPM-Pakete installiert. Diese Installation kann einige Sekunden dauern.

13 Löschen Sie den Webbrowser-Cache, um die neueste Version von Sentinel anzeigen zu lassen.

14 Löschen Sie den Java Web Start-Cache auf den Clientcomputern, um die neueste Version der Sentinel-Anwendungen zu verwenden.

Sie können den Java Web Start-Cache mit dem Befehl `javaws -clearcache` oder über das Java Control Center löschen. Weitere Informationen finden Sie unter http://www.java.com/en/download/help/plugin_cache.xml.

15 (Bedingt) Falls die PostgreSQL-Datenbank auf eine höhere Hauptversion aufgerüstet wurde (beispielsweise von 8.0 auf 9.0 oder von 9.0 auf 9.1), löschen Sie die alten PostgreSQL-Dateien aus der PostgreSQL-Datenbank. Weitere Informationen darüber, ob die PostgreSQL-Datenbank aufgerüstet wurde, finden Sie in den Sentinel-Versionshinweisen.

15a Wechseln Sie zum novell-Benutzer.

```
su novell
```

15b Wechseln Sie zum Ordner `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

15c Löschen Sie mit folgendem Befehl alle alten PostgreSQL-Dateien:

```
./delete_old_cluster.sh
```

16 (Bedingt) Wenn Sie die Kerberos-Authentifizierung verwenden, aktivieren Sie AES256 in der Java-Laufzeitumgebung, weil der Ordner `java` während der Aufrüstung durch Standarddateien ersetzt wird. Führen Sie die folgenden Schritte aus, um AES256 in der Java-Laufzeitumgebung zu aktivieren:

16a Laden Sie Java Cryptography Extension (JCE) 8 von der folgenden Adresse herunter: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

16b Extrahieren Sie die beiden `JAR`-Dateien und kopieren Sie sie in das Verzeichnis `/opt/novell/sentinel/jdk/jre/lib/security`.

16c (Bedingt) Wenn Sie Sentinel in einer Hochverfügbarkeitsumgebung ausführen, wiederholen Sie diese Schritte für alle Knoten im Cluster.

16d Starten Sie Sentinel neu.

Aufrüsten von Collector Manager oder Correlation Engine

Gehen Sie folgendermaßen vor, um den Collector Manager oder die Correlation Engine aufzurüsten:

1 Sichern Sie die Konfiguration, und erstellen Sie einen ESM-Export.

Weitere Informationen finden Sie im Abschnitt „Sichern und Wiederherstellen von Daten“ im *Sentinel -Administrationshandbuch*.

2 Navigieren Sie als Benutzer mit Verwalterfunktion zur **Sentinel Main**-Benutzeroberfläche.

3 Wählen Sie **Downloads** aus.

4 Klicken Sie im Abschnitt zum Collector Manager-Installationsprogramm auf **Download Installer (Installationsprogramm herunterladen)**.

5 Speichern Sie die Installationsdatei auf dem entsprechenden Collector Manager- oder Correlation Engine-Server.

6 Kopieren Sie die Datei an einen temporären Speicherort.

7 Extrahieren Sie den Inhalt der Datei.

8 Führen Sie das folgende Skript aus:

Für den Collector Manager:

```
./install-cm
```

Für die Correlation Engine:

```
./install-ce
```

9 Befolgen Sie die Anweisungen auf dem Bildschirm bis zum Abschluss der Installation.

10 (Bedingt) Führen Sie bei benutzerdefinierten Installationen den folgenden Befehl aus, um die Konfigurationen zwischen Sentinel-Server, Collector Manager und Correlation Engine zu synchronisieren:

```
/opt/novell/sentinel/setup/configure.sh
```

Aufrüsten des Betriebssystems

Diese Sentinel-Version enthält eine Reihe an Befehlen zur Verwendung während der Betriebssystemaufrüstung. Sie sorgen dafür, dass Sentinel danach ordnungsgemäß funktioniert.

HINWEIS: Rüsten Sie zunächst Sentinel auf, ehe Sie das Betriebssystem aufrüsten.

So rüsten Sie Ihr Betriebssystem auf:

1 Melden Sie sich an dem Sentinel-Server, dessen Betriebssystem aufzurüsten ist, als einer der folgenden Benutzertypen an:

- `Root`-Benutzer
- Nicht-root-Benutzer

2 Öffnen Sie eine Eingabeaufforderung und wechseln Sie zu dem Verzeichnis, in das die Sentinel-Installationsdatei extrahiert wurde.

3 Stoppen Sie die Sentinel-Dienste:

```
rcsentinel stop
```

4 (Bedingt) Wenn Sentinel vor der Aufrüstung des Betriebssystems im FIPS-Modus war, müssen die NSS-Datenbankdateien durch Ausführen des folgenden Befehls manuell aufgerüstet werden:

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Befolgen Sie die Anweisungen auf dem Bildschirm, um die NSS-Datenbank aufzurüsten.

Gewähren Sie dem Benutzer `novell` vollständige Berechtigungen für die folgenden Dateien:

```
cert9.db
key4.db
pkcs11.txt
```

5 Rüsten Sie Ihr Betriebssystem auf.

6 (Bedingt) Wenn Sie Mozilla Network Security Services (NSS) 3.29 verwenden, werden die zwei abhängigen RPM-Dateien `libfreebl3-hmac` und `libsoftokn3-hmac` nicht installiert. Installieren Sie die folgenden RPM-Dateien manuell: `libfreebl3-hmac` und `libsoftokn3-hmac`.

7 (Bedingt) Führen Sie für RHEL 7.*x* den folgenden Befehl aus, um zu ermitteln, ob Fehler in der RPM-Datenbank vorliegen:

```
rpm -qa --dbpath <Installationsspeicherort>/rpm | grep novell
```

Beispiel: `# rpm -qa --dbpath /custom/rpm | grep novell`

7a Wenn Fehler auftreten, führen Sie den folgenden Befehl aus, um die Fehler zu beheben:

```
rpm --rebuilddb --dbpath <Installationsspeicherort>/rpm
```

Beispiel: `# rpm --rebuilddb --dbpath /custom/rpm`

7b Führen Sie den in Schritt 7 erwähnten Befehl aus, um sicherzustellen, dass keine Fehler vorliegen.

8 Wiederholen Sie diese Prozedur für:

- Collector Manager-Instanzen
- Correlation Engine-Instanzen
- NetFlow Collector Manager-Instanzen

9 Starten Sie den Sentinel-Dienst neu:

```
rcsentinel restart
```

Dieser Schritt gilt nicht für Sentinel HA.

29 Aufrüsten von Sentinel Appliance

Die in diesem Kapitel beschriebenen Vorgehensweisen führen Sie durch die Aufrüstung von Sentinel Appliance. Sie können wahlweise Sentinel ohne Aufrüstung des SLES-Betriebssystems aufrüsten oder sowohl Sentinel als auch das SLES-Betriebssystem aufrüsten. Da Sentinel 8.2 Appliance nun SLES 12 SP 3 enthält, ist der SLES 11-Aktualisierungskanal nun veraltet. Der Kanal wird entfernt, sobald SUSE die allgemeine Unterstützung für SLES 11 beendet. Sie sollten daher auf Sentinel 8.2 Appliance aufrüsten, die das Betriebssystem SLES 12 SP3 enthält, um weiterhin Aktualisierungen für das Betriebssystem zu erhalten. Rüsten Sie zunächst Sentinel auf, ehe Sie das Betriebssystem aufrüsten.

Aufrüsten von Sentinel

Aufrüsten von Sentinel über den Appliance-Aktualisierungskanal

Sie können Sentinel unter Verwendung von Zypper aufrüsten. Zypper ist ein Befehlszeilenpaketmanager, mit dem Sie eine interaktive Aufrüstung der Appliance ausführen können. In Fällen, in denen zum Abschließen der Aufrüstung eine Benutzerinteraktion erforderlich ist, beispielsweise bei einer Aktualisierung der Endbenutzer-Lizenzvereinbarung, müssen Sie Sentinel Appliance mit Zypper aufrüsten.

So rüsten Sie die Appliance über den Appliance-Aktualisierungskanal auf:

1. Sichern Sie die Konfiguration, und erstellen Sie einen ESM-Export.

   Weitere Informationen finden Sie im Abschnitt „Sichern und Wiederherstellen von Daten“ im *Sentinel -Administrationshandbuch*.

2. (Bedingt) Wenn Sie die Konfigurationseinstellungen in den Dateien `server.xml`, `collector_mgr.xml` oder `correlation_engine.xml` angepasst haben, müssen Sie auch entsprechende Eigenschaftendateien mit der „obj-component id“ im Namen erstellen, damit die Änderungen auch nach der Aufrüstung wirksam sind. Weitere Informationen finden Sie unter „Maintaining Custom Settings in XML Files“ (Pflegen benutzerdefinierter Einstellungen in XML-Dateien) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).

3. Melden Sie sich in der Appliance-Konsole als Benutzer `root` an.

4. Führen Sie den folgenden Befehl aus:

   ```
   /usr/bin/zypper patch
   ```

5. (Bedingt) Wenn das Installationsprogramm meldet, dass Sie eine Abhängigkeit des OpenSSH-Pakets auflösen müssen, geben Sie die entsprechende Option ein, um das OpenSSH-Paket herabzustufen.

6. (Bedingt) Wenn das Installationsprogramm eine Änderung an der ncgOverlay-Architektur meldet, geben Sie die entsprechende Option ein, um die Architekturänderung zu akzeptieren.
7. (Bedingt) Wenn das Installationsprogramm meldet, dass Sie Abhängigkeiten einiger Appliance-Pakete auflösen müssen, geben Sie die entsprechende Option ein, um die abhängigen Pakete zu deinstallieren.
8. Klicken Sie auf `J`, um fortzufahren.
9. Geben Sie `yes` ein, um die Lizenzvereinbarung zu akzeptieren.
10. Starten Sie Sentinel Appliance neu.
11. (Bedingt) Führen Sie den folgenden Befehl aus, wenn Sentinel an einem benutzerdefinierten Port installiert ist oder der Collector Manager oder die Correlation Engine im FIPS-Modus ausgeführt wird:

    ```
    /opt/novell/sentinel/setup/configure.sh
    ```
12. Löschen Sie den Webbrowser-Cache, um die neueste Version von Sentinel anzeigen zu lassen.
13. Löschen Sie den Java Web Start-Cache auf den Clientcomputern, um die neueste Version der Sentinel-Anwendungen zu verwenden.

    Sie können den Java Web Start-Cache mit dem Befehl `javaws -clearcache` oder über das Java Control Center löschen. Weitere Informationen finden Sie unter http://www.java.com/en/download/help/plugin_cache.xml.
14. (Bedingt) Falls die PostgreSQL-Datenbank auf eine höhere Hauptversion aufgerüstet wurde (beispielsweise von 8.0 auf 9.0 oder von 9.0 auf 9.1), löschen Sie die alten PostgreSQL-Dateien aus der PostgreSQL-Datenbank. Weitere Informationen darüber, ob die PostgreSQL-Datenbank aufgerüstet wurde, finden Sie in den Sentinel-Versionshinweisen.

    14a Wechseln Sie zum novell-Benutzer.

    ```
    su novell
    ```

    14b Wechseln Sie zum Ordner `bin`:

    ```
    cd /opt/novell/sentinel/3rdparty/postgresql/bin
    ```

    14c Löschen Sie mit folgendem Befehl alle alten PostgreSQL-Dateien:

    ```
    ./delete_old_cluster.sh
    ```
15. (Bedingt) Befolgen Sie zum Aufrüsten von Collector Manager oder Correlation Engine Schritt 3 bis Schritt 11.
16. (Bedingt) Wenn Sie die Kerberos-Authentifizierung verwenden, aktivieren Sie AES256 in der Java-Laufzeitumgebung, weil der Ordner `java` während der Aufrüstung durch Standarddateien ersetzt wird. Führen Sie die folgenden Schritte aus, um AES256 in der Java-Laufzeitumgebung zu aktivieren:

    16a Laden Sie Java Cryptography Extension (JCE) 8 von der folgenden Adresse herunter: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

    16b Extrahieren Sie die beiden `JAR`-Dateien und kopieren Sie sie in das Verzeichnis `/opt/novell/sentinel/jdk/jre/lib/security`.

    16c Starten Sie Sentinel neu.
17. (Bedingt) Wenn Sie Sentinel in einer Hochverfügbarkeitsumgebung ausführen, wiederholen Sie diese Schritte für alle Knoten im Cluster.

18 (Bedingt) Zum Aufrüsten des Betriebssystems siehe „Aufrüsten des Betriebssystems“, auf Seite 162.

19 Starten Sie Sentinel neu.

Aufrüsten von Sentinel über SMT

In sicheren Umgebungen, in denen die Appliance ohne direkten Internetzugriff ausgeführt werden muss, können Sie die Appliance mit dem Abonnementverwaltungswerkzeug (Subscription Management Tool, SMT) konfigurieren, mit dem Sie die Appliance auf die neuesten verfügbaren Versionen aufrüsten können.

1 Stellen Sie sicher, dass die Appliance mit SMT konfiguriert wurde.

   Weitere Informationen finden Sie unter „Konfigurieren der Appliance mit SMT“, auf Seite 106.

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

   Weitere Informationen finden Sie im Abschnitt „Sichern und Wiederherstellen von Daten“ im *Sentinel -Administrationshandbuch*.

3 (Bedingt) Wenn Sie die Konfigurationseinstellungen in den Dateien `server.xml`, `collector_mgr.xml` oder `correlation_engine.xml` angepasst haben, müssen Sie auch entsprechende Eigenschaftendateien mit der „obj-component id“ im Namen erstellen, damit die Änderungen auch nach der Aufrüstung wirksam sind. Weitere Informationen finden Sie unter „Maintaining Custom Settings in XML Files“ (Pflegen benutzerdefinierter Einstellungen in XML-Dateien) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).

4 Melden Sie sich in der Appliance-Konsole als Benutzer `root` an.

5 Aktualisieren Sie das Repository für die Aufrüstung:

   ```
   zypper ref -s
   ```

6 Überprüfen Sie, ob die Appliance für die Aufrüstung aktiviert ist:

   ```
   zypper lr
   ```

7 (Optional) Überprüfen Sie die verfügbaren Aktualisierungen für die Appliance:

   ```
   zypper lu
   ```

8 (Optional) Überprüfen Sie die Pakete, die die verfügbaren Aktualisierungen für die Appliance beinhalten:

   ```
   zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
   ```

9 Aktualisieren Sie die Appliance:

   ```
   zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
   ```

10 Starten Sie die Appliance neu.

   ```
   rcsentinel restart
   ```

11 (Bedingt) Führen Sie den folgenden Befehl aus, wenn Sentinel an einem benutzerdefinierten Port installiert ist oder der Collector Manager oder die Correlation Engine im FIPS-Modus ausgeführt wird:

   ```
   /opt/novell/sentinel/setup/configure.sh
   ```

12 (Bedingt) Befolgen Sie zum Aufrüsten von Collector Manager oder Correlation Engine Schritt 4 bis Schritt 11.

13 (Bedingt) Wenn Sie die Kerberos-Authentifizierung verwenden, aktivieren Sie AES256 in der Java-Laufzeitumgebung, weil der Ordner `java` während der Aufrüstung durch Standarddateien ersetzt wird. Führen Sie die folgenden Schritte aus, um AES256 in der Java-Laufzeitumgebung zu aktivieren:

13a Laden Sie Java Cryptography Extension (JCE) 8 von der folgenden Adresse herunter: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

13b Extrahieren Sie die beiden `JAR`-Dateien und kopieren Sie sie in das Verzeichnis `/opt/novell/sentinel/jdk/jre/lib/security`.

13c Starten Sie Sentinel neu.

14 (Bedingt) Wenn Sie Sentinel in einer Hochverfügbarkeitsumgebung ausführen, wiederholen Sie diese Schritte für alle Knoten im Cluster.

15 (Bedingt) Zum Aufrüsten des Betriebssystems siehe „Aufrüsten des Betriebssystems“, auf Seite 162.

16 Starten Sie Sentinel neu.

Aufrüsten des Betriebssystems

Nach der Aufrüstung von Sentinel müssen Sie das Betriebssystem aufrüsten. Nachdem Sie das Betriebssystem aufgerüstet haben, müssen Sie die Appliance konfigurieren, um die neuen Funktionen von Sentinel Appliance Manager zu nutzen. Sentinel Appliance Manager bietet eine einfache Weboberfläche zur Konfiguration und Verwaltung der Appliance. Sie ersetzt die vorhandene WebYast-Funktionalität.

So rüsten Sie das Betriebssystem auf und konfigurieren die Appliance:

1 Rüsten Sie Sentinel auf. Weitere Informationen finden Sie unter „Aufrüsten von Sentinel“, auf Seite 159.

2 Stoppen Sie die Sentinel-Dienste:

```
rcsentinel stop
```

3 (Bedingt) Wenn Sentinel vor der Aufrüstung des Betriebssystems im FIPS-Modus war, müssen die NSS-Datenbankdateien durch Ausführen des folgenden Befehls manuell aufgerüstet werden:

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Befolgen Sie die Anweisungen auf dem Bildschirm, um die NSS-Datenbank aufzurüsten.

Gewähren Sie dem Benutzer `novell` vollständige Berechtigungen für die folgenden Dateien:

```
cert9.db
key4.db
pkcs11.txt
```

4 (Bedingt) Wenn Sie Mozilla Network Security Services (NSS) 3.29 verwenden, werden die zwei abhängigen RPM-Dateien `libfreebl3-hmac` und `libsoftokn3-hmac` nicht installiert. Installieren Sie die folgenden RPM-Dateien manuell: `libfreebl3-hmac` und `libsoftokn3-hmac`.

5 Laden Sie das Installationsprogramm für SLES 12 SP3 und das Dienstprogramm für nach der Aufrüstung von der Website Micro Focus Patch Finder herunter. Laden Sie für Sentinel als Hochverfügbarkeitsbereitstellung ebenfalls die Datei für die Hochverfügbarkeitsversion von SLES 12 SP3 herunter.

6 Befolgen Sie zum Aufrüsten des Betriebssystems die Aufforderungen im Installationsprogramm. Wenn Sie für die Hochverfügbarkeitsbereitstellung von Sentinel aufgefordert werden, Zusatzprodukte zu installieren, wählen Sie den Speicherort aus, in den Sie die Hochverfügbarkeitsdatei von SLES 12 SP3 heruntergeladen haben, und fahren Sie mit der Aufrüstung fort..

   Weitere Informationen zum Aufrüsten auf SLES 12 SP3 finden Sie in der SLES-Dokumentation.

7 Während des Aufrüstungsvorgangs benennt SLES die Datei `/etc/sysctl.conf` als Sicherung in `/etc/sysctl.conf.rpmsave` um und erstellt eine neue Datei `/etc/sysctl.conf`. Kopieren Sie nach der Aufrüstung den Inhalt der Datei `/etc/sysctl.conf.rpmsave` in die Datei `/etc/sysctl.conf`. Öffnen Sie die Datei `sysctl.conf` und suchen Sie die Zeichenfolge `# Added by sentinel vm.max_map_count`. Verschieben Sie diese Einstellung wie folgt in die nächste Zeile:

   Änderung

   ```
   net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count : 65530
   vm.max_map_count = 262144
   ```

   in

   ```
   net.core.wmem_max = 67108864
   # Added by sentinel vm.max_map_count : 65530
   vm.max_map_count = 262144
   ```

8 (Bedingt) Führen Sie für Hochverfügbarkeitsbereitstellungen von Sentinel die in den folgenden Abschnitten erläuterten Schritte aus:

   - „Konfigurieren von iSCSI-Zielen“, auf Seite 218
   - „Konfigurieren von iSCSI-Initiatoren“, auf Seite 219
   - „Konfigurieren des HA-Clusters“, auf Seite 220

9 Führen Sie zum Konfigurieren der Appliance über die Eingabeaufforderung das Dienstprogramm für nach der Aufrüstung aus:

   9a Entpacken Sie die Datei:

   `tar -xvf <`*`Dateiname des Installationsprogramms für das Dienstprogramm für nach der Aufrüstung`*`>.tar.gz`

   9b Wechseln Sie in das Verzeichnis, in das Sie das Dienstprogramm extrahiert haben:

   `cd <`*`Dateiname des Installationsprogramms für das Dienstprogramm für nach der Aufrüstung`*`>`

   9c Führen Sie zum Konfigurieren der Appliance das folgende Skript aus:

   `./appliance_SLESISO_post_upgrade.sh`

   HINWEIS: Führen Sie dieses Skript nicht remote aus, weil es eine Neukonfiguration des Netzwerks enthält.

   9d Befolgen Sie die Anweisungen auf dem Bildschirm, um die Konfiguration zu beenden.

   Das Skript konfiguriert die installierten Pakete neu und konfiguriert die Pakete zum Verwalten der Appliance.

10 Registrieren Sie sich mit Ihrem vorhandenen Registrierungscode erneut zum Erhalt von Aktualisierungen, um die neuesten Aktualisierungen für Sentinel und das Betriebssystem zu erhalten. Weitere Informationen finden Sie unter „Registrieren für Aktualisierungen“, auf Seite 104.

30 Konfiguration nach der Aufrüstung

Dieses Kapitel stellt die Konfigurationen nach der Aufrüstung vor.

Sichern von Daten in Elasticsearch

Sentinel nutzt Kibana, ein browserbasiertes Analyse- und Such-Dashboard, mit dem Sie Ereignisse und Warnmeldungen in Dashboards grafisch darstellen können. Sentinel speichert und indexiert Warnmeldungen in Elasticsearch. Sie können Sentinel so konfigurieren, dass auch die Ereignisse in Elasticsearch gespeichert und indexiert werden, um die Ereignisgrafikfunktion voll auszunutzen. Sentinel-Dashboards greifen auf Daten von Elasticsearch zu, um Ereignisse und Warnmeldungen in Dashboards zu präsentieren. Um sicherzustellen, dass in den Dashboards nur Daten angezeigt werden, zu deren Anzeige die Rolle des Benutzers berechtigt ist, und um den unbefugten Zugriff auf Daten in Elasticsearch zu vermeiden, müssen Sie das Elasticsearch-Sicherheits-Plugin installieren. Weitere Informationen finden Sie unter „Sichern von Daten in Elasticsearch“, auf Seite 77.

Ereignisgrafiken konfigurieren

Sentinel stellt Ereignisgrafiken bereit, die Daten in Diagrammen, Tabellen und Karten präsentieren. Diese Grafiken erleichtern die grafische Anzeige und Analyse großer Datenmengen, wie Ereignisse, IP-Flussereignisse und Warnmeldungen. Sie können auch eigene Ereignisgrafiken und Dashboards erstellen.

Sentinel nutzt Kibana, ein browserbasiertes Analyse- und Such-Dashboard, mit dem Sie Ereignisse suchen und grafisch präsentieren können. Kibana greift über den Grafikdatenspeicher (Elasticsearch) auf Daten zu, um die Ereignisse in Dashboards anzuzeigen. Standardmäßig enthält Sentinel einen Elasticsearch-Knoten. Sie müssen die Ereignisgrafikfunktion aktivieren, um Ereignisse in Elasticsearch zu speichern und zu indexieren. Weitere Informationen finden Sie unter „Grafikdatenspeicher konfigurieren“, auf Seite 43.

HINWEIS: Einige der Sentinel-Dashboards, die Kibana nutzen, werden nach dem Aufrüsten auf Sentinel 8.2 nicht geladen. Dieses Problem tritt auf, weil die Versionen von Elasticsearch und Kibana in Sentinel 8.2 aufgerüstet wurden und die vorhandene Kibana-Indexdatei nicht mit den

aufgerüsteten Versionen von Elasticsearch und Kibana kompatibel ist. Zum Beheben dieses Problems müssen Sie die vorhandene Kibana-Indexdatei manuell löschen und eine neue Kibana-Indexdatei erstellen. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7022736.

Erfassung von IP-Flussdaten konfigurieren

Sentinel nutzt nun ArcSight SmartConnectors, mit denen Sie Ihr Unternehmensnetzwerk besser überwachen können, indem Sie neben NetFlow-Daten auch IP-Flussdaten erfassen. SmartConnectors erfassen IP-Flussdaten als Ereignisse. Dies bietet folgende Vorteile:

- Sie können vorhandene Collector Manager-Instanzen zum Erfassen von IP-Flussdaten verwenden. Sie benötigen keine NetFlow Collector Manager-Instanzen mehr zum Erfassen von NetFlow-Daten.
- Sie können IP-Flussdaten in verschiedenen Bereichen von Sentinel nutzen, zum Beispiel in den Bereichen Ereignisgrafik, Ereignis-Routing, Datenverbund, Berichte und Korrelation.
- Sie können Datenbeibehaltungsrichtlinien auf IP-Flussdaten anwenden und die Daten so für die gewünschte Dauer speichern.

Nach der Aufrüstung von Sentinel können Sie entweder weiterhin die NetFlow-Funktionen nutzen oder die Erfassung von IP-Flussdaten konfigurieren. Seitdem die Funktionen für die Erfassung von IP-Flussdaten und deren Anzeige in Ereignisgrafiken verfügbar ist, werden die früheren NetFlow-Funktionen einschließlich NetFlow-Ansichten jedoch als veraltet betrachtet und werden in Zukunft zur Verbesserung des Benutzererlebnisses entfernt.

Nachdem die Erfassung der IP-Flussdaten aktiviert ist, gilt Folgendes:

- IP-Flussdaten werden als Ereignisse erfasst und daher im EPS-Wert berücksichtigt.
- NetFlow-Daten, die vor dem Aktivieren der Erfassung von IP-Flussdaten erfasst wurden, gehen verloren. Das veraltete NetFlow-System bietet eine maximale Beibehaltungsdauer von 3 Tagen. Sie können die IP-Flussereignisse beliebig lange beibehalten.
- NetFlow-Daten, die vor dem Aktivieren der Erfassung von IP-Flussdaten erfasst wurden, können nicht zur IP-Flussfunktion migriert werden.
- Die einzige Möglichkeit, diese Konfiguration rückgängig zu machen, besteht in der Neuinstallation von Sentinel.
- Sie werden von Sentinel Main abgemeldet und müssen sich neu anmelden.

So konfigurieren Sie die Erfassung von IP-Flussdaten:

1. Installieren und konfigurieren Sie ArcSight SmartConnector. Achten Sie bei der Konfiguration darauf, die relevanten SmartConnectors zum Erfassen von IP-Flussdaten zu konfigurieren.

   Informationen über das Konfigurieren von SmartConnectors finden Sie in der Dokumentation zu Universal Common Event Format Collector auf der Website für Sentinel-Plugins.
2. Wählen Sie in **Sentinel Main** > **Erfassung** > **IP-Fluss** den Eintrag **IP-Flussdaten erfassen** aus und klicken Sie dann auf **Aktivieren**.

HINWEIS: Da IP-Flussereignisse jetzt an Collector Manager gesendet werden, benötigen Sie keine NetFlow Collector Manager-Instanzen mehr. Vorhandene NetFlow Collector Manager-Instanzen können Sie daher deinstallieren. Weitere Informationen finden Sie unter „Deinstallieren von NetFlow Collector Manager“, auf Seite 235.

Konfiguration für den skalierbaren Datenmanager von Sentinel nach der Aufrüstung

Elasticsearch-Sicherheits-Plugin installieren

Zusätzlich zu externen Elasticsearch-Knoten enthält Sentinel jetzt standardmäßig einen lokalen Elasticsearch-Knoten für die Datengrafiken. Sie müssen deshalb ein Elasticsearch-Plugin für das lokale Elasticsearch installieren. Weitere Informationen finden Sie unter „Installieren des Elasticsearch-Sicherheits-Plugins“, auf Seite 78.

Da Elasticsearch und Kibana in Sentinel aufgerüstet wurden, müssen alle Elasticsearch-Sicherheits-Plugins in den vorhandenen Elasticsearch-Knoten neu bereitstellen. Weitere Informationen über das neue Bereitstellen des Elasticsearch-Sicherheits-Plugins finden Sie in „Elasticsearch-Sicherheits-Plugin neu bereitstellen“, auf Seite 82.

Aktualisieren von Spark-Anwendungen unter YARN

Während der Sentinel-Aufrüstung werden auch einige Spark-Anwendungsdateien aktualisiert. Sie müssen die SparkAnwendungen mit diesen aktualisierten Dateien neu übertragen, indem Sie die folgenden Schritte ausführen:

1. Melden Sie sich mit dem Benutzer `novell` beim SSDM-Server an und kopieren Sie die Dateien auf den Spark-Verlaufsserver, auf dem HDFS NameNode installiert ist:

   ```
   cd /etc/opt/novell/sentinel/scalablestore
   ```

   ```
   scp SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties
   log4j.properties manage_spark_jobs.sh root@<hdfs_node>:<Zielverzeichnis>
   ```

   <*Zielverzeichnis*> ist ein beliebiges Verzeichnis, in dem Sie die kopierten Dateien ablegen möchten. Stellen Sie außerdem sicher, dass der Benutzer `hdfs` vollständige Berechtigungen für dieses Verzeichnis hat.

2. Melden Sie sich als root-Benutzer beim <*hdfs_node*>-Server an und ändern Sie die Eigentümerschaft der kopierten Dateien in den Benutzer `hdfs`:

   ```
   cd <Zielverzeichnis>
   ```

   ```
   chown hdfs SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties
   log4j.properties manage_spark_jobs.sh
   ```

   Weisen Sie dem Skript `manage_spark_jobs.sh` die Berechtigung zum Ausführen zu.

3. Vergewissern Sie sich, dass die Spark-Aufträge die Verarbeitung aller Daten abgeschlossen haben:

   Wechseln Sie zur YARN ResourceManager-Weboberfläche und zeigen Sie jede Sentinel Spark-Anwendung an. Die Spark-Streaming-Anwendungsdaten zeigen eine auf null abfallende Eingangsrate, wenn alle Daten von Kafka verarbeitet wurden.

4. Führen Sie folgenden Befehl aus, um die Datenverarbeitung zu stoppen:

   ```
   ./manage_spark_jobs.sh stop
   ```

5. Löschen Sie den Datenverarbeitungs-Checkpoint:

```
sudo -u hdfs hadoop fs -rm -R -skipTrash  /spark/checkpoint
```

`/spark/checkpoint` ist das Checkpoint-Verzeichnis.

6 Führen Sie das folgende Skript aus, um die Spark-Aufträge neu zu senden:

```
./manage_spark_jobs.sh start
```

Es dauert eine Weile, bis der Befehl oben den Absendevorgang abgeschlossen hat.

7 (Bedingt) Führen Sie den folgenden Befehl aus, um den Status der gesendeten Spark-Aufträge zu überprüfen:

```
./manage_spark_jobs.sh status
```

8 Nehmen Sie die Ereignisweiterleitung zu Kafka wieder auf, damit Spark mit der Verarbeitung der Ereignisse beginnt:

8a Klicken Sie in Sentinel Main auf **Speicher** > **Skalierbarer Speicher** > **Erweiterte Konfiguration** > **Kafka**.

8b Legen Sie die folgende Eigenschaft auf „falsch“ fest:

```
pause.events.tokafka
```

8c Klicken Sie auf **Speichern**.

Aktivieren der Sentinel-Funktionen

Wenn Sie von SSDM 8.0.*x.x* aufrüsten, sind einige Sentinel-Funktionen, die in Sentinel 8.1 oder höher hinzugefügt wurden, standardmäßig nicht verfügbar. Sie müssen diese Funktionen manuell in der Datei `/etc/opt/novell/sentinel/config/ui-configuration.properties` aktivieren.

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

2 Öffnen Sie die Datei `/etc/opt/novell/sentinel/config/ui-configuration.properties`.

3 Ändern Sie die folgenden Eigenschaften auf den Wert „falsch“:

```
alerts.hideUI
solutionDesigner.launcher.hideUI
correlation.hideUI
scc.configurations.solutionPacks.hideUI
people.hideUI
permission.knowledgeBase.hideUI
scc.menuBarItem.toolsMenu.hideUI
scc.toolBarItem.peopleBrowser.hideUI
integration.hideUI
```

4 Aktualisieren Sie den Sentinel-Browser.

Aktualisieren von Dashboards und Visualisierungen im SSDM

Nach dem Aufrüsten des skalierbaren Datenmanagers von Sentinel (Sentinel Scalable Data Manager, SSDM) müssen die Dashboards und Grafiken aktualisiert werden, damit die entsprechenden Verbesserungen der neuesten Version angewendet werden.

Beim Aufrüsten von SSDM werden Dashboards und Visualisierungen nicht standardmäßig aktualisiert. Allerdings lassen sie sich nach dem Aufrüsten manuell aktualisieren. Löschen Sie dazu die vorhandenen Dashboards und Visualisierungen und führen Sie das Skript `load_kibana_data.sh` aus. Daraufhin werden die neuesten Dashboards und Visualisierungen installiert.

WICHTIG: Bei der Aktualisierung gehen jegliche Anpassungen Ihrer Dashboards und Visualisierungen verloren.

So aktualisieren Sie Dashboards und Visualisierungen:

1. Melden Sie sich an der SSDM-Weboberfläche an und navigieren Sie zu „Event Visualization“ (Ereignisvisualisierung).
2. Unter „Event Visualization“ (Ereignisvisualisierung) navigieren Sie zu **Settings** > **Objects** > **Dashboards** (Einstellungen > Objekte > Dashboards).
3. Wählen Sie die zu aktualisierenden Dashboards aus und klicken Sie auf **Löschen**.
4. Klicken Sie auf **Visualizations** (Visualisierungen). Wählen Sie die zu aktualisierenden Visualisierungen aus und klicken Sie auf **Löschen**.
5. Melden Sie sich an der SSDM-Weboberfläche ab.
6. Melden Sie sich beim SSDM-Server als der Benutzer `novell` an.
7. Navigieren Sie zum Verzeichnis `/opt/novell/sentinel/bin`.
8. Führen Sie mit folgendem Befehl `load_kibana_data.sh` aus:

   ```
   ./load_kibana_data.sh http://<IP-Adresse>:<Port>> <alerts/events/misc>
   ```

   Beispiel:

   ```
   ./load_kibana_data.sh http://127.0.0.1:9200 alerts
   ./load_kibana_data.sh http://127.0.0.1:9200 events
   ```
9. Melden Sie sich bei der SSDM-Weboberfläche an und navigieren Sie zu „Event Visualization“ (Ereignisvisualisierung), um die aktualisierten Dashboards und Visualisierungen anzuzeigen.

Hinzufügen des JDBC DB2-Treibers

Fügen Sie nach der Aufrüstung von Sentinel den richtigen JDBC-Treiber hinzu und konfigurieren Sie ihn für die Datenerfassung und Datensynchronisierung. Führen Sie dazu die folgenden Schritte aus:

1. Kopieren Sie die richtige Version des IBM DB2 JDBC-Treibers (`db2jcc-*.jar`) für Ihre DB2-Datenbankversion in den Ordner `/opt/novell/sentinel/lib`.
2. Achten Sie darauf, die erforderliche Eigentümerschaft und die erforderlichen Berechtigungen für die Treiberdatei festzulegen.
3. Konfigurieren Sie diesen Treiber für die Datenerfassung. Weitere Informationen finden Sie in der Datenbank-Connector-Dokumentation.

Konfiguration von Datenverbundeigenschaften in Sentinel Appliance

Führen Sie nach der Aufrüstung von Sentinel Appliance folgende Schritte aus, damit die Datenverbundfunktion keine Fehler in Umgebungen anzeigt, in denen zwei oder mehr NICs konfiguriert sind:

1. Fügen Sie auf dem autorisierten Requester-Server die folgende Eigenschaft in die Datei `/etc/opt/novell/sentinel/config/configuration.properties` ein:

   ```
   sentinel.distsearch.console.ip=<eine IP-Adresse des autorisierten Requesters>
   ```

2 Fügen Sie auf dem Datenquellenserver die folgende Eigenschaft in die Datei `/etc/opt/novell/sentinel/config/configuration.properties` ein:

   ```
   sentinel.distsearch.target.ip=<eine IP-Adresse der Datenquelle>
   ```

3 Starten Sie Sentinel neu:

   ```
   rcsentinel restart
   ```

4 Melden Sie sich beim autorisierten Requester-Server an, und klicken Sie auf Integration. Wenn die hinzuzufügende Datenquelle bereits vorhanden ist, löschen Sie die Datenquelle, und fügen Sie sie mit einer der in Schritt 2 angegebenen IP-Adressen wieder hinzu.

   Fügen Sie ggf. auch autorisierte Requester mit den in Schritt 1 angegebenen IP-Adressen hinzu.

Sentinel Appliance für Aktualisierungen registrieren

Wenn Sie das Betriebssystem aufgerüstet haben, müssen Sie Sentinel Appliance neu registrieren, um Aktualisierungen für Sentinel und die neuesten Betriebssystemaktualisierungen zu erhalten. Sie können Ihren vorhandenen Registrierungsschlüssel für die erneute Registrierung zum Erhalt von Aktualisierungen verwenden. Informationen zur Registrierung der Appliance finden Sie in „Registrieren für Aktualisierungen“, auf Seite 104.

Aktualisieren externer Datenbanken zur Datensynchronisierung

Seit Sentinel 8.x erlaubt das Ereignisfeld `Message (msg)` (Nachricht) 8.000 statt 4.000 Zeichen, um Platz für mehr Informationen zu schaffen.

Wenn Sie in einer früheren Sentinel-Version eine Datensynchronisierungsrichtlinie erstellt haben, durch die das Ereignisfeld „Message (msg)“ (Nachricht) mit einer externen Datenbank synchronisiert wird, müssen Sie die Größe der entsprechend zugeordneten Spalte der externen Datenbank entsprechend anpassen.

HINWEIS: Der obige Schritt ist nur erforderlich, wenn Sie frühere Sentinel-Versionen auf Version 8.x aufrüsten.

Sentinel im Mehr-Faktor-Authentifizierungsmodus neu authentifizieren

Wenn Sie den Sentinel-Server im MFA-Modus aufrüsten, werden vorhandene NetFlow Collector Manager-Instanzen nicht automatisch neu am Sentinel-Server authentifiziert. Führen Sie die folgenden Schritte aus, um die NetFlow Collector Manager-Instanzen manuell neu am Sentinel-Server zu authentifizieren.

So authentifizieren Sie Sentinel im MFA-Modus neu:

1 Melden Sie sich beim Computer der NetFlow Collector Manager-Instanz an.

2 Wechseln Sie zu `/opt/novell/sentinel/setup`.

3 Führen Sie das Skript `configure.sh` aus.

   Sie werden zur Anmeldung am Sentinel-Server aufgefordert.

4 Geben Sie Ihren LDAP-Benutzernamen und das zugehörige Passwort an.

5 Geben Sie die Sentinel-Client-ID und das Sentinel-Client-Geheimnis an.

Öffnen Sie die folgende URL, um die Sentinel-Client-ID und das Sentinel-Clientgeheimnis abzurufen:

`https://Sentinel_FQDN:port/SentinelAuthServices/oauth/clients`

Hierbei gilt:

- `Sentinel_FQDN` ist der vollständig qualifizierte Domänenname des Sentinel-Servers.

  Beispiel: `abc.netiq.com`

  `abc` seht für den Hostnamen des Sentinel-Servers und `netiq.com` ist der Domänenname.
- `Port` ist der von Sentinel verwendete Port (üblicherweise 8443).

Die angegebene URL verwendet zum Abrufen der Sentinel-Client-ID und des Sentinel-Clientgeheimnisses Ihre aktuelle Sentinel-Sitzung.

31 Aufrüsten von Sentinel-Plugins

Die Aufrüstinstallationen von Sentinel rüsten nicht die Plugins auf, es sei denn, ein bestimmtes Plugin ist nicht mit der neuesten Version von Sentinel kompatibel.

Neue und aktualisierte Sentinel-Plugins, auch Lösungspakete, werden regelmäßig auf die Website für Sentinel-Plugins hochgeladen. Laden Sie die aktuellste Version eines Plugins herunter, um die neuesten Fehlerbehebungen, Dokumentationsaktualisierungen und Verbesserungen für das entsprechende Plugin zu erhalten. Informationen zur Installation eines Plugins finden Sie in der Dokumentation für das jeweilige Plugin.

VI Migrieren von Daten vom herkömmlichen Speicher

Durch das Migrieren von Daten von Sentinel mit herkömmlichem Speicher können Sie vorhandene Sentinel-Daten und den bereits geleisteten Arbeitsaufwand nutzen. Um Daten von Sentinel mit herkömmlichem Speicher zu migrieren, müssen die Sentinel-Versionen des Sentinel-Ursprungsservers und des Sentinel-Zielservers übereinstimmen. Wenn Sie beispielsweise Daten von Sentinel 8.1 (Ursprung) zu Sentinel 8.2 (Ziel) migrieren möchten, müssen Sie zuerst Sentinel 8.1 auf Sentinel 8.2 aufrüsten. Anschließend können Sie den Datenmigrationsvorgang starten.

Dieser Abschnitt enthält Informationen über das Migrieren von vorhandenen Daten zur gewünschten Datenspeicherkomponente.

32 Migrieren von Daten zum skalierbaren Speicher

Die Migration kann von einem einzelnen oder von mehreren Sentinel-Servern mit herkömmlichem Speicher erfolgen. Der zu befolgende Datenmigrationsvorgang hängt davon ab, wie Sie die Sentinel-Bereitstellung einrichten und pflegen möchten.

Tabelle 32-1 *Datenmigrationsvorgang für Ihre Sentinel-Bereitstellung*

Sentinel-Bereitstellung	Migrationsvorgang
Sie haben einen einzelnen Sentinel-Server und möchten diesen auf einen skalierbaren Speicher aufrüsten.	Migrieren Sie die Ereignisdaten und die Rohdaten vom herkömmlichen Speicher zum skalierbaren Speicher, nachdem Sie den Sentinel-Server aufgerüstet und den skalierbaren Speicher aktiviert haben. Weitere Informationen finden Sie unter Kapitel 34, „Migrieren von Daten“, auf Seite 185.
Sie haben einen einzelnen Sentinel-Server mit herkömmlichem Speicher und möchten einen weiteren Sentinel-Server einrichten, der mit einem skalierbaren Speicher arbeitet, um auf diese Weise alle Funktionen von Sentinel nutzen zu können.	Verwenden Sie zum Migrieren der Daten von Sentinel mit herkömmlichem Speicher zu Sentinel mit skalierbarem Speicher das Sicherungs- und Wiederherstellungsprogramm. Weitere Informationen zur Verwendung des Sicherungs- und Wiederherstellungsprogramms finden Sie unter „Backing Up and Restoring Data“ (Sichern und Wiederherstellen von Daten) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Sentinel-Bereitstellung	Migrationsvorgang
Sie verfügen über eine mehrschichtige Einrichtung mit mehreren Sentinel-Servern und planen, einen neuen Sentinel-Server oder einen der vorhandenen Server für einen skalierbaren Speicher zu verwenden. Neben den Ereignisdaten und Rohdaten müssen Sie Konfigurationsdaten migrieren.	In einer mehrschichtigen Einrichtung können Sie einen der herkömmlichen Sentinel-Server auswählen, der den größten Teil der Daten enthält, und die Daten mithilfe des Sicherungs- und Wiederherstellungsprogramms migrieren. Wenn Sie Daten von den anderen Sentinel-Servern sichern möchten, müssen Sie die Konfigurationsdaten, Ereignisdaten und Rohdaten von diesen Servern mit einem anderen Verfahren migrieren. Dies wird weiter unten in diesem Abschnitt beschrieben. Außerdem muss ein Teil der Konfigurationen manuell neu erstellt werden. Es ist nicht möglich, Daten von mehreren Servern mit dem Sicherungs- und Wiederherstellungsprogramm zu migrieren, weil dieses Dienstprogramm beim Wiederherstellen die vorhandenen Daten jeweils überschreibt. Wenn Sie beispielsweise bereits Daten von Server A wiederhergestellt haben und dann versuchen, Daten von Server B wiederherzustellen, überschreibt das Dienstprogramm dabei die bereits von Server A wiederhergestellten Daten. Befolgen Sie daher zur Berücksichtigung des anwendbaren Datenmigrationsvorgangs die Anweisungen in den folgenden Abschnitten in der angegeben Reihenfolge: ◆ Migrationsfähige Daten ◆ Migrieren von Konfigurationsdaten ◆ Migrieren von Daten ◆ Migrieren von Warnmeldungen und NetFlow-Daten ◆ Aktualisieren der Sentinel-Clients ◆ Importieren der ESM-Konfiguration

Migrationsfähige Daten

Sie können Ereignisdaten, Rohdaten und bestimmte Konfigurationsdaten migrieren. Gewisse Konfigurationsdaten können nicht migriert werden und müssen manuell neu erstellt werden.

Tabelle 32-2 Migrationsfähige Konfigurationsdaten und neu zu erstellende Konfigurationsdaten

Migrationsfähige Konfigurationsdaten	Manuell neu zu erstellende Konfigurationsdaten
◆ Korrelationsregeln ◆ Aktionen ◆ Zuordnungen ◆ Filter ◆ Bedrohungs-Feeds ◆ ESM-Konfiguration ◆ Warnmeldungen außer Knowledgebase-Daten ◆ NetFlow	◆ Mandanten, Rollen, Benutzer und LDAP-Konfiguration ◆ Routing-Regeln für Ereignisse und Warnmeldungen ◆ Beibehaltungsrichtlinien für Daten und Warnmeldungen ◆ Dashboards ◆ Echtzeitansichten ◆ Identitätsinformationen ◆ Konfiguration der Feeds ◆ Konfiguration der Aktions- und Integrator-Plugins ◆ Sicherheitskonfiguration

Migrieren von Konfigurationsdaten

Vor der Migration der Ereignisdaten müssen Sie zuerst die Konfigurationsdaten auf den Sentinel-Zielserver migrieren. Bestimmte Konfigurationsdaten lassen sich mit Solution Designer und den Export- und Importoptionen in der Ereignisquellenverwaltung (ESM) sichern. Die verbleibenden Konfigurationsdaten können nicht gesichert oder exportiert werden und müssen manuell neu erstellt werden.

- „Sichern von Daten auf dem Ursprungsserver“, auf Seite 179
- „Wiederherstellen von Daten auf dem Zielserver“, auf Seite 180

Sichern von Daten auf dem Ursprungsserver

Sie müssen die erforderlichen Daten mit den verschiedenen Optionen in Sentinel sichern.

- „Verwenden von Lösungspaketen“, auf Seite 180
- „Verwenden der Option zum Exportieren der Konfiguration in ESM“, auf Seite 180

Verwenden von Lösungspaketen

Sichern Sie die folgenden Konfigurationsdaten auf dem Ursprungsserver mithilfe von Solution Designer:

Tabelle 32-3 *Konfigurationsdaten*

	Daten	Anmerkungen
❒	Korrelationsregeln	Erstellen Sie separate Steuerungen für jede Correlation Engine-Instanz, damit Sie die Regeln separat für jede Correlation Engine-Instanz migrieren können.
❒	Aktionen	Nur JavaScript-Aktionen können gesichert werden, nicht veraltete Aktionen wie dynamische Listen oder die Aktion „Vorfall erstellen“.
❒	Ereignisbereicherungen	Sentinel sichert auch die verknüpften Zuordnungen für die Ereignisfelder. Es ist daher nicht erforderlich, die verknüpften Zuordnungen nach dem Wiederherstellen der Ereignisbereicherungsdaten neu zu erstellen.
❒	Filter	Sichert alle benutzerdefinierten Filter.
❒	Feeds	Das Lösungspaket sichert nur die Feed-Plugins, nicht jedoch die Plugin-Konfiguration.

Informationen zum Sichern von Daten in Solution Designer finden Sie in „Creating Solution Packs“ (Erstellen von Lösungspaketen) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Verwenden der Option zum Exportieren der Konfiguration in ESM

Sichern Sie Ihre Datenerfassungskonfiguration mithilfe der Exportoption in ESM. Weitere Informationen finden Sie im Abschnitt „Exporting Configurations“ (Exportieren der Konfiguration) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Wiederherstellen von Daten auf dem Zielserver

- „Installieren von Konfigurationsdaten aus dem Lösungspaket“, auf Seite 180
- „Erneutes manuelles Erstellen der Konfiguration“, auf Seite 181

Installieren von Konfigurationsdaten aus dem Lösungspaket

Importieren Sie die Konfigurationsdaten, die Sie auf dem Ursprungsserver mit Solution Designer gesichert haben. Weitere Informationen finden Sie im Abschnitt „Installing Content from Solution Packs“ (Installieren von Inhalten aus Lösungspaketen) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Benennen Sie Objekte wie Filter, Aktionen und Korrelationsregeln mit doppelten Namen um. Standardmäßig sind alle Filter nach dem Importieren auf den Zielserver öffentlich. Weisen Sie die Berechtigungen für jeden Filter erneut zu.

Erneutes manuelles Erstellen der Konfiguration

Außer den aus dem Lösungspaket importierten Konfigurationsdaten müssen alle anderen Konfigurationsdaten manuell neu erstellt werden. Weitere Informationen zu den manuell neu zu erstellenden Konfigurationen finen Sie in Tabelle 32-2, „Migrationsfähige Konfigurationsdaten und neu zu erstellende Konfigurationsdaten“, auf Seite 179.

Migrieren von Ereignisdaten und Rohdaten

Informationen zur Migration von Ereignis- und Rohdaten finden Sie in Migrieren von Daten.

Migrieren von Warnmeldungen und NetFlow-Daten

Mithilfe des Sicherungs- und Wiederherstellungsprogramms können Sie Warnmeldungen und NetFlow-Daten vom Ursprungsserver zum Zielserver migrieren. Für Warnmeldungen stellt das Dienstprogramm die Ereignisse wieder her, die die Warnmeldung ausgelöst haben. Die verknüpften Korrelationsregeln und Knowledgebase-Informationen werden jedoch nicht wiederhergestellt.

Verwenden Sie zum Sichern und Wiederherstellen von Warnmeldungen und NetFlow-Daten die folgenden Befehle:

```
For backing up:
./backup_util.sh -i

For restore:
./backup_util.sh -m restore -f <backup_file_path>
```

Für Warnmeldungen und NetFlow-Daten können Sie wahlweise die vorhandenen Daten überschreiben oder die neuen Daten anfügen. Wählen Sie die gewünschte Option.

Obwohl mit dem oben aufgeführten Befehl die Sicherheitsintelligenzdaten gesichert und wiederhergestellt werden, können Sie diese Daten nicht verwenden, weil in SSDM keine Sicherheitsintelligenz verfügbar ist.

Ausführliche Informationen zur Verwendung des Sicherungs- und Wiederherstellungsprogramms finden Sie unter „Backing Up and Restoring Data“ (Sichern und Wiederherstellen von Daten) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

Aktualisieren der Sentinel-Clients

Die Konfiguration vorhandener Collector Manager-Instanzen, Correlation Engine-Instanzen und NetFlow Collector Manager-Instanzen muss so aktualisiert werden, dass diese Komponenten mit dem Sentinel-Zielserver kommunizieren. Weitere Informationen finden Sie im Abschnitt „Updating Sentinel Clients“ (Aktualisieren der Sentinel-Clients) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

HINWEIS: Auch wenn Sie bereits Ereignisdaten vom Ursprungsserver migriert haben, müssen sie das Datenmigrationsskript erneut ausführen, um Ereignisdaten zu migrieren, die während des Datenmigrationsvorgangs oder danach empfangen wurden. Weitere Informationen finden Sie unter Kapitel 34, „Migrieren von Daten“, auf Seite 185.

Importieren der ESM-Konfiguration

Importieren Sie die Datenerfassungskonfiguration, die Sie auf dem Ursprungsserver verwenden, mithilfe der Option „Konfiguration importieren“ in der ESM-Benutzeroberfläche. Weitere Informationen finden Sie im Abschnitt „Importing Configurations“ (Importieren der Konfiguration) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

33 Migrieren von Daten zu Elasticsearch

Standardmäßig speichert Sentinel Daten in einem dateibasierten herkömmlichen Speicher und indexiert Daten lokal auf dem Sentinel-Server. Wenn Sie Ereignisgrafiken aktivieren, speichert und indexiert Sentinel Daten nicht nur im dateibasierten herkömmlichen Speicher, sondern auch in Elasticsearch. In den Dashboards werden nur die Ereignisse angezeigt, die nach der Aktivierung der Ereignisgrafik verarbeitet wurden. Um die im dateibasierten Speicher vorhandenen Ereignisse anzuzeigen, migrieren Sie die Daten von einem dateibasierten Speicher zu Elasticsearch. Informationen zum Migrieren von Daten zu Elasticsearch finden Sie in Kapitel 34, „Migrieren von Daten“, auf Seite 185.

34 Migrieren von Daten

Mit dem Skript `data_uploader.sh` können Sie Daten zu einer der folgenden Datenspeicherkomponenten migrieren:

- **Kafka:** Sie können sowohl Ereignisdaten als auch Rohdaten zu Kafka migrieren. Führen Sie das Skript getrennt für die Ereignisdaten und die Rohdaten aus. Das Skript migriert die Daten zu den Kafka-Themen.

  Sie können Anpassungen angeben, beispielsweise das Komprimieren der Daten beim Migrieren oder das Senden in Stapeln. Erstellen Sie zum Festlegen dieser Anpassungen eine Eigenschaftendatei und fügen Sie die erforderlichen Eigenschaften im Format mit Schlüssel und Wert hinzu. Beispielsweise können Sie die folgenden Eigenschaften hinzufügen:

  ```
  compression.type=lz4
  ```

  ```
  batch.size=20000
  ```

  Weitere Informationen zu Kafka-Eigenschaften finden Sie in der Kafka-Dokumentation. Legen Sie die Eigenschaften und ihre Werte nach eigenem Ermessen fest. Das Skript validiert die Eigenschaften nicht.

  HINWEIS: Stellen Sie sicher, dass der Sentinel-Server für den gesamten Kafka-Cluster alle Kafka-Broker-Hostnamen in gültige IP-Adressen auflösen kann. Wenn DNS nicht eingerichtet ist, um dies zu ermöglichen, fügen Sie die Kafka-Broker-Hostnamen zur Datei `/etc/hosts` des Sentinel-Servers hinzu.

- **Elasticsearch:** Sie können nur Ereignisdaten zu Elasticsearch migrieren. Bevor Sie Daten migrieren, stellen Sie sicher, dass Sie die Ereignisgrafiken aktiviert haben. Weitere Informationen finden Sie unter „Ereignisgrafik aktivieren“, auf Seite 123.

Das Skript überträgt Daten für den angegebenen Datumsbereich (von/bis). Wenn Sie das Skript ausführen, werden die obligatorischen und optionalen Parameter angezeigt, die Sie zum Initiieren der Datenmigration angeben sollten. Außerdem werden die relevanten Eigenschaften angezeigt, die Sie für die gewünschte Datenspeicherkomponente verwenden sollten.

Das Skript muss mit dem Benutzer „novell“ ausgeführt werden. Stellen Sie daher sicher, dass der Benutzer „novell“ entsprechende Berechtigungen für die Datenverzeichnisse und alle angegebenen Dateien hat. Standardmäßig migriert das Skript Daten vom primären Speicher. Wenn Sie Daten vom sekundären Speicher migrieren möchten, geben Sie beim Ausführen des Skripts den entsprechenden Pfad für den sekundären Speicher an.

So migrieren Sie Daten:

1. Melden Sie sich beim Sentinel-Server als der Benutzer „novell“ an.
2. Führen Sie das folgende Skript aus:

   ```
   /opt/novell/sentinel/bin/data_uploader.sh
   ```

3. Befolgen Sie die Bildschirmanweisungen und führen Sie das Skript erneut mit den erforderlichen Parametern aus.

Die migrierten Daten haben den im Zielserver festgelegten Beibehaltungszeitraum.

Nachdem die Daten migriert wurden, zeichnet das Skript den Status auf, zum Beispiel, ob die Partitionen erfolgreich migriert wurden, ob Fehler beim Migrieren der Partitionen aufgetreten sind oder wie viele Ereignisse migriert wurden. Bei Partitionen mit dem Datum des Vortages oder des heutigen Datums zeigt der Datenübertragungsstatus „IN_PROGRESS“ (In Bearbeitung) an, um möglicherweise spät empfangene Ereignisse zu berücksichtigen.

Wenn das Migrieren der Daten nicht erfolgreich abgeschlossen wurde oder der Migrationsstatus für die Partitionen „IN_PROGRESS“ (In Bearbeitung) anzeigt, führen Sie das Skript erneut aus. Wenn Sie das Skript erneut ausführen, wird zuerst die Statusdatei überprüft, um zu ermitteln, welche Partitionen bereits migriert wurden. Anschließend werden nur die verbleibenden Partitionen migriert. Zur Fehlersuche pflegt das Skript Protokolle im Verzeichnis /`var/opt/novell/sentinel/log/data_uploader.log`.

VII Bereitstellen von Sentinel für Hochverfügbarkeitssysteme

In diesem Abschnitt wird beschrieben, wie Sentinel in einem Aktiv-Passiv-Hochverfügbarkeitsmodus installiert wird, wodurch Sentinel ein Failover in einen redundanten Clusterknoten durchführen kann, falls Hardware- oder Softwarefehler auftreten. Wenden Sie sich an den Technischen Support von , um weitere Informationen zur Bereitstellung von Hochverfügbarkeitssystemen und Disaster Recovery in Ihrer Sentinel-Umgebung zu erhalten.

HINWEIS: Die Hochverfügbarkeitskonfiguration wird nur auf dem Sentinel-Server unterstützt. Die Collector Manager- und Correlation Engine-Instanzen können jedoch weiter mit dem Sentinel-Hochverfügbarkeitsserver kommunizieren.

---

35 Konzepte

Hochverfügbarkeit bezieht sich auf eine Entwicklungsmethode, die ein System so verfügbar halten soll, wie es praktisch umsetzbar ist. Es wird beabsichtigt, die Gründe für Ausfallzeiten wie Systemfehler und Wartungstätigkeiten zu minimieren. Außerdem soll die Zeit verkürzt werden, die zur Erkennung von und Wiederherstellung nach auftretenden Ausfallereignissen benötigt wird. In der Praxis werden automatische Methoden der Erkennung von und Wiederherstellung nach Ausfallereignissen schnell erforderlich, weil höhere Verfügbarkeitsgrade errreicht werden müssen.

Weitere Informationen zur Hochverfügbarkeit finden Sie im SUSE High Availability Guide (Handbuch zur SUSE-Hochverfügbarkeit).

Externe Systeme

Sentinel ist eine komplexe, mehrschichtige Anwendung, die von einer großen Vielzahl von Diensten abhängt und diese bereitstellt. Außerdem kann es in mehrere Systeme von Drittanbietern zur Datenerfassung, Datenfreigabe und Vorfallbehebung integriert werden. Die meisten Hochverfügbarkeitslösungen ermöglichen es den Anwendern, Abhängigkeiten zwischen den Diensten, die hochverfügbar sein sollten, zu definieren, doch dies trifft nur auf Dienste zu, die im Knoten selbst ausgeführt werden. Sentinel-externe Systeme wie Ereignisquellen müssen separat konfiguriert werden, um so verfügbar zu sein, wie es im Unternehmen erforderlich ist. Diese müssen auch konfiguriert werden, um Situationen ordnungsgemäß verarbeiten zu können, in denen Sentinel für eine bestimmte Zeit nicht verfügbar ist, wie zum Beispiel bei Failover-Ereignissen. Wenn die Zugriffsrechte stark eingeschränkt sind, zum Beispiel wenn authentifizierte Sitzungen zum Senden und/oder Empfangen von Daten zwischen dem Drittanbietersystem und Sentinel verwendet werden, muss das Drittanbietersystem so konfiguriert werden, dass es Sitzungen von beliebigen Clusterknoten akzeptiert oder dort initiiert (Sentinel sollte zu diesem Zweck mit einer virtuellen IP-Adresse konfiguriert werden).

Freigegebener Speicher

Alle Hochverfügbarkeits-Cluster erfordern irgendeine Form von freigegebenem Speicher, sodass diese Anwendungsdaten schnell von einem Clusterknoten in ein anderen verschoben werden können, falls im ursprünglichen Knoten ein Fehler auftritt. Der Speicher selbst sollte hochverfügbar sein. Dies wird normalerweise durch die Verbindung der SAN-Technologie (Storage Area Network, SAN) mit den Clusterknoten über ein FibreChannel-Netzwerk erreicht. Andere Systeme verwenden NAS (Network Attached Storage), iSCSI oder andere Technologien, die ein Ferneinhängen eines

freigegebenen Speichers zulassen. Die grundlegenden Anforderungen des freigegebenen Speichers bestehen darin, dass der Cluster den Speicher sauber von einem fehlerhaften Clusterknoten an einen neuen Clusterknoten verschieben kann.

Es gibt zwei grundlegende Vorgehensweisen, die Sentinel für den freigegebenen Speicher verwenden kann. Bei der ersten werden alle Komponenten (Anwendungs-Binärdateien, Konfiguration und Ereignisdaten) im freigegebenen Speicher gesucht. Bei einem Failover wird der Speicher am primären Knoten ausgehängt und in den Sicherungsknoten verschoben. Dadurch wird die gesamte Anwendung und Konfiguration des freigegebenen Speichers geladen. Bei der zweiten Vorgehensweise werden die Ereignisdaten im freigegebenen Speicher gespeichert, doch die Anwendungs-Binärdateien und die Konfiguration bleiben auf jedem Clusterknoten. Bei einem Failover werden nur die Ereignisdaten in den Sicherungsknoten verschoben.

Jede Vorgehensweise hat Vorteile und Nachteile, doch bei der zweiten Vorgehensweise kann die Sentinel-Installation die FHS-konformen Standardinstallationspfade verwenden. Außerdem ermöglicht sie die Überprüfung der RPM-Softwarepaketerstellung und auch die Anwendung von Patches und die Neukonfiguration bei laufendem Betrieb, um die Ausfallzeit zu minimieren.

Diese Lösung führt Sie durch ein Beispiel einer Installation in einem Cluster, der den freigegebenen iSCSI-Speicher verwendet und die Anwendungsbinärdateien/-konfiguration auf jedem Clusterknoten sucht.

Dienstüberwachung

Eine entscheidende Komponente in jeder hochverfügbaren Umgebung ist eine zuverlässige, konsistente Methode zur Überwachung der Ressourcen, die hochverfügbar sein sollten, und der Ressourcen, von denen diese abhängen. Die SLE HAE verwendet zur Durchführung dieser Überwachung eine Komponente namens Resource Agent. Deren Aufgabe besteht darin, den Status der einzelnen Ressourcen anzugeben und diese Ressource (auf Anfrage) zu starten oder zu stoppen.

Resource Agent muss einen zuverlässigen Status für die überwachten Ressourcen angeben, um unnötige Ausfallzeiten zu verhindern. Ein falscher Positiv-Status (wenn eine Ressource als fehlerhaft gilt, doch den Fehler selbst wieder beheben könnte) kann zur Dienstmigration (und damit verbundenen Ausfallzeit) führen, obwohl dies überhaupt nicht notwendig wäre. Ein falscher Negativ-Status (wenn der Resource Agent meldet, dass eine Ressource funktioniert, obwohl sie dies nicht ordnungsgemäß tut) kann die ordnungsgemäße Verwendung des Diensts verhindern. Andererseits kann die externe Überwachung eines Diensts recht schwierig sein. Ein Webdienst-Port zum Beispiel könnte zwar auf ein einfaches Ping reagieren, liefert jedoch keine korrekten Daten, wenn eine echte Anfrage ausgestellt wird. In vielen Fällen muss in den Dienst die Funktion zur Selbstdiagnose integriert sein, um eine wirklich präzise Messung durchführen zu können.

Diese Lösung bietet die Basisversion des OCF Resource Agent für Sentinel, der das System auf größere Fehler in der Hardware, im Betriebssystem oder im Sentinel-System überwachen kann. Zu diesem Zeitpunkt basieren die Fähigkeiten zur externen Überwachung von Sentinel auf IP-Port-Tests und es besteht durchaus die Gefahr für die Ablesung eines falschen Positiv- und falschen Negativ-Status. Wir planen, sowohl Sentinel als auch den Resource Agent langfristig zu verbessern, um die Genauigkeit dieser Komponente zu erhöhen.

Fencing

In einem HA-Cluster werden kritische Dienste ständig überwacht und automatisch in anderen Knoten neu gestartet, falls sie fehlerhaft sind. Diese Automatisierung kann jedoch Probleme mit sich bringen, wenn im primären Knoten Kommunikationsprobleme auftreten. Obwohl der in diesem Knoten

ausgeführte Dienst anscheinend ausgefallen ist, wird er in Wahrheit weiter ausgeführt und schreibt weiterhin Daten in den freigegebenen Speicher. In diesem Fall kann der Start einer Reihe von Diensten auf einem Sicherungsknoten leicht zu Datenbeschädigung führen.

Cluster verwenden eine Vielzahl an Methoden (wie zum Beispiel Split Brain Detection (SBD) und Shoot The Other Node In The Head (STONITH)), um dies zu verhindern. Diese werden kollektiv als Fencing bezeichnet. Primäres Ziel ist es, die Beschädigung der Daten im freigegebenen Speicher zu verhindern.

36 Systemanforderungen

Bei der Zuweisung von Cluster-Ressourcen zur Unterstützung einer Hochverfügbarkeitsinstallation sind die folgenden Anforderungen zu erfüllen:

- ❒ (Bedingt) Bei Hochverfügbarkeits-Appliance-Installationen muss die Hochverfügbarkeitsversion von Sentinel Appliance mit einer gültigen Lizenz verfügbar sein. Die Hochverfügbarkeitsversion von Sentinel Appliance ist eine ISO-Appliance mit den folgenden Paketen:
  - Betriebssystem: SLES 12 SP3
  - Paket: SLES High Availability Extension (SLES HAE)
  - Sentinel-Software (mit Hochverfügbarkeits-RPM)
- ❒ (Bedingt) In herkömmlichen Hochverfügbarkeitsinstallationen muss Folgendes verfügbar sein:
  - Betriebssystem: SLES 11 SP4 oder SLES 12 SP1 oder höher
  - SLES HAE-ISO-Image mit gültigen Lizenzen
  - Sentinel-Installationsprogramm (TAR-Datei)
- ❒ (Bedingt) Wenn Sie das SLES-Betriebssystem mit Kernel-Version 3.0.101 oder höher verwenden, müssen Sie den Watchdog-Treiber manuell in den Computer laden. Den richtigen Watchdog-Treiber für Ihre Computer-Hardware erhalten Sie bei Ihrem Hardware-Händler. So laden Sie den Watchdog-Treiber:
  1. Zum Laden des Watchdog-Treibers in der aktuellen Sitzung führen Sie in der Befehlszeile den folgenden Befehl aus:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. Fügen Sie in der Datei `/etc/init.d/boot.local` die folgende Zeile hinzu, um sicherzustellen, dass der Computer bei jedem Booten automatisch den Watchdog-Treiber lädt:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```
- ❒ Vergewissern Sie sich, dass jeder Clusterknoten, auf dem Sentinel-Services gehostet werden, die in Kapitel 5, „Erfüllen der Systemanforderungen“, auf Seite 37 angegebenen Anforderungen erfüllt.
- ❒ Stellen Sie sicher, dass genügend freigegebener Speicherplatz für die Sentinel-Daten und -Anwendung zur Verfügung steht.
- ❒ Stellen Sie sicher, dass Sie für die Dienste eine virtuelle IP-Adresse verwenden, die bei Failover von Knoten zu Knoten migriert werden kann.
- ❒ Stellen Sie sicher, dass das Gerät für den freigegebenen Speicher die in Kapitel 5, „Erfüllen der Systemanforderungen“, auf Seite 37 genannten Leistungs- und Größenanforderungen erfüllt. Verwenden Sie eine mit iSCSI-Zielen konfigurierte Standard-SLES-VM als freigegebenen Speicher.

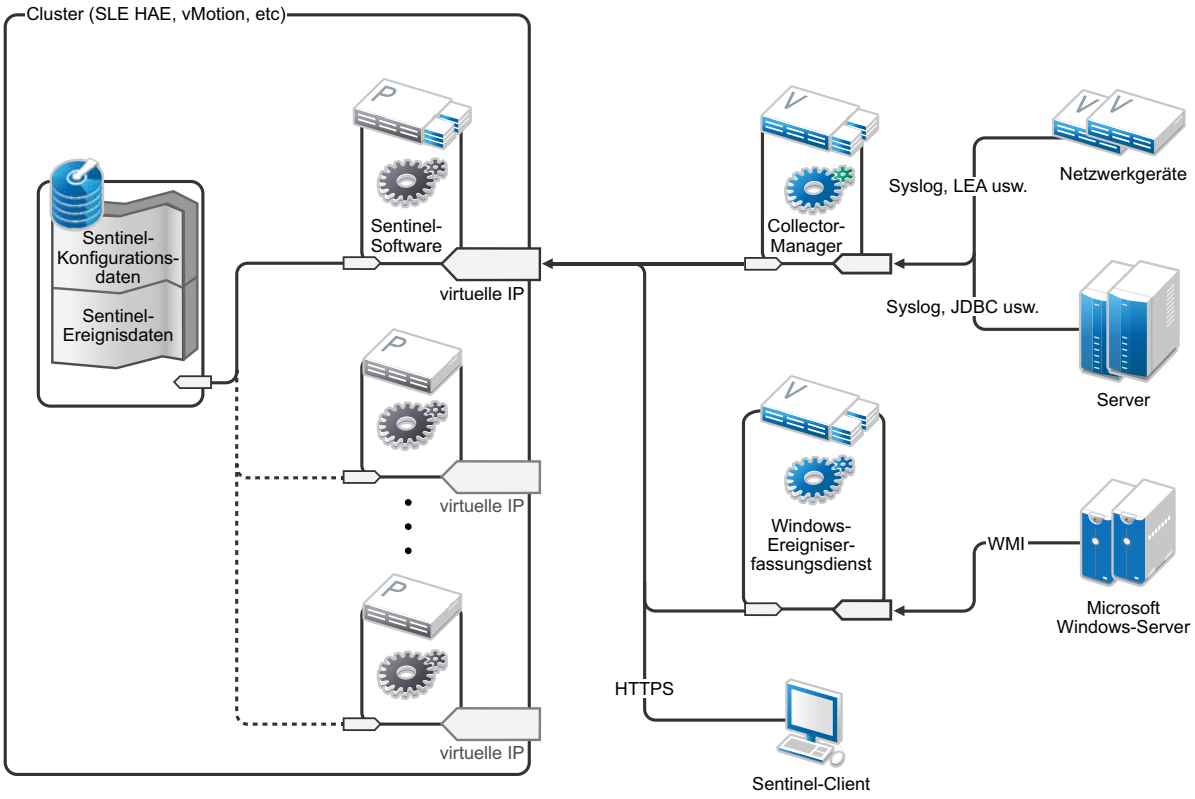
  Für iSCSI sollten Sie die größte von der verwendeten Hardware unterstützte MTU (Message Transfer Unit) verwenden. Größere MTUs verbessern die Speicherleistung. In Sentinel können Probleme auftreten, wenn die Latenz und Bandweite zum Speicher nicht den Mindestempfehlungen entspricht.

- ❒ Stellen Sie sicher, dass mindestens zwei Clusterknoten vorhanden sind, die die Ressourcenanforderungen zum Ausführen von Sentinel in einer Kundenumgebung erfüllen. Es wird empfohlen, zwei SLES-VM zu verwenden.
- ❒ Stellen Sie sicher, dass Sie eine Methode der Kommunikation zwischen den Clusterknoten und dem freigegebenen Speicher erstellen, beispielsweise FibreChannel für ein SAN. Verwenden Sie eine dedizierte IP-Adresse für die Verbindung zum iSCSI-Ziel.
- ❒ Stellen Sie sicher, dass eine virtuelle IP-Adresse verfügbar ist, die innerhalb eines Clusters von einem Knoten zu einem anderen migriert werden kann, um als externe IP-Adresse für Sentinel zu fungieren.
- ❒ Stellen Sie sicher, dass mindestens eine IP-Adresse pro Clusterknoten für die interne Clusterkommunikation verfügbar ist. Sie können eine einfache Unicast-IP-Adresse verwenden, für Produktionsumgebungen sollte jedoch Multicast bevorzugt werden.

37 Installation und Konfiguration

In diesem Kapitel finden Sie die Vorgehensweise zur Installation und Konfiguration von Sentinel in einer Hochverfügbarkeitsumgebung.

Im folgenden Diagramm ist eine Aktiv-Passiv-HA-Architektur dargestellt.



Das System einrichten

Konfigurieren Sie die Computerhardware, die Netzwerkhardware, die Speicherhardware, die Betriebssysteme, die Benutzerkonten und andere grundlegende Systemressourcen entsprechend der dokumentierten Anforderungen für Sentinel sowie der lokalen Anforderungen des Kunden. Testen Sie die Systeme, um die ordnungsgemäße Funktion und Stabilität sicherzustellen.

Die folgende Checkliste unterstützt Sie bei der ersten Einrichtung und Konfiguration:

	Checklistenelemente
❑	Die CPU-, RAM- und Speicherplatzeigenschaften für jeden Clusterknoten müssen den Systemanforderungen entsprechen, die auf Basis der erwarteten Ereignisrate in Kapitel 5, „Erfüllen der Systemanforderungen“, auf Seite 37 definiert sind.
❑	Die Speicherplatz- und E/A-Eigenschaften für die Speicherknoten müssen den Systemanforderungen entsprechen, die auf Basis der erwarteten Ereignisrate und Datenbeibehaltungsrichtlinien für den Primär- und Sekundärspeicher in Kapitel 5, „Erfüllen der Systemanforderungen“, auf Seite 37 definiert sind.
❑	Wenn Sie die Betriebssystem-Firewalls konfigurieren möchten, um den Zugriff auf Sentinel und den Cluster einzuschränken, finden Sie detaillierte Informationen darüber, welche Ports abhängig von der lokalen Konfiguration und den Quellen, die Ereignisdaten senden, im Abschnitt Kapitel 8, „Verwendete Ports“, auf Seite 61.
❑	Stellen Sie sicher, dass alle Clusterknoten zeitlich synchronisiert sind. Sie können hierzu NTP oder eine ähnliche Methode verwenden.
❑	◆ Für den Cluster ist eine zuverlässige Hostnamenauflösung erforderlich. Geben Sie alle internen Cluster-Hostnamen in die Datei `/etc/hosts` ein, um die Clusterbeständigkeit im Falle eines DNS-Fehlers zu gewährleisten. ◆ Weisen Sie einer Loopback-IP-Adresse keinen Hostnamen zu. ◆ Deaktivieren Sie die Option **Hostnamen zu Loopback-IP zuweisen**, wenn Sie bei der Installation des Betriebssystems Hostnamen und Domänennamen definieren.

Sie können die folgende Konfiguration verwenden:

- (Bedingt) Bei herkömmlichen Hochverfügbarkeits-Installationen:
  - Zwei Clusterknoten-VMs unter SLES 11 SP4 oder SLES 12 SP1 oder höher.
  - (Bedingt) Wenn Sie eine grafische Benutzeroberfläche für die Konfiguration benötigen, können Sie das X-Window-System installieren. Legen Sie die Bootskripte zum Starten ohne X fest (Runlevel 3), um sie nur bei Bedarf starten zu können.
- (Bedingt) Bei Hochverfügbarkeits-Appliance-Installationen: Zwei Clusterknoten-VMs auf Basis einer HA-ISO-Appliance. Weitere Informationen zum Installieren der Hochverfügbarkeits-ISO-Appliance finden Sie unter „Installieren von Sentinel“, auf Seite 100.
- Die Knoten verfügen über einen NIC für den externen Zugriff und einen für die iSCSI-Kommunikation.
- Konfigurieren Sie die externen NICs mit IP-Adressen, die den Fernzugriff über SSH oder ähnliches zulassen. Für dieses Beispiel verwenden wir 172.16.0.1 (node01) und 172.16.0.2 (node02).
- Jeder Knoten sollte genügend Speicherplatz für das Betriebssystem, die Sentinel-Binärdateien und die Konfigurationsdaten, die Clustersoftware, den temporären Speicher etc. haben. Weitere Informationen finden Sie in den Systemanforderungen für SLES und SLES HAE sowie in den Sentinel-Anwendungsanforderungen.

- Eine virtuelle Maschine unter SLES 11 SP4 oder SLES 12 SP1 oder höher, die mit iSCSI-Zielen für freigegebenen Speicher konfiguriert ist
  - (Bedingt) Wenn Sie eine grafische Benutzeroberfläche für die Konfiguration benötigen, können Sie das X-Window-System installieren. Legen Sie die Bootskripte zum Starten ohne X fest (Runlevel 3), um sie nur bei Bedarf starten zu können.
  - Das System verfügt über zwei NICs – einen für den externen Zugriff und einen für die iSCSI-Kommunikation.
  - Konfigurieren Sie den externen NIC mit einer IP-Adresse, die den Fernzugriff über SSH oder ähnliches zulässt. Beispiel: 172.16.0.3 (storage03).
  - Das System sollte über genügend Speicherplatz für das Betriebssystem, einen temporären Speicher und ein großes Volume für den freigegebenen Speicher für Sentinel-Daten verfügen sowie über etwas Speicherplatz für eine SBD-Partition. Weitere Informationen finden Sie in den Systemanforderungen für SLES sowie in den Sentinel-Anforderungen für den Ereignisdatenspeicher.

HINWEIS: In einem Produktionscluster können Sie interne, nicht weiterleitbare IP-Adressen auf separaten NICs (möglicherweise zwei, aus Redundanzgründen) für die interne Clusterkommunikation verwenden.

Einrichtung des freigegebenen Speichers

Richten Sie Ihren freigegebenen Speicher ein und stellen Sie sicher, dass Sie ihn in jedem Clusterknoten einhängen können. Wenn Sie FibreChannel und ein SAN verwenden, müssen Sie unter Umständen physische Verbindungen und eine zusätzliche Konfiguration angeben. Sentinel speichert die Datenbanken und Ereignisdaten in diesem freigegebenen Speicher. Vergewissern Sie sich, dass der freigegebene Speicher eine in Bezug auf die erwartete Ereignisrate und die Datenbeibehaltungsrichtlinien geeignete Größe hat.

Hier ein Beispiel für die Einrichtung von freigegebenem Speicher:

Eine typische Implementierung könnte ein schnelles SAN verwenden, das über FibreChannel an alle Clusterknoten angehängt wird und über ein großes RAID-Array zum Speichern der lokalen Ereignisdaten verfügt. Ein separater NAS- oder iSCSI-Knoten könnte für den langsameren Sekundärspeicher verwendet werden. Wenn der Clusterknoten den Primärspeicher als normales Blockgerät einhängen kann, kann er auch für die Lösung verwendet werden. Der Sekundärspeicher kann auch als Blockgerät eingehängt werden oder könnte ein NFS- oder CIFS-Volume sein.

HINWEIS: Konfigurieren Sie den freigegebenen Speicher und testen Sie das Mounten des Speichers an jedem Clusterknoten. Die Clusterkonfiguration übernimmt dann jedoch das eigentliche Einhängen des Speichers.

So erstellen Sie iSCSI-Ziele, die auf einer virtuellen SLES-Maschine gehostet werden:

1. Stellen Sie eine Verbindung zu `storage03` (der im Schritt Das System einrichten erstellten virtuellen Maschine) her und starten Sie eine Konsolensitzung.
2. Erstellen Sie mit dem folgenden Befehl eine leere Datei beliebiger Größe für den Sentinel-Primärspeicher:

   `dd if=/dev/zero of=/localdata count=<`*`Dateigröße`*`> bs=<`*`Bit-Größe`*`>`

   Mit folgendem Befehl erstellen Sie zum Beispiel eine 20-GB-Datei voller Nullen, die vom Pseudogerät `/dev/zero` kopiert wird:

```
dd if=/dev/zero of=/localdata count=20480000 bs=1024
```

3 Wiederholen Sie die Schritte 1 und 2, um auf dieselbe Weise eine Datei für den Sekundärspeicher zu erstellen.

   Verwenden Sie für den Sekundärspeicher zum Beispiel folgenden Befehl:

```
dd if=/dev/zero of=/networkdata count=20480000 bs=1024
```

HINWEIS: In diesem Beispiel werden zwei Dateien mit der gleichen Größe und den gleichen Leistungsmerkmalen erstellt, die die beiden Datenträger darstellen. Für eine Produktionsbereitstellung können Sie den Primärspeicher in ein schnelles SAN stellen und den Sekundärspeicher in ein langsameres iSCSI-, NFS- oder CIFS-Volume.

Zum Konfigurieren von iSCSI-Zielen und Initiatorgeräten befolgen Sie die Anleitungen in den folgenden Abschnitten:

- „Konfigurieren von iSCSI-Zielen“, auf Seite 198
- „Konfigurieren von iSCSI-Initiatoren“, auf Seite 200

Konfigurieren von iSCSI-Zielen

Nachstehend wird erklärt, wie Sie die Dateien `localdata` und `networkdata` als iSCSI-Ziele konfigurieren.

Weitere Informationen zur Konfiguration von iSCSI-Zielen finden Sie unter Creating iSCSI Targets with YaST (Erstellen von iSCSI-Zielen mit YaST) in der SUSE-Dokumentation.

1 Führen Sie YaST von der Befehlszeile aus (oder verwenden Sie die grafische Benutzeroberfläche, falls bevorzugt): `/sbin/yast`

2 Wählen Sie **Netzwerkgeräte** > **Netzwerkeinstellungen** aus.

3 Vergewissern Sie sich, dass die Registerkarte **Überblick** ausgewählt ist.

4 Wählen Sie den sekundären NIC aus der angezeigten Liste aus, fahren Sie anschließend fort bis zur Registerkarte „Bearbeiten“ und drücken Sie die `Eingabetaste`.

5 Weisen Sie auf der Registerkarte **Adresse** eine statische IP-Adresse von 10.0.0.3 zu. Dies ist die IP-Adresse für die interne iSCSI-Kommunikation.

6 Klicken Sie auf **Weiter** und anschließend auf **OK**.

7 (Bedingt) In der Hauptmaske:

   - Unter SLES 11 SP4 wählen Sie **Netzwerkdienste** > **iSCSI-Ziel**.
   - Unter SLES 12 SP1 oder höher wählen Sie **Netzwerkdienste** > **iSCSI-LIO-Ziel**.

   HINWEIS: Wenn diese Option nicht angezeigt wird, navigieren Sie zu **Software** > **Software Management** > **iSCSI LIO Server** (Software > Softwareverwaltung > iSCSI-LIO-Server) und installieren Sie das iSCSI-LIO-Paket.

   ---

8 (Bedingt) Installieren Sie bei entsprechender Aufforderung die erforderliche Software:

   - Bei SLES 11 SP4: `iscsitarget RPM`
   - SLES 12 SP1 oder höher: `iscsiliotarget RPM`

9 (Bedingt) Führen Sie unter SLES 12 SP1 oder höher die folgenden Schritte für alle Knoten im Cluster aus:

   9a Öffnen Sie mit folgendem Befehl die Datei, die den iSCSI-Initiatornamen enthält:

```
cat /etc/iscsi/initiatorname.iscsi
```

9b Notieren Sie sich den Initiatornamen, da dieser bei der Konfiguration von iSCSI-Initiatoren zur Anwendung kommt:

Beispiel:

```
InitiatorName=iqn.1996-04.de.suse:01:441d6988994
```

Initiatornamen werden bei der Konfiguration von iSCSI-Ziel-Clients benötigt.

10 Klicken Sie auf **Dienst** und wählen Sie die Option **Beim Booten** aus, um sicherzustellen, dass der Dienst beim Booten des Betriebssystems gestartet wird.

11 Deaktivieren Sie auf der Registerkarte **Global** die Option **Keine Authentifizierung**, um die Authentifizierung zu aktivieren, und geben Sie dann den Berechtigungsnachweis für die eingehende und ausgehende Authentifizierung an.

Die Option **Keine Authentifizierung** ist standardmäßig aktiviert. Sie sollten jedoch die Authentifizierung aktivieren, um sicherzustellen, dass die Konfiguration sicher ist.

12 Klicken Sie auf **Ziele** und anschließend auf **Hinzufügen**, um ein neues Ziel hinzuzufügen.

Das iSCSI-Ziel generiert automatisch eine ID und bietet dann eine leere Liste der verfügbaren LUNs (Laufwerke) an.

13 Klicken Sie auf **Hinzufügen**, um ein neues LUN hinzuzufügen.

14 Belassen Sie die LUN-Nummer als 0, durchsuchen Sie anschließend das Dialogfeld **Pfad** (unter Type=fileio) und wählen Sie die Datei `/localdata` aus, die Sie erstellt haben. Wenn Sie über einen dedizierten Datenträger für den Speicher verfügen, geben Sie ein Blockgeräte an wie zum Beispiel `/dev/sdc`.

15 Wiederholen Sie die Schritte 13 und 14. Fügen Sie diesmal LUN 1 hinzu und wählen Sie `/networkdata` aus.

16 (Bedingt) Führen Sie unter SLES 11 SP4 die folgenden Schritte aus:

16a Behalten Sie für die anderen Optionen die Standardwerte bei und klicken Sie auf **OK** und dann auf **Weiter**.

16b (Bedingt) Wenn Sie die Authentifizierung in Schritt 11 aktiviert haben, geben Sie den Berechtigungsnachweis zur Authentifizierung ein.

Wählen Sie einen Client und dann **Edit Auth** > **Incoming Authentication** (Authentifizierung bearbeiten > eingehende Authentifizierung) aus und geben Sie den Benutzernamen und das Passwort an.

17 (Bedingt) Führen Sie unter SLES 12 SP1 oder höher die folgenden Schritte aus:

17a Behalten Sie für die anderen Optionen die Standardwerte bei und klicken Sie auf **Weiter**.

17b Klicken Sie auf **Hinzufügen**. Wenn Sie zur Eingabe des Clientnamens aufgefordert werden, geben Sie den in Schritt 9 notierten Initiatornamen an. Wiederholen Sie diesen Schritt, um alle Clientnamen unter Angabe des Initiatornamens hinzuzufügen.

Die Clientnamen werden in der Clientliste aufgeführt.

17c (Bedingt) Wenn Sie die Authentifizierung in Schritt 11 aktiviert haben, geben Sie den Berechtigungsnachweis zur Authentifizierung ein.

Wählen Sie einen Client und dann **Edit Auth** > **Incoming Authentication** (Authentifizierung bearbeiten > eingehende Authentifizierung) aus und geben Sie den Benutzernamen und das Passwort an. Wiederholen Sie dies für alle Clients.

18 Klicken Sie erneut auf **Weiter**, um die Standardoptionen für die Authentifizierung auszuwählen, und dann auf **Fertig stellen**, um die Konfiguration zu beenden. Akzeptieren Sie den Neustart von iSCSI.

19 Beenden Sie YaST.

HINWEIS: Mit dieser Prozedur werden zwei iSCSI-Ziele am Server mit der Adresse 10.0.0.3 ausgewiesen. Stellen Sie sicher, dass die freigegebenen Speichergeräte mit den lokalen Daten in jedem Clusterknoten eingehängt werden können.

Konfigurieren von iSCSI-Initiatoren

Nachstehend wird erklärt, wie Sie die iSCSI-Initiatorgeräte formatieren.

Weitere Informationen zur Konfiguration von iSCSI-Initiatoren finden Sie unter Configuring the iSCSI Initiator (Konfigurieren des iSCSI-Initiators) in der SUSE-Dokumentation.

1. Stellen Sie eine Verbindung zu einem der Clusterknoten (node01) her und starten Sie YaST.
2. Wählen Sie **Netzwerkgeräte** > **Netzwerkeinstellungen** aus.
3. Vergewissern Sie sich, dass die Registerkarte **Überblick** ausgewählt ist.
4. Wählen Sie den sekundären NIC aus der angezeigten Liste aus, fahren Sie anschließend fort bis zur Registerkarte „Bearbeiten“ und drücken Sie die Eingabetaste.
5. Klicken Sie auf **Adresse** und weisen Sie eine statische IP-Adresse von 10.0.0.1 zu. Dies ist die IP-Adresse für die interne iSCSI-Kommunikation.
6. Wählen Sie **Weiter** aus und klicken Sie anschließend auf **OK**.
7. Klicken Sie auf **Netzwerkdienste** > **iSCSI-Initiator**.
8. Installieren Sie bei entsprechender Aufforderung die erforderliche Software (`iscsiclient`-RPM).
9. Klicken Sie auf **Dienst** und wählen Sie **Beim Booten** aus, um sicherzustellen, dass der iSCSI-Dienst beim Booten gestartet wird.
10. Klicken Sie auf **Erkannte Ziele** und wählen Sie **Ermittlung** aus.
11. Geben Sie die IP-Adresse des iSCSI-Ziels an (10.0.0.3).

    (Bedingt) Wenn Sie die Authentifizierung in Schritt 11 in „Konfigurieren von iSCSI-Zielen“, auf Seite 198 aktiviert haben, deaktivieren Sie **Keine Authentifizierung**. Geben Sie im Feld **Outgoing Authentication** (Ausgehende Authentifizierung) den Benutzernamen und das Passwort ein, den bzw. das Sie während der Konfiguration des iSCSI-Ziels angelegt haben.

    Klicken Sie auf **Weiter**.
12. Wählen Sie zunächst das erkannte iSCSI-Ziel mit der IP-Adresse 10.0.0.3 aus und anschließend die Option **Anmelden**.
13. Führen Sie die folgenden Schritte aus:

    13a Wechseln Sie im Dropdown-Menü **Startup** (Start) zu „Automatic“ (Automatisch).

    13b (Bedingt) Wenn Sie die Authentifizierung aktiviert haben, deaktivieren Sie **Keine Authentifizierung**.

    Der in Schritt 11 angegebene Berechtigungsnachweis (Benutzername und Passwort) sollte im Abschnitt **Outgoing Authentication** (Ausgehende Authentifizierung) angezeigt werden. Wird er es nicht, geben Sie ihn dort ein.

    13c Klicken Sie auf **Weiter**.
14. Wechseln Sie zur Registerkarte **Verbundene Ziele**, um sicherzustellen, dass wir mit dem Ziel verbunden sind.
15. Beenden Sie die Konfiguration. Damit sollten die iSCSI-Ziele als Blockgeräte im Clusterknoten eingehängt sein.
16. Wählen Sie im YaST-Hauptmenü **System** > **Partitionierer** aus.

17 In der Systemansicht sollten neue Festplatten der folgenden Typen aufgelistet sein (z. B. `/dev/sdb` und `/dev/sdc`):

- Unter SLES 11 SP4: IET-VIRTUAL-DISK
- Unter SLES 12 SP1 oder höher: LIO-ORG-FILEIO

Gehen Sie mit der Tabulatortaste zur ersten Festplatte in der Liste (sollte der Primärspeicher sein), wählen Sie sie aus und drücken Sie auf die Eingabetaste.

18 Wählen Sie **Hinzufügen** aus, um der leeren Festplatte eine neue Partition hinzuzufügen. Formatieren Sie die Festplatte als primäre -Partition, doch hängen Sie sie nicht ein. Vergewissern Sie sich, dass die Option **Partition nicht einhängen** ausgewählt ist.

19 Wählen Sie **Weiter** und anschließend **Fertig stellen**, nachdem Sie sich die Änderungen angesehen haben, die vorgenommen werden.

Der formatierte Datenträger (z. B. `/dev/sdb1`) sollte jetzt bereit sein. In den folgenden Anleitungsschritten wird er als `/dev/<SHARED1>` bezeichnet.

20 Gehen Sie zurück zum **Partitionierer** und wiederholen Sie den Partitionierungs- und Formatierungsvorgang (Schritte 16–19) für `/dev/sdc` oder welches Blockgerät auch immer dem Sekundärspeicher entspricht. Dies sollte zu einer Partition `/dev/sdc1` oder einer ähnlichen formatierten Festplatte führen (weiter unten als `/dev/<NETWORK1>` bezeichnet).

21 Beenden Sie YaST.

22 (Bedingt) Wenn Sie eine herkömmliche Hochverfügbarkeits-Installation vornehmen, erstellen Sie einen Einhängepunkt, und testen Sie das Einhängen der lokalen Partition wie folgt (der Gerätename ergibt sich dabei aus der jeweiligen Implementierung):

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

Sie sollten in der Lage sein, Dateien auf der neuen Partition zu erstellen und die Dateien dort zu sehen, wo auch immer die Partition eingehängt ist.

23 (Bedingt) Wenn Sie eine herkömmliche Hochverfügbarkeits-Installation vornehmen, gehen Sie zum Aushängen wie folgt vor:

```
# umount /var/opt/novell
```

24 (Bedingt) Wiederholen Sie für Hochverfügbarkeits-Appliance-Installationen die Schritte 1 bis 15, um sicherzustellen, dass jeder Clusterknoten den lokalen freigegebenen Speicher einhängen kann. Ersetzen Sie die Knoten-IP-Adresse in Schritt 5 jeweils durch eine andere IP-Adresse für jeden Clusterknoten.

25 (Bedingt) Wiederholen Sie für herkömmliche Appliance-Installationen die Schritte 1 bis 15, 22 und 23, um sicherzustellen, dass jeder Clusterknoten den lokalen freigegebenen Speicher einhängen kann. Ersetzen Sie die Knoten-IP-Adresse in Schritt 6 jeweils durch eine andere IP-Adresse für jeden Clusterknoten.

Sentinel-Installation

Zur Installation von Sentinel haben Sie zwei Möglichkeiten: Die erste Möglichkeit ist, jeden Teil von Sentinel im freigegebenen Speicher zu installieren und dabei die Option `--location` zu verwenden, um die Sentinel-Installation dorthin umzuadressieren, wo der freigegebene Speicher eingehängt ist. Die zweite Möglichkeit ist, nur die variablen Anwendungsdaten im freigegebenen Speicher zu installieren.

Installieren Sie Sentinel auf jedem Clusterknoten, der als Host fungieren kann. Bei der Erstinstallation von Sentinel müssen Sie eine vollständige Installation einschließlich Anwendungsbinärdaten, Konfiguration und aller Datenablagen ausführen. Bei den folgenden Installationen auf anderen Clusterknoten installieren Sie dann nur die Anwendung. Die Sentinel-Daten sind nach dem Einhängen des freigegebenen Speichers verfügbar.

Erste Installation im Knoten

- „Herkömmliche Hochverfügbarkeits-Installation“, auf Seite 202
- „Installation der Hochverfügbarkeitsversion von Sentinel Appliance“, auf Seite 203

Herkömmliche Hochverfügbarkeits-Installation

1. Stellen Sie eine Verbindung zu einem der Clusterknoten her (node01) und öffnen Sie ein Konsolenfenster.
2. Laden Sie das Sentinel-Installationsprogramm (a tar.gz file) herunter und speichern Sie es im Verzeichnis `/tmp` im Clusterknoten.
3. Führen Sie die folgenden Schritte aus, um die Installation zu starten:

   3a Führen Sie folgende Kommandos aus:

   ```
   mount /dev/<SHARED1> /var/opt/novell
   cd /tmp
   tar -xvzf sentinel_server*.tar.gz
   cd sentinel_server*
   ./install-sentinel --record-unattended=/tmp/install.props
   ```

   3b Wählen Sie bei entsprechender Aufforderung die Konfigurationsmethode aus, indem Sie `2` für die benutzerdefinierte Konfiguration eingeben.
4. Führen Sie die Installation aus und konfigurieren Sie das Produkt entsprechend.
5. Starten Sie Sentinel und prüfen Sie die Basisfunktionen. Sie können die standardmäßige externe Clusterknoten-IP-Adresse verwenden, um auf das Produkt zuzugreifen.
6. Fahren Sie Sentinel herunter und dismounten Sie den freigegebenen Speicher. Verwenden Sie hierzu folgende Befehle:

   ```
   rcsentinel stop
   umount /var/opt/novell
   ```

   Durch diesen Schritt werden die Autostart-Skripte entfernt, sodass der Cluster das Produkt verwalten kann.

   ```
   cd /
   insserv -r sentinel
   ```

Installation der Hochverfügbarkeitsversion von Sentinel Appliance

Die Hochverfügbarkeitsversion von Sentinel Appliance umfasst die bereits installierte und konfigurierte Sentinel-Software. So konfigurieren Sie die Sentinel-Software für Hochverfügbarkeit:

1. Stellen Sie eine Verbindung zu einem der Clusterknoten her (node01) und öffnen Sie ein Konsolenfenster.
2. Wechseln Sie zu folgendem Verzeichnis:

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

3. Speichern Sie die Konfiguration:

   3a Führen Sie den folgenden Befehl aus:

   ```
   ./configure.sh --record-unattended=/tmp/install.props --no-start
   ```

   Mit diesem Befehl wird die Konfiguration in der Datei `install.props` gespeichert. Dies ist erforderlich, um die Clusterressourcen mit dem Skript `install-resources.sh` zu konfigurieren.

   3b Wählen Sie bei entsprechender Aufforderung die Konfigurationsmethode aus, indem Sie `2` für die benutzerdefinierte Konfiguration eingeben.

   3c Wenn Sie aufgefordert werden, das Passwort anzugeben, geben Sie `2` ein, um ein neues Passwort einzugeben.

   Mit `1` wird das Passwort nicht in der Datei `install.props` gespeichert.

4. Fahren Sie Sentinel mit dem folgenden Befehl herunter:

   ```
   rcsentinel stop
   ```

   Durch diesen Schritt werden die Autostart-Skripte entfernt, sodass der Cluster das Produkt verwalten kann.

   ```
   insserv -r sentinel
   ```

5. Verschieben Sie den Sentinel-Datenordner mit den nachfolgenden Befehlen in den freigegebenen Speicher. Durch dieses Verschieben können die Knoten über den freigegebenen Speicher auf den Sentinel-Datenordner zugreifen.

   ```
   mkdir -p /tmp/new

   mount /dev/<SHARED1> /tmp/new

   mv /var/opt/novell/* /tmp/new

   umount /tmp/new/
   ```

6. Überprüfen Sie das Verschieben des Sentinel-Datenordners in den freigegebenen Speicher mit den folgenden Befehlen:

   ```
   mount /dev/<SHARED1>  /var/opt/novell/

   umount /var/opt/novell/
   ```

Nachfolgende Installation im Knoten

- „Herkömmliche Hochverfügbarkeits-Installation“, auf Seite 204
- „Installation der Hochverfügbarkeitsversion Sentinel Appliance“, auf Seite 204

Wiederholen Sie die Installation in anderen Knoten:

Das ursprüngliche Sentinel-Installationsprogramm erstellt ein Benutzerkonto, das von dem Produkt verwendet werden kann, welches zum Zeitpunkt der Installation die nächste verfügbare Benutzer-ID verwendet. Bei nachfolgenden Installationen im unbeaufsichtigten Modus wird versucht, dieselbe Benutzer-ID für die Erstellung von Konten zu verwenden, doch es besteht die Möglichkeit, dass Konflikte auftreten (wenn die Clusterknoten zum Zeitpunkt der Installation nicht identisch sind). Es wird dringend empfohlen, eine der folgenden Maßnahmen zu ergreifen:

- Synchronisieren Sie die Benutzerkontodatenbank in allen Clusterknoten (manuell über LDAP oder ähnliches) und vergewissern Sie sich, dass die Synchronisierung vor weiteren Installationen durchgeführt wird. In diesem Fall erkennt das Installationsprogramm das vorhandene Benutzerkonto und verwendet das vorhandene Konto.
- Beobachten Sie die Ausgabe der nachfolgenden unbeaufsichtigten Installationen - eine Warnung wird angezeigt, wenn das Benutzerkonto nicht mit derselben Benutzer-ID erstellt werden konnte.

Herkömmliche Hochverfügbarkeits-Installation

1. Stellen Sie eine Verbindung zu allen weiteren Clusterknoten (node02) her und öffnen Sie ein Konsolenfenster.
2. Führen Sie folgende Befehle aus:

```
cd /tmp

scp root@node01:/tmp/sentinel_server*.tar.gz .

scp root@node01:/tmp/install.props .

tar -xvzf sentinel_server*.tar.gz

cd sentinel_server*

./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props

insserv -r sentinel
```

Installation der Hochverfügbarkeitsversion Sentinel Appliance

1. Stellen Sie eine Verbindung zu allen weiteren Clusterknoten (node02) her und öffnen Sie ein Konsolenfenster.
2. Führen Sie den folgenden Befehl aus:

```
insserv -r sentinel
```

3. Stoppen Sie die Sentinel-Dienste.

```
rcsentinel stop
```

4. Entfernen Sie das Sentinel-Verzeichnis.

```
rm -rf /var/opt/novell/*
```

Am Ende dieses Vorgangs sollte Sentinel in allen Knoten installiert sein, doch es funktioniert wahrscheinlich zunächst nur im ersten Knoten und in den anderen erst nach der Synchronisierung der verschiedenen Schlüssel, was nach der Konfiguration der Clusterressourcen der Fall ist.

Clusterinstallation

Installieren Sie die Clustersoftware nur für herkömmliche Hochverfügbarkeitsinstallationen. Die Hochverfügbarkeitsversion von Sentinel Appliance umfasst die Cluster-Software und erfordert keine manuelle Installation.

Verwenden Sie die folgende Prozedur für die Einrichtung der SLES-Hochverfügbarkeitserweiterung mit einem Sentinel-spezifischen Resource Agent-Overlay:

1. Installieren Sie die Clustersoftware auf jedem Knoten.
2. Registrieren Sie jeden Clusterknoten im Clustermanager.
3. Überprüfen Sie, ob jeder Clusterknoten in der Clusterverwaltungskonsole angezeigt wird.

   HINWEIS: Der OCF Resource Agent für Sentinel ist ein einfaches Shell-Skript, das eine Reihe von Überprüfungen durchführt, um festzustellen, ob Sentinel funktionsfähig ist. Wenn Sie zur Überwachung von Sentinel nicht den OCF Resource Agent verwenden, müssen Sie eine ähnliche Überwachungslösung für die lokale Clusterumgebung entwickeln. Um eine eigene Lösung zu entwickeln, überprüfen Sie den vorhandenen Resource Agent, der in der Datei `Sentinelha.rpm` im Sentinel-Downloadpaket gespeichert ist.

   ---

4. Installieren Sie die Kernsoftware der SLE-Hochverfügbarkeitserweiterung gemäß den Anweisungen in der Dokumentation zur SLE-Hochverfügbarkeitserweiterung.Informationen zur Installation der SLES-Add-ons finden Sie im Bereitstellungshandbuch.
5. Wiederholen Sie Schritt 4 auf allen Clusterknoten. Mit dem Add-on werden neben der zentralen Software für die Clusterverwaltung und Kommunikation auch viele Resource Agents installiert, die zur Überwachung von Clusterressourcen verwendet werden.
6. Installieren Sie einen zusätzlichen RPM, um die zusätzlichen Sentinel-spezifischen Cluster-Resource Agents bereitzustellen. Der Hochverfügbarkeits-RPM ist in der Datei `novell-Sentinelha-<Sentinel-Version>*.rpm` im standardmäßigen Sentinel-Download verfügbar, den Sie zur Installation des Produkts entpackt haben.
7. Kopieren Sie in jedem Clusterknoten die Datei `novell-Sentinelha-<Sentinel-Version>*.rpm` in das Verzeichnis `/tmp`. Führen Sie dann folgende Befehle aus:

```
cd /tmp
```

```
rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

Clusterkonfiguration

Sie müssen die Clustersoftware konfigurieren, um jeden Clusterknoten als Mitglied des Clusters zu registrieren. Als Teil der Konfiguration können Sie auch Fencing und STONITH-Ressourcen („Shoot The Other Node In The Head“) einrichten, um die Clusterkonsistenz zu gewährleisten.

WICHTIG: Die Prozeduren in diesem Abschnitt verwenden die Befehle `rcopenais` und `openais`, die nur mit SLES 11 SP4 funktionieren. Verwenden Sie für SLES 12 SP2 und höher den Befehl `systemctl pacemaker.service`.

Verwenden Sie beispielsweise für den Befehl `/etc/rc.d/openais start` den Befehl `systemctl start pacemaker.service`.

Verwenden Sie die folgende Prozedur für die Clusterkonfiguration:

Für diese Lösung verwenden Sie private IP-Adressen für die interne Clusterkommunikation und Unicast, um zu vermeiden, dass eine Multicast-Adresse von einem Netzwerkadministrator angefragt werden muss. Außerdem müssen Sie ein iSCSI-Ziel verwenden, das auf derselben virtuellen SLES-Maschine konfiguriert ist, auf der auch der freigegebene Speicher gehostet wird, um als SBD-Gerät (Systemspaltungserkennung) für Fencing-Zwecke zu dienen.

SBD-Einrichtung

1. Stellen Sie eine Verbindung zu `storage03` her und starten Sie eine Konsolensitzung. Erstellen Sie mit dem folgenden Befehl eine leere Datei beliebiger Größe:

   `dd if=/dev/zero of=/sbd count=<Dateigröße> bs=<Bit-Größe>`

   Mit folgendem Befehl erstellen Sie zum Beispiel eine 1-MB-Datei voller Nullen, die vom Pseudogerät `/dev/zero` kopiert wird:

   ```
   dd if=/dev/zero of=/sbd count=1024 bs=1024
   ```

2. Führen Sie YaST von der Befehlszeile oder der grafischen Benutzeroberfläche aus: `/sbin/yast`
3. Wählen Sie **Netzwerkdienste** > **iSCSI-Ziel** aus.
4. Klicken Sie auf **Ziele** und wählen Sie das vorhandene Ziel aus.
5. Wählen Sie **Bearbeiten** aus. Auf der Benutzeroberfläche wird eine Liste von verfügbaren LUNs (Laufwerken) angezeigt.
6. Wählen Sie **Hinzufügen** aus, um ein neues LUN hinzuzufügen.
7. Belassen Sie die LUN-Nummer bei 2. Durchsuchen Sie das Dialogfeld **Pfad** und wählen Sie die Datei `/sbd` aus, die Sie erstellt haben.
8. Belassen Sie die anderen Optionen wie standardmäßig eingestellt, wählen Sie **OK** und dann **Weiter** aus und klicken Sie anschließend erneut auf **Weiter**, um die Standardoptionen für die Authentifizierung auszuwählen.
9. Beenden Sie die Konfiguration mit **Fertig stellen**. Starten Sie die Dienste neu, falls erforderlich. Beenden Sie YaST.

HINWEIS: Bei den folgenden Schritten müssen alle Clusterknoten den Hostnamen aller anderen Clusterknoten auflösen können (im Dateisynchronisierungsdienst csync2 treten andernfalls Fehler auf). Wenn das DNS nicht eingerichtet oder verfügbar ist, fügen Sie jedem Host in Datei `/etc/hosts` Einträge hinzu, die jede IP-Adresse und deren Hostnamen auflisten (wie durch den Hostnamenbefehl gemeldet). Achten Sie auch darauf, einer Loopback-IP-Adresse keinen Hostnamen zuzuweisen.

Führen Sie die folgenden Schritte aus, um am Server unter der IP-Adresse 10.0.0.3 (storage03) ein iSCSI-Ziel für das SBD-Gerät auszuweisen.

Knotenkonfiguration

Stellen Sie eine Verbindung zu einem Clusterknoten (node01) her und öffnen Sie eine Konsole:

1. YaST ausführen.
2. Öffnen Sie **Netzwerkdienste** > **iSCSI-Initiator**.
3. Wählen Sie **Verbundene Ziele** aus und anschließend das iSCSI-Ziel, das Sie oben konfiguriert haben.
4. Wählen Sie die Option **Abmelden** aus und melden Sie sich vom Ziel ab.
5. Wechseln Sie zur Registerkarte **Erkannte Ziele**, wählen Sie das **Ziel** aus und melden Sie sich erneut an, um die Geräteliste zu aktualisieren (lassen Sie für den Start die Option **automatisch** aktiviert und deaktivieren Sie **Keine Authentifizierung**).
6. Wählen Sie **OK** aus, um das iSCSI-Initior-Werkzeug zu beenden.

7. Öffnen Sie **System** > **Partitionierer** und kennzeichnen Sie das SBD-Gerät als 1MB IET-VIRTUAL-DISK. Es wird als **/dev/sdd** oder ähnlich aufgeführt – notieren Sie sich, wie es heißt.
8. Beenden Sie YaST.
9. Führen Sie den Befehl `ls -l /dev/disk/by-id/` und notieren Sie sich die Geräte-ID, die mit dem Gerätenamen verknüpft ist, den Sie oben gefunden haben.
10. (Bedingt) Führen Sie einen der folgenden Befehle aus:
    - Unter SLES 11 SP4:

      `sleha-init`
    - Unter SLES 12 SP1 oder höher:

      `ha-cluster-init`
11. Wenn Sie aufgefordert werden, die Netzwerkadresse für die Verbindung einzugeben, geben Sie die IP-Adresse des externen NIC an (172.16.0.1).
12. Akzeptieren Sie die standardmäßige Multicast-Adresse und den Port. Sie werden später überschrieben.
13. Geben Sie `y` ein, um SBD zu aktivieren. Geben Sie anschließend die `/dev/disk/by-id/<Geräte-ID>` an, wobei `<Geräte-ID>` die ID bezeichnet, die Sie oben gefunden haben (Sie können die Tabulatortaste verwenden, um den Pfad automatisch einzutragen).
14. (Bedingt) Geben Sie `N` ein, wenn die folgende Aufforderung angezeigt wird:

    ```
    Do you wish to configure an administration IP? [y/N]
    ```

    Zur Konfiguration einer IP-Adresse für die Verwaltung, geben Sie während der in „Ressourcenkonfiguration“, auf Seite 209 beschriebenen Prozedur die virtuelle IP-Adresse an.
15. Beenden Sie den Assistenten und vergewissern Sie sich, dass keine Fehler gemeldet wurden.
16. Starten Sie YaST.
17. Wählen Sie **Hochverfügbarkeit** > **Cluster** aus (oder bei einigen Systemen nur „Cluster“).
18. Vergewissern Sie sich, dass im Feld auf der linken Seite die Option **Kommunikationskanäle** ausgewählt ist.
19. Gehen Sie mit der Tabulatortaste zur ersten Zeile der Konfiguration und ändern Sie die Auswahl von **udp** zu **udpu** (dadurch wird Multicast deaktiviert und Unicast ausgewählt).
20. Wählen Sie die Option **Mitgliedsadresse hinzufügen** aus und geben Sie diesen Knoten (172.16.0.1) an. Wiederholen Sie dies und fügen Sie den (die) anderen Clusterknoten hinzu: 172.16.0.2.
21. Wählen Sie zum Beenden der Konfiguration **Fertig stellen** aus.
22. Beenden Sie YaST.
23. Führen Sie den Befehl /etc/rc.d/openais aus, um die Clusterdienste mit dem neuen Synchronisierungsprotokoll neu zu starten.

Stellen Sie eine Verbindung zu jedem weiteren Clusterknoten (node02) her und öffnen Sie die Konsole:

1. YaST ausführen.
2. Öffnen Sie **Netzwerkdienste** > **iSCSI-Initiator**.
3. Wählen Sie **Verbundene Ziele** aus und anschließend das iSCSI-Ziel, das Sie oben konfiguriert haben.
4. Wählen Sie die Option **Abmelden** aus und melden Sie sich vom Ziel ab.

5 Wechseln Sie zur Registerkarte **Erkannte Ziele**, wählen Sie das **Ziel** aus und melden Sie sich erneut an, um die Geräteliste zu aktualisieren (lassen Sie für den Start die Option **automatisch** aktiviert und deaktivieren Sie **Keine Authentifizierung**).

6 Wählen Sie **OK** aus, um das iSCSI-Inititor-Werkzeug zu beenden.

7 (Bedingt) Führen Sie einen der folgenden Befehle aus:

- Unter SLES 11 SP4:

  ```
  sleha-join
  ```

- Unter SLES 12 SP1 oder höher:

  ```
  ha-cluster-join
  ```

8 Geben Sie die IP-Adresse des ersten Clusterknotens ein.

(Bedingt) Wenn der Cluster nicht richtig gestartet wird, führen Sie die folgenden Schritte aus:

1 Führen Sie den Befehl `crm status` aus, um zu überprüfen, ob die Knoten verbunden sind. Wenn die Knoten nicht verbunden sind, starten Sie alle Knoten im Cluster neu.

2 Kopieren Sie die Datei `/etc/corosync/corosync.conf` manuell von `node01` zu `node02` oder führen Sie `csync2 -x -v` auf `node01` aus. Sie können den Cluster auch manuell über YaST im `node02` einrichten.

3 (Bedingt) Wenn mit dem Befehl `csync2 -x -v` aus Schritt 1 nicht alle Dateien synchronisiert werden, führen Sie folgende Prozedur durch:

3a Leeren Sie die csync2-Datenbank im Verzeichnis `/var/lib/csync2` auf allen Knoten.

3b Aktualisieren Sie auf allen Knoten die csync2-Datenbank, um sie auf den Stand des Dateisystems zu bringen. Merken Sie dabei nichts für die Synchronisierung mit anderen Servern vor:

```
csync2 -cIr /
```

3c Führen Sie auf dem aktiven Knoten Folgendes aus:

3c1 Ermitteln Sie alle Unterschiede zwischen den aktiven und passiven Knoten und kennzeichnen Sie diese Unterschiede für die Synchronisierung:

```
csync2 -TUXI
```

3c2 Setzen Sie die Datenbank zurück, um zu erzwingen, dass der aktive Knoten alle Konflikte überschreibt:

```
csync2 -fr /
```

3c3 Starten Sie die Synchronisierung für alle anderen Knoten:

```
csync2 -xr /
```

3d Überprüfen Sie auf allen Knoten, ob alle Dateien synchronisiert sind:

```
csync2 -T
```

Dieser Befehl listet nur die nicht synchronisierten Dateien auf.

4 Führen Sie auf Knoten `node02` den folgenden Befehl aus:

Unter SLES 11 SP4:

```
/etc/rc.d/openais start
```

Unter SLES 12 SP1 oder höher:

```
systemctl start pacemaker.service
```

(Bedingt) Wenn der `xinetd`-Service den neuen `csync2`-Service nicht ordnungsgemäß hinzufügt, funktioniert das Skript nicht richtig. Der `xinetd`-Service ist erforderlich, damit der andere Knoten die Clusterkonfigurationsdateien bis zu diesem Knoten synchronisieren kann. Wenn Sie Fehler wie `csync2 run failed` sehen, könnte dieses Problem bei Ihnen aufgetreten sein.

Führen Sie zur Fehlerbehebung den Befehl `kill -HUP `cat /var/run/xinetd.init.pid` aus und führen Sie anschließend das Skript`sleha-join` erneut aus.

5 Führen Sie auf jedem Clusterknoten `crm_mon` aus, um zu überprüfen, ob der Cluster richtig ausgeführt wird. Sie können den Cluster auch mit 'hawk', der Webkonsole, überprüfen. Der standardmäßige Anmeldename ist `hacluster`, das Passwort lautet `linux`.

(Bedingt) Führen Sie je nach Umgebung die folgenden Aufgaben aus, um zusätzliche Parameter zu bearbeiten:

1 Um zu verhindern, dass der Ausfall eines Knotens in einem Cluster mit zwei Knoten nicht das gesamte Cluster beendet, legen Sie die globale Clusteroption `no-quorum-policy` auf `ignore` fest:

```
crm configure property no-quorum-policy=ignore
```

HINWEIS: Wenn der Cluster aus mehr als zwei Knoten besteht, legen Sie diese Option nicht fest.

---

2 Um sicherzustellen, dass der Clustermanager zulässt, dass Ressourcen vor Ort ausgeführt oder verschoben werden, legen Sie die globale Clusteroption `default-resource-stickiness` auf 1 fest:

```
crm configure property default-resource-stickiness=1
```.

Ressourcenkonfiguration

Mit der SLE-Hochverfügbarkeitserweiterung werden standardmäßig Resource Agents bereitgestellt. Wenn Sie die SLE-Hochverfügbarkeitserweiterung nicht verwenden möchten, müssen Sie diese zusätzlichen Ressourcen mit einer alternativen Technologie überwachen:

- Eine Dateisystemressource, die dem freigegebenen Speicher entspricht, den die Software verwendet.
- Eine IP-Adressenressource, die der virtuellen IP-Adresse entspricht, über die auf die Services zugegriffen wird.
- Die PostgreSQL-Datenbanksoftware, die Konfigurations- und Ereignis-Metadaten speichert.

Verwenden Sie die folgende Prozedur für die Ressourcenkonfiguration:

Das Skript `crm` hilft Ihnen bei der Clusterkonfiguration. Das Skript zieht relevante Konfigurationsvariablen aus der Datei der unbeaufsichtigten Einrichtung, die als Teil der Sentinel-Installation erstellt wurde. Wenn Sie keine Einrichtungsdatei erstellt haben oder die Konfiguration der Ressourcen ändern möchten, können Sie das Skript mit der folgenden Prozedur entsprechend bearbeiten.

1 Stellen Sie eine Verbindung zu dem Knoten her, auf dem Sie Sentinel ursprünglich installiert haben.

HINWEIS: Dies muss der Knoten sein, auf dem Sie die vollständige Sentinel-Installation ausgeführt haben.

---

2 Bearbeiten Sie das Skript so, dass es den folgenden Angaben entspricht (`<SHARED1>` ist das zuvor erstellte freigegebene Volume):

```
mount /dev/<SHARED1> /var/opt/novell

cd /usr/lib/ocf/resource.d/novell

./install-resources.sh
```

3 (Bedingt) Möglicherweise treten Probleme mit den neuen Ressourcen im Cluster auf. Ist dies der Fall, führen Sie den folgenden Befehl auf node02 aus:

Unter SLES 11 SP4:

```
/etc/rc.d/openais start
```

Unter SLES 12 SP1:

```
systemctl start pacemaker.service
```

4 Das Skript `install-resources.sh` fordert Sie auf, einige Werte einzugeben, nämlich die virtuelle IP-Adresse, die für den Zugriff auf Sentinel verwendet werden soll, und den Gerätenamen des freigegebenen Speichers. Die erforderlichen Clusterressourcen werden dann automatisch erstellt. Beachten Sie, dass das Skript ein bereits eingehängtes freigegebenes Volume benötigt sowie dass dafür die Datei der unbeaufsichtigten Installation, die bei der Sentinel-Installation erstellt wurde, vorhanden sein muss (`/tmp/install.props`). Sie brauchen dieses Skript nur im ersten installierten Knoten auszuführen. Alle relevanten Konfigurationsdateien werden automatisch mit den anderen Knoten synchronisiert.

5 Wenn Ihre Umgebung von dieser von empfohlenen Lösung abweicht, können Sie die Datei `resources.cli` bearbeiten (im selben Verzeichnis) und die Definitionen der Primitivdaten dort ändern. Beispielsweise verwendet die empfohlene Lösung eine einfache Dateisystemressource. Sie möchten stattdessen vielleicht eine eher Cluster-bewusste cLVM-Ressource verwenden.

6 Nach der Ausführung des Shell-Skripts können Sie einen `crm status`-Befehl ausstellen. Die Ausgabe sollte folgendermaßen aussehen:

```
crm status
```

```
Last updated: Thu Jul 26 16:34:34 2012
Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
Stack: openais
Current DC: node01 - partition with quorum
Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
2 Nodes configured, 2 expected votes
5 Resources configured.

Online: [ node01, node02 ]
stonith-sbd    (stonith:external/sbd):    Started node01
 Resource Group: sentinelgrp
     sentinelip    (ocf::heartbeat:IPaddr2):    Started node01
     sentinelfs    (ocf::heartbeat:Filesystem):    Started node01
     sentineldb    (ocf::novell:pgsql):    Started node01
     sentinelserver    (ocf::novell:sentinel):    Started node01
```

7 Zu diesem Zeitpunkt sollten die relevanten Sentinel-Ressourcen im Cluster bereits konfiguriert sein. Sie können nachprüfen, wie sie konfiguriert und im Clusterverwaltungswerkzeug gruppiert sind, indem Sie zum Beispiel den crm-Status ausführen.

Konfiguration des Sekundärspeichers

Führen Sie die folgenden Schritte aus, um den Sekundärspeicher so zu konfigurieren, dass Sentinel Ereignispartitionen zu günstigeren Speichern migrieren kann:

HINWEIS: Dieser Prozess ist optional und der Sekundärspeicher muss nicht wie der Rest des Systems hochverfügbar sein. Sie können ein beliebiges Verzeichnis (von einem SAN eingehängt oder nicht), ein NFS- oder ein CIFS-Volume verwenden.

1. Klicken Sie in der oberen Menüleiste der Benutzeroberfläche von Sentinel Main auf **Speicher**.
2. Wählen Sie **Konfiguration** aus.
3. Wählen Sie eines der Optionsfelder unter „Sekundärspeicher nicht konfiguriert“ aus.

Verwenden Sie ein einfaches iSCSI-Ziel als freigegebenen Netzwerkspeicherort, dessen Konfiguration in etwa dem Primärspeicher entspricht. In der Produktionsumgebung setzen Sie möglicherweise andere Speichermethoden ein.

Mit der folgenden Prozedur können Sie den Sekundärspeicher für Sentinel konfigurieren:

HINWEIS: Für das iSCSI-Ziel wird das Ziel als ein Verzeichnis gemountet, das als sekundärer Speicher dient. Das eingehängte Verzeichnis muss auf ähnliche Weise wie die Konfiguration des Primärspeicherdateisystems als Dateisystemressource konfiguriert werden. Dies wurde nicht automatisch als Teil des Ressourceninstallationsskripts eingerichtet, da es andere mögliche Variationen gibt.

1. Sehen Sie sich die oben beschriebenen Schritte an, um zu ermitteln, welche Partition zur Verwendung als Sekundärspeicher erstellt wurde (`/dev/<NETWORK1>` oder etwas wie `/dev/sdc1`). Erstellen Sie gegebenenfalls ein leeres Verzeichnis, in dem die Partition eingehängt werden kann (wie `/var/opt/netdata`).
2. Richten Sie das Netzwerkdateisystem als Clusterressource ein. Verwenden Sie dazu die Benutzeroberfläche von Sentinel Main oder führen Sie den folgenden Befehl aus:

   ```
   crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
   ```

   wobei `/dev/<NETWORK1>` die Partition bezeichnet, die oben im Abschnitt „Einrichtung des freigegebenen Speichers“ erstellt wurde, und <PATH> ein lokales Verzeichnis, in dem die Partition eingehängt werden kann.
3. Fügen Sie die neue Ressource der Gruppe der verwalteten Ressourcen hinzu:

   ```
   crm resource stop sentinelgrp
   crm configure delete sentinelgrp
   crm configure group sentinelgrp sentinelip sentinelfs sentinelnetfs sentineldb sentinelserver
   crm resource start sentinelgrp
   ```
4. Sie können eine Verbindung zu dem Knoten herstellen, auf dem aktuell die Ressourcen gehostet werden (verwenden Sie den Befehl `crm status` oder `Hawk`) und vergewissern Sie sich, dass der Sekundärspeicher korrekt eingehängt wurde (verwenden Sie den Befehl`mount`).
5. Melden Sie sich bei der Benutzeroberfläche von Sentinel Main an.
6. Wählen Sie **Speicher** und **Konfiguration** aus und anschließend das **SAN (lokal eingehängt)** unter „Sekundärspeicher“, das nicht konfiguriert ist.
7. Geben Sie den Pfad ein, unter dem der Sekundärspeicher eingehängt ist, zum Beispiel `/var/opt/netdata`.

Verwenden Sie einfache Versionen der erforderlichen Ressourcen, wie den einfachen Resource Agent für das Dateisystem. Sie können komplexere Clusterressourcen wie cLVM (eine Version des logischen Volumes des Dateisystems) verwenden, falls erforderlich.

38 Konfiguration von Sentinel HA als SSDM

In diesem Kapitel wird erklärt, wie sich Sentinel HA als SSDM konfigurieren lässt. Die Anleitung gilt sowohl für herkömmliche als auch für Appliance-Installationen.

So konfigurieren Sie Sentinel HA als SSDM:

1. Installieren und konfigurieren Sie skalierbaren Speicher für Sentinel. Weitere Informationen finden Sie unter Kapitel 13, „Installation und Einrichtung von skalierbarem Speicher“, auf Seite 85.
2. Aktivieren Sie den skalierbaren Speicher auf dem aktiven Knoten. Weitere Informationen finden Sie im Abschnitt „Enabling Scalable Storage Post-Installation“ (Aktivierung des skalierbaren Speichers nach der Installation) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).
3. Führen Sie auf dem aktiven Knoten folgenden Befehl aus:

   ```
   csync2 -x -v
   ```

   Damit wird die SSDM-Konfiguration auf allen passiven Knoten synchronisiert.
4. (Bedingt) Wenn mit dem Befehl `csync2 -x -v` aus Schritt 3 nicht alle Dateien synchronisiert werden, führen Sie folgende Schritte aus:

   4a Leeren Sie die csync2-Datenbank (im Verzeichnis `/var/lib/csync2`) auf allen Knoten.

   4b Führen Sie auf allen Servern den folgenden Befehl aus, um die csync2-Datenbank auf den Stand des Dateisystems zu bringen. Merken Sie dabei nichts für die Synchronisierung mit anderen Servern vor:

   ```
   csync2 -cIr /
   ```

   4c Ermitteln Sie mit folgendem Befehl alle Unterschiede zwischen autorisierten und Remote-Servern und setzen Sie Synchronisierungsmarker:

   ```
   csync2 -TUXI
   ```

   4d Setzen Sie mit folgendem Befehl die Datenbank zurück, um die Priorität des aktuellen Servers bei allen Konflikten zu erzwingen:

   ```
   csync2 -fr /
   ```

   4e Starten Sie mit folgendem Befehl die Synchronisierung mit allen anderen Servern:

   ```
   csync2 -xr /
   ```

   4f Überprüfen Sie mit folgendem Befehl, ob alle Dateien synchronisiert sind:

   ```
   csync2 -T
   ```

   Bei diesem Befehl sind nach erfolgreicher Synchronisierung keine Dateien aufgelistet.

39 Aufrüsten von Sentinel in einer Hochverfügbarkeits-Umgebung

Wenn Sie Sentinel in einer Hochverfügbarkeits-Umgebung aufrüsten, rüsten Sie zunächst die passiven Knoten und dann die aktiven Knoten im Cluster auf.

Voraussetzungen

- Laden Sie das aktuellste Installationsprogramm von der Download-Website herunter.
- Wenn Sie das SLES-Betriebssystem mit Kernel-Version 3.0.101 oder höher verwenden, müssen Sie den Watchdog-Treiber manuell in den Computer laden. Den richtigen Watchdog-Treiber für Ihre Computer-Hardware erhalten Sie bei Ihrem Hardware-Händler. So laden Sie den Watchdog-Treiber:
  1. Zum Laden des Watchdog-Treibers in der aktuellen Sitzung führen Sie in der Befehlszeile den folgenden Befehl aus:

     ```
     /sbin/modprobe -v --ignore-install <Name des Watchdog-Treibers>
     ```

  2. Soll der Computer den Watchdog-Treiber automatisch bei jedem Booten laden, fügen Sie die folgende Zeile in die Datei `/etc/init.d/boot.local` ein:

     ```
     /sbin/modprobe -v --ignore-install <Name des Watchdog-Treibers>
     ```

Aufrüsten einer herkömmlichen Sentinel-Hochverfügbarkeits-Installation

In diesem Abschnitt wird sowohl das Aufrüsten einer herkömmlichen Sentinel-Installation als auch das Aufrüsten des Betriebssystems in einer herkömmlichen Sentinel-Installation erläutert.

WICHTIG: Die Prozeduren in diesem Abschnitt verwenden die Befehle `rcopenais` und `openais`, die nur mit SLES 11 SP4 funktionieren. Verwenden Sie für SLES 12 SP2 und höher den Befehl `systemctl pacemaker.service`.

Verwenden Sie beispielsweise für den Befehl `/etc/rc.d/openais start` den Befehl `systemctl start pacemaker.service`.

Aufrüsten einer Sentinel-Hochverfügbarkeits-Installation

1 Aktivieren Sie den Wartungsmodus im Cluster:

```
crm configure property maintenance-mode=true
```

Der Wartungsmodus trägt dazu bei, Störungen der ausgeführten Clusterressourcen während der Aktualisierung von Sentinel zu vermeiden. Sie können den Befehl von einem beliebigen Clusterknoten aus ausführen.

2 Überprüfen Sie, ob der Wartungsmodus aktiv ist:

```
crm status
```

Die Clusterressourcen sollten im Zustand „nicht verwaltet“ angezeigt werden.

3 Rüsten Sie den passiven Clusterknoten auf:

3a Stoppen Sie den Clusterstapel:

```
rcopenais stop
```

Durch Stoppen des Clusterstapels wird sichergestellt, dass auf die Ressourcen weiterhin zugegriffen werden kann und das Fencing der Knoten wird verhindert.

3b Melden Sie sich am Server, auf dem Sentinel aufgerüstet werden soll, als `root` an.

3c Extrahieren Sie die Installationsdateien aus der TAR-Datei:

```
tar xfz <Installationsdatei-Name>
```

3d Führen Sie im Verzeichnis, in dem die Installationsdateien extrahiert wurden, folgenden Befehl aus:

```
./install-sentinel --cluster-node
```

3e Starten Sie nach dem Abschluss der Aufrüstung den Clusterstapel neu:

```
rcopenais start
```

Wiederholen Sie Schritt 3 für alle passiven Clusterknoten.

3f Entfernen Sie die Autostart-Skripte, sodass der Cluster das Produkt verwalten kann.

```
cd /
insserv -r sentinel
```

4 Rüsten Sie den aktiven Clusterknoten auf:

4a Sichern Sie die Konfiguration, und erstellen Sie einen ESM-Export.

Weitere Informationen zum Sichern von Daten finden Sie im Abschnitt „Backing Up and Restoring Data (Sichern und Wiederherstellen von Daten)“ im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).

4b Stoppen Sie den Clusterstapel:

```
rcopenais stop
```

Durch Stoppen des Clusterstapels wird sichergestellt, dass auf die Ressourcen weiterhin zugegriffen werden kann und das Fencing der Knoten wird verhindert.

4c Melden Sie sich am Server, auf dem Sentinel aufgerüstet werden soll, als `root` an.

4d Führen Sie den folgenden Befehl aus, um die Installationsdateien aus der TAR-Datei zu extrahieren:

```
tar xfz <Installationsdatei-Name>
```

4e Führen Sie im Verzeichnis, in dem die Installationsdateien extrahiert wurden, folgenden Befehl aus:

```
./install-sentinel
```

4f Starten Sie nach dem Abschluss der Aufrüstung den Clusterstapel:

```
rcopenais start
```

4g Entfernen Sie die Autostart-Skripte, sodass der Cluster das Produkt verwalten kann.

```
cd /
insserv -r sentinel
```

4h Führen Sie den folgenden Befehl aus, um alle Änderungen der Konfigurationsdateien zu synchronisieren:

```
csync2 -x -v
```

5 Deaktivieren Sie den Wartungsmodus im Cluster:

```
crm configure property maintenance-mode=false
```

Sie können den Befehl von einem beliebigen Clusterknoten aus ausführen.

6 Überprüfen Sie, ob der Wartungsmodus inaktiv ist:

```
crm status
```

Die Clusterressourcen sollten im Zustand „gestartet“ angezeigt werden.

7 (Optional:) Überprüfen Sie, ob die Sentinel-Aufrüstung erfolgreich war:

```
rcsentinel version
```

Aufrüsten des Betriebssystems

In diesem Abschnitt wird erläutert, wie sich das Betriebssystem in einem Sentinel-HA-Cluster auf eine Hauptversion aufrüsten lässt, z. B. von SLES 11 auf SLES 12. Bei der Betriebssystemaufrüstung sind einige Konfigurationsschritte vorzunehmen, damit Sentinel HA danach ordnungsgemäß funktioniert.

Befolgen Sie die Anleitungen in den folgenden Abschnitten:

- „Aufrüsten des Betriebssystems“, auf Seite 217
- „Konfigurieren von iSCSI-Zielen“, auf Seite 218
- „Konfigurieren von iSCSI-Initiatoren“, auf Seite 219
- „Konfigurieren des HA-Clusters“, auf Seite 220

Aufrüsten des Betriebssystems

So rüsten Sie das Betriebssystem auf:

1 Melden Sie sich an einem beliebigen Knoten im Sentinel-HA-Cluster als `root`-Benutzer an.

2 Aktivieren Sie den Wartungsmodus im Cluster mit dem folgenden Befehl:

```
crm configure property maintenance-mode=true
```

Der Wartungsmodus trägt dazu bei, Störungen der ausgeführten Clusterressourcen während der Aufrüstung des Betriebssystems zu vermeiden.

3 Überprüfen Sie mit dem folgenden Befehl, ob der Wartungsmodus aktiv ist:

```
crm status
```

Die Clusterressourcen sollten im Zustand „nicht verwaltet“ angezeigt werden.

4 Vergewissern Sie sich, dass Sie Sentinel auf allen Clusterknoten auf Version 8.2 oder höher aufgerüstet haben.

5 Vergewissern Sie sich, dass alle Knoten im Cluster für SLES und SLESHA registriert sind.

6 Führen Sie diese Schritte aus, um das Betriebssystem auf dem passiven Clusterknoten aufzurüsten:

6a Führen Sie folgenden Befehl aus, um den Clusterstapel zu stoppen:

`rcopenais stop`

Durch Stoppen des Clusterstapels wird sichergestellt, dass auf die Ressourcen weiterhin zugegriffen werden kann und das Fencing der Knoten wird verhindert.

6b Führen Sie ein Upgrade des Betriebssystems aus. Weitere Informationen finden Sie in Aufrüsten des Betriebssystems.

7 Wiederholen Sie Schritt 6 auf allen passiven Knoten, um das Betriebssystem aufzurüsten.

8 Wiederholen Sie Schritt 6 auf dem aktiven Knoten, um dessen Betriebssystem aufzurüsten.

9 Wiederholen Sie Schritt 6b, um das Betriebssystem des freigegebenen Speichers aufzurüsten.

10 Stellen Sie sicher, dass das Betriebssystem auf jedem Knoten im Cluster auf SLES 12 SP3 aufgerüstet ist.

Konfigurieren von iSCSI-Zielen

So konfigurieren Sie iSCSI-Ziele:

1 Überprüfen Sie, ob auf dem freigegebenen Speicher das iSCSI-LIO-Paket installiert ist. Ist es das nicht, öffnen Sie YaST2 Software Management und installieren die das iSCSI-LIO-Paket (`iscsiliotarget` RPM).

2 Führen Sie die folgenden Schritte auf jedem Knoten im Cluster aus:

2a Öffnen Sie mit folgendem Befehl die Datei, die den iSCSI-Initiatornamen enthält:

```
cat /etc/iscsi/initiatorname.iscsi
```

2b Notieren Sie sich den Initiatornamen, da dieser bei der Konfiguration von iSCSI-Initiatoren zur Anwendung kommt:

Beispiel:

```
InitiatorName=iqn.1996-04.de.suse:01:441d6988994
```

Initiatornamen werden bei der Konfiguration von iSCSI-Ziel-Clients benötigt.

3 Klicken Sie auf **Dienst** und wählen Sie die Option **Beim Booten** aus, um sicherzustellen, dass der Dienst beim Booten des Betriebssystems gestartet wird.

4 Deaktivieren Sie auf der Registerkarte **Global** die Option **Keine Authentifizierung**, um die Authentifizierung zu aktivieren, und geben Sie dann den Benutzernamen und das Passwort für die eingehende und ausgehende Authentifizierung an.

Die Option **Keine Authentifizierung** ist standardmäßig aktiviert. Sie sollten jedoch die Authentifizierung aktivieren, um sicherzustellen, dass die Konfiguration sicher ist.

5 Klicken Sie auf **Ziele** und anschließend auf **Hinzufügen**, um ein neues Ziel hinzuzufügen.

6 Klicken Sie auf **Hinzufügen**, um ein neues LUN hinzuzufügen.

7 Belassen Sie die LUN-Nummer als 0, durchsuchen Sie das Dialogfeld **Pfad** (unter Type=fileio) und wählen Sie die Datei `/localdata` aus, die Sie erstellt haben. Wenn Sie über einen dedizierten Datenträger für den Speicher verfügen, geben Sie ein Blockgeräte an wie zum Beispiel `/dev/sdc`.

8 Wiederholen Sie die Schritte 6 und 7. Fügen Sie diesmal LUN 1 hinzu und wählen Sie `/networkdata` aus.

9 Wiederholen Sie die Schritte 6 und 7. Fügen Sie diesmal LUN 2 hinzu und wählen Sie `/sbd` aus.

10 Behalten Sie für die anderen Optionen die Standardwerte bei. Klicken Sie auf **Weiter**.

11 Klicken Sie auf **Hinzufügen**. Wenn Sie zur Eingabe des Clientnamens aufgefordert werden, geben Sie den in Schritt 2 notierten Initiatornamen an. Wiederholen Sie diesen Schritt, um alle Clientnamen unter Angabe des Initiatornamens hinzuzufügen.

Die Clientnamen werden in der Clientliste aufgeführt.

12 (Bedingt) Wenn Sie in Schritt 4 die Authentifizierung aktiviert haben, geben Sie den im selben Schritt angegebenen Berechtigungsnachweis für die Authentifizierung ein.

   Wählen Sie einen Client und dann **Edit Auth** > **Incoming Authentication** (Authentifizierung bearbeiten > eingehende Authentifizierung) aus und geben Sie den Benutzernamen und das Passwort an. Wiederholen Sie dies für alle Clients.

13 Klicken Sie auf **Weiter**, um die Standardoptionen für die Authentifizierung auszuwählen, und dann auf **Fertig stellen**, um die Konfiguration zu beenden. Wenn Sie dazu aufgefordert werden, starten Sie iSCSI neu.

14 Beenden Sie YaST.

Konfigurieren von iSCSI-Initiatoren

So konfigurieren Sie iSCSI-Initiatoren:

1 Stellen Sie eine Verbindung zu einem der Clusterknoten (node01) her und starten Sie YaST.

2 Klicken Sie auf **Netzwerkdienste** > **iSCSI-Initiator**.

3 Installieren Sie bei entsprechender Aufforderung die erforderliche Software (`iscsiclient`-RPM).

4 Klicken Sie auf **Dienst** und wählen Sie **Beim Booten** aus, um sicherzustellen, dass der iSCSI-Dienst beim Booten gestartet wird.

5 Klicken Sie auf **Erkannte Ziele**.

   HINWEIS: Löschen Sie angezeigte iSCSI-Ziele, die schon vorher vorhanden waren.

   Wählen Sie **Ermittlung** aus, um ein neues iSCSI-Ziel hinzuzufügen.

6 Geben Sie die IP-Adresse des iSCSI-Ziels an (10.0.0.3).

   (Bedingt) Wenn Sie die Authentifizierung in Schritt 4 in „Konfigurieren von iSCSI-Zielen“, auf Seite 218 aktiviert haben, deaktivieren Sie **Keine Authentifizierung**. Geben Sie im Bereich **Outgoing Authentication** (Ausgehende Authentifizierung) den Berechtigungsnachweis für die Authentifizierung ein, den Sie bei der Konfiguration der iSCSI-Ziele angegeben haben.

   Klicken Sie auf **Weiter**.

7 Wählen Sie zunächst das erkannte iSCSI-Ziel mit der IP-Adresse 10.0.0.3 aus und anschließend die Option **Anmelden**.

8 Führen Sie die folgenden Schritte aus:

   8a Wechseln Sie im Dropdown-Menü **Startup** (Start) zu „Automatic“ (Automatisch).

   8b (Bedingt) Wenn Sie die Authentifizierung aktiviert haben, deaktivieren Sie **Keine Authentifizierung**.

   Der angegebene Berechtigungsnachweis (Benutzername und Passwort) sollte im Abschnitt **Outgoing Authentication** (Ausgehende Authentifizierung) angezeigt werden. Wird er es nicht, geben Sie ihn dort ein.

   8c Klicken Sie auf **Weiter**.

9 Wechseln Sie zur Registerkarte **Verbundene Ziele**, um sicherzustellen, dass Sie mit dem Ziel verbunden sind.

10 Beenden Sie die Konfiguration. Damit sollten die iSCSI-Ziele als Blockgeräte im Clusterknoten eingehängt sein.

11 Wählen Sie im YaST-Hauptmenü **System** > **Partitionierer** aus.

12 In der Systemansicht sollten alle neuen Festplatten vom Typ LIO-ORG-FILEIO (z. B. `/dev/sdb` und `/dev/sdc`) sowie bereits formatierte Datenträger (z. B. `/dev/sdb1` oder `/dev/<SHARED1`) aufgelistet sein.

13 Wiederholen Sie auf jedem Knoten die Schritte 1 bis 12.

Konfigurieren des HA-Clusters

So konfigurieren Sie den HA-Cluster:

1 Starten Sie YaST2 und navigieren Sie zu **Hochverfügbarkeit** > **Cluster**.

2 Wenn Sie dazu aufgefordert werden, installieren Sie das HA-Paket und lösen Sie die Abhängigkeiten auf.

Nach der Installation des HA-Pakets wird „Cluster – Kommunikationskanäle“ angezeigt.

3 Stellen Sie sicher, dass die Übertragungsoption `Unicast` ausgewählt ist.

4 Wählen Sie die Option **Mitgliedsadresse hinzufügen** aus und geben Sie die IP-Adresse des Knotens an. Wiederholen Sie dies, um alle anderen Clusterknoten-IP-Adressen hinzuzufügen.

5 Vergewissern Sie sich, dass die Option **Auto Generate Node ID** (Knoten-ID automatisch generieren) ausgewählt ist.

6 Vergewissern Sie sich, dass auf allen Knoten der HAWK-Service aktiviert ist. Ist er das nicht, aktivieren Sie ihn mit dem folgendem Befehl:

```
service hawk start
```

7 Führen Sie den folgenden Befehl aus:

```
ls -l /dev/disk/by-id/
```

Die SBD-Partitions-ID wird angezeigt. Zum Beispiel `scsi-1LIO-ORG_FILEIO:33caaa5a-a0bc-4d90-b21b-2ef33030cc53`.

Kopieren Sie die ID.

8 Öffnen Sie die SBD-Datei (`/etc/sysconfig/sbd`) und ersetzen Sie die ID von `SBD_DEVICE` durch die ID, die Sie in Schritt 7 kopiert haben.

9 Führen Sie den folgenden Befehl aus, um den Pacemaker-Service neu zu starten:

```
rcpacemaker restart
```

10 Führen Sie den folgenden Befehl aus, um die Autostart-Skripte zu entfernen, damit der Cluster das Produkt verwalten kann.

```
cd /
insserv -r sentinel
```

11 Wiederholen Sie auf jedem Clusterknoten die Schritte 1 bis 10.

12 Führen Sie den folgenden Befehl aus, um alle Änderungen der Konfigurationsdateien zu synchronisieren:

```
csync2 -x -v
```

13 Deaktivieren Sie den Wartungsmodus im Cluster mit dem folgenden Befehl:

```
crm configure property maintenance-mode=false
```

Sie können den Befehl von einem beliebigen Clusterknoten aus ausführen.

14 Überprüfen Sie mit dem folgenden Befehl, ob der Wartungsmodus inaktiv ist:

```
crm status
```

Die Clusterressourcen sollten im Zustand „gestartet“ angezeigt werden.

Aufrüsten einer Hochverfügbarkeitsinstallation von Sentinel Appliance

Sie können eine Hochverfügbarkeitsinstallation von Sentinel Appliance mit dem zypper-Patch aufrüsten.

WICHTIG: Die Prozeduren in diesem Abschnitt verwenden die Befehle `rcopenais` und `openais`, die nur mit SLES 11 SP4 funktionieren. Verwenden Sie für SLES 12 SP2 und höher den Befehl `systemctl pacemaker.service`.

Verwenden Sie beispielsweise für den Befehl `/etc/rc.d/openais start` den Befehl `systemctl start pacemaker.service`.

- „Aufrüsten einer Hochverfügbarkeitsinstallation von Sentinel Appliance mit zypper“, auf Seite 221

Aufrüsten einer Hochverfügbarkeitsinstallation von Sentinel Appliance mit zypper

Vor dem Aufrüsten müssen Sie alle Appliance-Knoten über Sentinel Appliance Manager registrieren. Weitere Informationen finden Sie unter „Registrieren für Aktualisierungen“, auf Seite 104. Wenn Sie die Appliance nicht registrieren, gibt Sentinel eine Warnmeldung aus.

1. Aktivieren Sie den Wartungsmodus im Cluster.

   ```
   crm configure property maintenance-mode=true
   ```

   Der Wartungsmodus trägt dazu bei, Störungen der ausgeführten Clusterressourcen während der Aktualisierung der Sentinel-Software zu vermeiden. Sie können den Befehl von einem beliebigen Clusterknoten aus ausführen.

2. Überprüfen Sie, ob der Wartungsmodus aktiv ist.

   ```
   crm status
   ```

   Die Clusterressourcen sollten im Zustand „nicht verwaltet“ angezeigt werden.

3. Rüsten Sie den passiven Clusterknoten auf:

   3a Stoppen Sie den Clusterstapel.

   ```
   rcopenais stop
   ```

   Durch Stoppen des Clusterstapels wird sichergestellt, dass auf die Ressourcen weiterhin zugegriffen werden kann und das Fencing der Knoten wird verhindert.

   3b Laden Sie die Aufrüstungen für die Hochverfügbarkeitsinstallation von Sentinel Appliance herunter.

   ```
   zypper -v patch
   ```

   3c (Bedingt) Wenn das Installationsprogramm meldet, dass Sie eine Abhängigkeit des OpenSSH-Pakets auflösen müssen, geben Sie die entsprechende Option ein, um das OpenSSH-Paket herabzustufen.

   3d (Bedingt) Wenn das Installationsprogramm eine Änderung an der ncgOverlay-Architektur meldet, geben Sie die entsprechende Option ein, um die Architekturänderung zu akzeptieren.

   3e (Bedingt) Wenn das Installationsprogramm meldet, dass Sie Abhängigkeiten einiger Appliance-Pakete auflösen müssen, geben Sie die entsprechende Option ein, um die abhängigen Pakete zu deinstallieren.

3f Starten Sie nach dem Abschluss der Aufrüstung den Clusterstapel.

```
rcopenais start
```

4 Wiederholen Sie Schritt 3 für alle passiven Clusterknoten.

5 Rüsten Sie den aktiven Clusterknoten auf:

5a Sichern Sie die Konfiguration, und erstellen Sie einen ESM-Export.

Weitere Informationen zum Sichern von Daten finden Sie im Abschnitt „Backing Up and Restoring Data“ (Sichern und Wiederherstellen von Daten) im *Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

5b Stoppen Sie den Clusterstapel.

```
rcopenais stop
```

Durch Stoppen des Clusterstapels wird sichergestellt, dass auf die Ressourcen weiterhin zugegriffen werden kann und das Fencing der Knoten wird verhindert.

5c Laden Sie die Aufrüstungen für die Hochverfügbarkeitsversion von Sentinel Appliance herunter.

```
zypper -v patch
```

5d (Bedingt) Wenn das Installationsprogramm meldet, dass Sie eine Abhängigkeit des OpenSSH-Pakets auflösen müssen, geben Sie die entsprechende Option ein, um das OpenSSH-Paket herabzustufen.

5e (Bedingt) Wenn das Installationsprogramm eine Änderung an der ncgOverlay-Architektur meldet, geben Sie die entsprechende Option ein, um die Architekturänderung zu akzeptieren.

5f (Bedingt) Wenn das Installationsprogramm meldet, dass Sie Abhängigkeiten einiger Appliance-Pakete auflösen müssen, geben Sie die entsprechende Option ein, um die abhängigen Pakete zu deinstallieren.

5g Starten Sie nach dem Abschluss der Aufrüstung den Clusterstapel.

```
rcopenais start
```

5h Führen Sie den folgenden Befehl aus, um alle Änderungen der Konfigurationsdateien zu synchronisieren:

```
csync2 -x -v
```

6 Deaktivieren Sie den Wartungsmodus im Cluster.

```
crm configure property maintenance-mode=false
```

Sie können den Befehl von einem beliebigen Clusterknoten aus ausführen.

7 Überprüfen Sie, ob der Wartungsmodus inaktiv ist.

```
crm status
```

Die Clusterressourcen sollten im Zustand „gestartet“ angezeigt werden.

8 (Optional:) Überprüfen Sie, ob die Sentinel-Aufrüstung erfolgreich war:

```
rcsentinel version
```

9 (Bedingt) Zum Aufrüsten des Betriebssystems siehe „Aufrüsten des Betriebssystems“, auf Seite 162.

40 Datensicherung und -wiederherstellung

Der hochverfügbare Failover-Cluster, der in diesem Dokument beschrieben wird, bietet eine Redundanzstufe. Wenn bei dem Dienst in einem Knoten im Cluster Fehler auftreten, wird somit automatisch ein Failover in einen anderen Knoten im Cluster durchgeführt und der Dienst wird dort wiederhergestellt. Wenn ein Ereignis wie dieses auftritt, ist es wichtig, den fehlerhaften Knoten wieder in einen betriebsbereiten Zustand zu versetzen, damit die Redundanz im System wiederhergestellt werden und im Fall eines weiteren Fehlers als Schutz fungieren kann. In diesem Abschnitt wird die Wiederherstellung des fehlerhaften Knotens unter einer Reihe von Fehlerbedingungen beschrieben.

Sicherung

Obwohl ein hochverfügbarer Failover-Cluster wie der in diesem Dokument beschriebene eine Redundanzschicht bietet, ist es doch wichtig, regelmäßig eine herkömmliche Sicherung der Konfiguration und Daten zu erstellen, die bei Verlust oder Beschädigung nicht leicht wiederherstellbar wären. Im Abschnitt „Sichern und Wiederherstellen von Daten“ im *Sentinel -Verwaltungshandbuch* wird beschrieben, wie die in Sentinel integrierten Werkzeuge zur Erstellung einer Sicherung verwendet werden. Diese Werkzeuge sollten im aktiven Knoten im Cluster verwendet werden, weil der Passivknoten im Cluster nicht über den erforderlichen Zugriff auf das freigegebene Speichergerät verfügt. Andere handelsübliche Sicherungswerkzeuge könnten stattdessen ebenfalls verwendet werden, könnten jedoch andere Anforderungen haben bezüglich der Knoten, in denen sie verwendet werden können.

Recovery

Vorübergehender Fehler

Wenn der Fehler ein temporärer Fehler war und die Anwendung, die Betriebssystemsoftware und die Konfiguration nicht beschädigt wurden, wird der betriebsbereite Zustand eines Knoten einfach durch Löschen des temporären Fehlers (zum Beispiel durch Neubooten des Knotens) wiederhergestellt. Die Benutzeroberfläche für die Clusterverwaltung kann für ein Failback des ausgeführten Diensts zurück zum ursprünglichen Clusterknoten verwendet werden, falls gewünscht.

Beschädigung des Knotens

Wenn der Fehler eine Beschädigung der Anwendung, der Betriebssystemsoftware oder der Konfiguration im Speichersystem des Knotens verursacht hat, muss die beschädigte Software neu installiert werden. Wiederholen Sie die Schritte zum Hinzufügen eines Knotens zum Cluster, die weiter oben in diesem Dokument beschrieben wurden, um den Knoten in einem betriebsbereiten

Zustand wiederherzustellen. Die Benutzeroberfläche für die Clusterverwaltung kann für ein Failback des ausgeführten Diensts zurück zum ursprünglichen Clusterknoten verwendet werden, falls gewünscht.

Konfiguration der Clusterdaten

Wenn auf dem freigebenen Speichergerät eine Datenbeschädigung auftritt, die verhindert, dass das freigegebene Speichergerät wiederhergestellt wird, führt dies dazu, dass die Beschädigung den gesamten Cluster betrifft. Er kann dann nicht automatisch über den in diesem Dokument beschriebenen hochverfügbaren Failover-Cluster wiederhergestellt werden. Im Abschnitt „Sichern und Wiederherstellen von Daten“ im *Sentinel -Verwaltungshandbuch* wird beschrieben, wie die in Sentinel integrierten Werkzeuge zum Wiederherstellen von einer Sicherung verwendet werden. Diese Werkzeuge sollten im aktiven Knoten im Cluster verwendet werden, weil der Passivknoten im Cluster nicht über den erforderlichen Zugriff auf das freigegebene Speichergerät verfügt. Andere handelsüblichen Werkzeuge für die Sicherung und Wiederherstellung könnten stattdessen ebenfalls verwendet werden, könnten jedoch andere Anforderungen haben bezüglich der Knoten, in denen sie verwendet werden können.

VIII Anhänge

A Fehlersuche

Dieser Abschnitt behandelt einige Probleme, die bei der Installation auftreten können, sowie die entsprechenden Abhilfemaßnahmen.

Installationsfehler aufgrund einer falschen Netzwerkkonfiguration

Beim ersten Booten stellt das Installationsprogramm fest, dass die Netzwerkeinstellungen falsch sind. Es wird eine Fehlermeldung angezeigt. Wenn das Netzwerk nicht verfügbar ist, tritt beim Installieren von Sentinel auf der Appliance ein Fehler auf.

Zur Behebung dieses Problems müssen die Netzwerkeinstellungen ordnungsgemäß konfiguriert werden. Geben Sie zum Überprüfen der Konfiguration den Befehl `ipconfig` ein, um die gültige IP-Adresse zurückzugeben, und den Befehl `hostname -f`, um den gültigen Hostnamen zurückzugeben.

Die UUID wird für Images von Collector Manager- oder Correlation Engine-Instanzen nicht erstellt

Wenn Sie Images von einem Collector Manager-Server erstellen (z. B. mit ZENworks Imaging) und diese Images auf anderen Computern wiederherstellen, führt Sentinel keine eindeutige Identifizierung dieser neuen Collector Manager-Instanzen durch. Die Ursache hierfür sind doppelte UUIDs.

Sie müssen eine neue 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 `/var/opt/novell/sentinel/data`.
2. Starten Sie den Collector Manager neu.

   Der Collector Manager generiert automatisch die UUID.

In Internet Explorer ist die Benutzeroberfläche von Sentinel Main nach der Anmeldung leer

Wenn die Sicherheitsstufe in Internet Explorer auf „Hoch“ eingestellt ist, wird nach dem Anmelden bei Sentinel eine leere Seite angezeigt. Das Popupfenster für das Herunterladen von Dateien wird möglicherweise vom Browser gesperrt. Um dieses Problem zu umgehen, legen Sie zunächst die Sicherheitsstufe auf „Mittelhoch“ fest und ändern Sie sie dann folgendermaßen in „Benutzerdefiniert“ um:

1. Wechseln Sie zu **Extras > Internetoptionen > Sicherheit**, und legen Sie die Sicherheitsstufe auf **Mittelhoch** fest.
2. Stellen Sie sicher, dass die Option **Extras > Einstellungen der Kompatibilitätsansicht** nicht ausgewählt ist.
3. Navigieren Sie zu **Extras > Internetoptionen > Sicherheit (Registerkarte) > Stufe anpassen**, führen Sie einen Bildlauf nach unten bis zum Bereich **Download** durch und wählen Sie unter **Automatische Eingabeaufforderung für Dateidownloads** die Option **Aktivieren** aus.

Sentinel wird auf Windows Server 2012 R2 in Internet Explorer 11 nicht gestartet

Wenn Sie Windows Server 2012 R2 verwenden, wird Sentinel in Internet Explorer 11 aufgrund der standardmäßigen Sicherheitskonfigurationen von Internet Explorer 11 nicht gestartet. Fügen Sie Sentinel manuell zur Liste der vertrauenswürdigen Sites hinzu, bevor Sie Sentinel starten.

Sentinel zur Liste der vertrauenswürdigen Sites hinzufügen

1. Öffnen Sie Internet Explorer 11.
2. Klicken Sie auf das Symbol **Einstellungen** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Sites** > **Sites**.
3. Fügen Sie den Sentinel-Host zur Liste der vertrauenswürdigen Sites hinzu.

Sentinel kann lokale Berichte nicht mit standardmäßiger EPS-Lizenz ausführen

Wenn Ihre Umgebung mit der standardmäßigen 25-EPS-Lizenz verwendet wird und Sie einen Bericht ausführen, tritt beim Ausführen des Berichts der folgende Fehler auf: `License for Distributed Search feature is expired` (Lizenz für Funktion der verteilten Suche ist abgelaufen).

Führen Sie die folgenden Schritte aus, um Berichte in der gleichen JVM wie Sentinel auszuführen:

1. Melden Sie sich am Sentinel-Server an und öffnen Sie die Datei `/etc/opt/novell/sentinel/config/obj-component.JasperReportingComponent.properties`.
2. Suchen Sie die Eigenschaft `reporting.process.oktorunstandalone`.
3. (Bedingt) Wenn die Eigenschaft nicht in der Datei vorhanden ist, fügen Sie sie hinzu.
4. Legen Sie den Wert der Eigenschaft auf `false` fest. Beispiel:

   ```
   reporting.process.oktorunstandalone=false
   ```
5. Starten Sie Sentinel neu.

Synchronisierung muss in Sentinel High Availability manuell gestartet werden, nachdem der aktive Knoten in den FIPS 140-2-Modus konvertiert wurde

Problem: Wenn Sie in Sentinal HA den aktiven Knoten in den FIPS 140-2-Modus konvertieren, wird die Synchronisierung zur Konvertierung aller passiven Knoten in den FIPS 140-2-Modus nicht richtig ausgeführt. Sie müssen die Synchronisierung manuell starten.

Behelfslösung: Synchronisieren Sie alle passiven Knoten auf folgende Weise manuell auf FIPS 140-2:

1. Melden Sie sich mit dem Benutzer „root“ am aktiven Knoten an.
2. Öffnen Sie die Datei `/etc/csync2/csync2.cfg`.
3. Ändern Sie die folgende Zeile:

   ```
   include /etc/opt/novell/sentinel/3rdparty/nss/*;
   ```

   in

   ```
   include /etc/opt/novell/sentinel/3rdparty/nss;
   ```
4. Speichern Sie die Datei `csync2.cfg`.
5. Starten Sie die Synchronisierung manuell, indem Sie folgenden Befehl ausführen:

   ```
   csync2 -x -v
   ```

Benutzeroberfläche von Sentinel Main zeigt nach der Konvertierung zum skalierbaren Datenmanager eine leere Seite an

Problem: Nach der Aktivierung des skalierbaren Datenmanagers von Sentinel zeigt der Browser nach der Anmeldung bei der Benutzeroberfläche von Sentinel Main eine leere Seite an.

Behelfslösung: Schließen Sie den Browser und melden Sie sich erneut bei der Benutzeroberfläche von Sentinel Main an. Das Problem tritt nur einmal bei der ersten Anmeldung bei der Benutzeroberfläche von Sentinel Main nach der Aktivierung des skalierbaren Datenmanagers auf.

Beim Bearbeiten einiger gespeicherter Suchen fehlt der Bereich „Ereignisfelder“ auf der Zeitplanseite

Problem: Wenn Sie eine gespeicherte Suche bearbeiten, die von Sentinel 7.2 auf eine spätere Version aufgerüstet wurde, fehlt auf der Zeitplanseite der Bereich **Ereignisfelder**, in dem die Ausgabefelder für die CSV-Datei mit den Suchergebnissen festgelegt werden.

Behelfslösung: Erstellen und planen Sie die Suche nach der Aufrüstung von Sentinel neu, damit der Bereich **Ereignisfelder** auf der Zeitplanseite angezeigt wird.

Sentinel gibt keine korrelierten Ereignisse zurück, wenn Sie Ereignisse für die bereitgestellte Regel mit der standardmäßigen Suche über die ausgelöste Anzahl suchen

Problem: Sentinel gibt keine korrelierten Ereignisse zurück, wenn Sie zum Suchen aller korrelierten Ereignisse, die nach dem Bereitstellen oder Aktivieren der Regel generiert wurden, auf der Korrelationsübersichtsseite der Regel im Bereich **Aktivitätsstatistik** auf das Symbol **Ausgelöste Anzahl** klicken.

Behelfslösung: Ändern Sie den Wert im Feld **Von** auf der Seite der Ereignissuche in einen Wert, der einen Zeitpunkt vor der im Feld aufgefüllten Zeit darstellt, und klicken Sie erneut auf **Suchen**.

Sicherheitsintelligenz-Dashboard zeigt beim erneuten Generieren einer Grundkonfiguration eine ungültige Grundkonfigurationsdauer an

Problem: Während der erneuten Generierung der Sicherheitsintelligenz-Grundkonfiguration werden das Start- und Enddatum falsch als „1.1.1970“ angezeigt.

Behelfslösung: Wenn die Neugenerierung der Grundkonfiguration abgeschlossen ist, werden die richtigen Daten angezeigt.

Sentinel-Server wird heruntergefahren, wenn eine Suche ausgeführt wird und eine einzelne Partition eine große Anzahl Ereignisse enthält

Problem: Der Sentinel-Server wird heruntergefahren, wenn eine Suche ausgeführt wird und eine einzelne Partition eine große Anzahl Ereignisse enthält.

Behelfslösung: Erstellen Sie Beibehaltungsrichtlinien so, dass an einem Tag mindestens zwei Partitionen geöffnet sind. Wenn mehrere Partitionen geöffnet sind, wird die Anzahl der in den Partitionen indexierten Ereignisse reduziert.

Sie können Beibehaltungsrichtlinien erstellen, die Ereignisse auf Grundlage des Felds `estzhour` filtern. Dieses Feld dient der Nachverfolgung der Stunde des Tages. Sie können also eine Beibehaltungsrichtlinie mit dem Filter `estzhour:[0 TO 11]` und eine weitere Beibehaltungsrichtlinie mit dem Filter `estzhour:[12 TO 23]` erstellen.

Weitere Informationen finden Sie im Abschnitt „Configuring Data Retention Policies“ (Datenbeibehaltungsrichtlinien konfigurieren) im *Sentinel Administration Guide* (Sentinel-Administrationshandbuch).

Fehler beim Verwenden des Skripts „report_dev_setup.sh“ zum Konfigurieren von Sentinel-Ports für Firewall-Ausnahmen in aufgerüsteten Sentinel Appliance-Installationen

Problem: Sentinel zeigt einen Fehler an, wenn Sie Sentinel-Ports für Firewall-Ausnahmen mit dem Skript `report_dev_setup.sh` konfigurieren.

Behelfslösung: Führen Sie die folgenden Schritte aus, um Sentinel-Ports für Firewall-Ausnahmen zu konfigurieren:

1. Öffnen Sie die Datei `/etc/sysconfig/SuSEfirewall2`.
2. Ändern Sie die folgende Zeile:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   in

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Starten Sie Sentinel neu.

B Deinstallation

In diesem Anhang finden Sie Informationen über die Deinstallation von Sentinel und die Aufgaben nach der Deinstallation.

Checkliste für die Deinstallation

Verwenden Sie die folgende Checkliste, um Sentinel zu deinstallieren:

- ❒ Deinstallieren Sie den Sentinel-Server.
- ❒ Deinstallieren Sie den Collector Manager und die Correlation Engine, falls vorhanden.
- ❒ Führen Sie die Aufgaben nach der Deinstallation durch, um die Deinstallation von Sentinel abzuschließen.

Deinstallieren von Sentinel

Zum Entfernen einer Sentinel-Installation steht Ihnen ein Deinstallationsskript zur Verfügung. Vor dem Durchführen einer neuen Installation sollten Sie alle folgenden Schritte durchführen, um sicherzustellen, dass keine Dateien oder Systemeinstellungen einer vorherigen Installation übrig bleiben.

WARNUNG: Diese Anweisungen beinhalten Änderungen an Betriebssystemeinstellungen und Dateien. Wenn Sie keine Erfahrung im Ändern dieser Systemeinstellungen bzw. Dateien haben, wenden Sie sich an den Systemadministrator.

Deinstallieren des Sentinel-Servers

Gehen Sie folgendermaßen vor, um den Sentinel-Server zu deinstallieren:

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

   HINWEIS: Sie können den Sentinel-Server nicht als Nicht-root-Benutzer deinstallieren, wenn die Installation mit dem Benutzer `root` ausgeführt wurde. Der Sentinel-Server kann jedoch mit einem Nicht-root-Benutzer deinstalliert werden, wenn auch die Installation mit einem Nicht-root-Benutzer ausgeführt wurde.

   ---

2. Greifen Sie auf das folgende Verzeichnis zu:

   ```
   <sentinel_installation_path>/opt/novell/sentinel/setup/
   ```

3. Führen Sie den folgenden Befehl aus:

```
./uninstall-sentinel
```

4 Wenn Sie aufgefordert werden, zu bestätigen, dass Sie mit der Deinstallation fortfahren möchten, drücken Sie „j“.

Das Skript stoppt den Service zunächst und entfernt ihn dann vollständig.

Deinstallieren von Collector Manager und Correlation Engine

Gehen Sie folgendermaßen vor, um den Collector Manager und die Correlation Engine zu deinstallieren:

1 Melden Sie sich als `root` beim Computer der Collector Manager-Instanz und der Correlation Engine-Instanz an.

HINWEIS: Sie können die Remote-Instanz von Collector Manager nicht als Nicht-root-Benutzer deinstallieren, wenn die Installation mit dem Benutzer `root` ausgeführt wurde. Die Deinstallation kann jedoch von einem Nicht-root-Benutzer vorgenommen werden, wenn auch die Installation mit einem Nicht-root-Benutzer ausgeführt wurde.

---

2 Gehen Sie zu folgender Position:

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

3 Führen Sie den folgenden Befehl aus:

```
./uninstall-sentinel
```

Das Skript zeigt eine Warnmeldung an, die darauf hinweist, dass der Collector Manager bzw. die Correlation Engine mit allen verknüpften Daten vollständig entfernt wird.

4 Geben Sie „y“ ein, um den Collector Manager bzw. die Correlation Engine zu entfernen.

Das Skript stoppt den Service zunächst und entfernt ihn dann vollständig. Die Collector Manager- und Correlation Engine-Symbole werden jedoch weiterhin im inaktiven Status in der Benutzeroberfläche von Sentinel Main angezeigt.

5 (Bedingt) Wenn Ereignisgrafiken aktiviert sind, müssen Sie das Elasticsearch-Sicherheits-Plugin neu bereitstellen. Weitere Informationen finden Sie unter „Elasticsearch-Sicherheits-Plugin neu bereitstellen“, auf Seite 82.

6 Führen Sie folgende zusätzliche Schritte aus, um den Collector Manager und die Correlation Engine manuell aus der Benutzeroberfläche von Sentinel Main zu löschen:

Collector Manager:

1. Öffnen Sie **Ereignisquellenverwaltung > Live-Ansicht**.
2. Klicken Sie mit der rechten Maustaste auf den Collector Manager, den Sie löschen möchten, und anschließend auf **Löschen**.

Correlation Engine:

1. Melden Sie sich als Administrator bei der **Sentinel Main**-Benutzeroberfläche an.
2. Erweitern Sie den Abschnitt **Korrelation** und wählen Sie die zu löschende Correlation Engine aus.
3. Klicken Sie auf die Schaltfläche **Löschen** (Papierkorbsymbol).

Deinstallieren von NetFlow Collector Manager

Gehen Sie folgendermaßen vor, um den NetFlow Collector Manager zu deinstallieren:

1. Melden Sie sich beim Computer der NetFlow Collector Manager-Instanz an.

   HINWEIS: Sie müssen sich mit demselben Benutzerberechtigungsnachweis anmelden, mit dem der NetFlow Collector Manager installiert wurde.

2. Wechseln Sie zu folgendem Verzeichnis:

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

3. Führen Sie den folgenden Befehl aus:

   ```
   ./uninstall–sentinel
   ```

4. Zum Deinstallieren des Collector Managers geben Sie y ein.

   Das Skript stoppt den Dienst zunächst und deinstalliert ihn dann vollständig.

Nach der Deinstallation auszuführende Aufgaben

Durch das Deinstallieren des Sentinel-Servers wird der Sentinel-Administratorbenutzer nicht aus dem Betriebssystem entfernt. Sie müssen diesen Benutzer manuell entfernen.

Nach der Deinstallation von Sentinel bleiben bestimmte Systemeinstellungen vorhanden. Vor einer neuen Installation von Sentinel sollten diese Einstellungen entfernt werden, besonders wenn bei der Deinstallation von Sentinel Fehler aufgetreten sind.

So bereinigen Sie manuell die Sentinel-Systemeinstellungen:

1. Melden Sie sich als `root`-Benutzer an.
2. Stellen Sie sicher, dass alle Sentinel-Prozesse gestoppt wurden.
3. Entfernen Sie die Inhalte von `/opt/novell/sentinel` bzw. vom Verzeichnis, in dem die Sentinel-Software installiert wurde.
4. Stellen Sie sicher, dass niemand als Sentinel-Administrator-Systembenutzer (standardmäßig „novell“) angemeldet ist, und entfernen Sie dann den Benutzer, das Basisverzeichnis und die Gruppe.

   ```
   userdel -r novell
   ```

   ```
   groupdel novell
   ```

5. Starten Sie das Betriebssystem neu.