NetIQ® Sentinel™

Installations- und Konfigurationshandbuch

Februar 2015

www.netiq.com/documentation

Rechtliche Hinweise

Inhalt

Info zu diesem Handbuch und zur Bibliothek

Das *Installations- und Konfigurationshandbuch* enthält eine Einführung zu NetIQ 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.

Info zu NetIQ Corporation

NetIQ ist ein globaler Hersteller von Unternehmenssoftware. Unser Blickpunkt liegt auf drei besonderen Herausforderungen, die Sie in Ihrer Umgebung meistern müssen: Änderungen, Komplexität und Risiken. Unser Ziel ist es, Sie dabei zu unterstützen.

Unser Standpunkt

Sich an Änderungen anzupassen und Komplexität und Risiken zu beherrschen ist nichts Neues

Unter den verschiedenen Herausforderungen, denen Sie gegenüberstehen, beeinflussen diese drei Punkte sicherlich am meisten Ihre Möglichkeiten, Ihre physikalischen, virtuellen und Cloud-Umgebungen sicher zu messen, zu überwachen und zu verwalten.

Kritische Geschäftsservices schneller und besser bereitstellen

Wir sind davon überzeugt, dass IT-Organisationen über eine möglichst große Kontrolle verfügen müssen, um eine zeitgerechte und kostenwirksame Servicebereitstellung zu ermöglichen. Der von Änderungen und Komplexität ausgehende, kontinuierliche Druck steigt ständig, weil sich die Unternehmen ständig ändern und die erforderlichen Technologien zur Verwaltung der Änderungen immer komplexer werden.

Unsere Philosophie

Intelligente Lösungen entwickeln, nicht einfach Software

Um zuverlässige Lösungen für die Kontrolle anbieten zu können, stellen wir erst einmal sicher, dass wir das Szenario, in dem Unternehmen wie das Ihre täglich arbeiten, gründlich verstehen. Nur so können wir praxistaugliche, intelligente IT-Lösungen entwickeln, die nachweisbar messbare Ergebnisse liefern. Und das ist für uns wesentlich bereichernder, als einfach eine Software zu verkaufen.

Ihr Erfolg ist unsere Leidenschaft

Ihr Erfolg ist der Wegweiser für unser Geschäft. Wir wissen, dass Sie von der Produktkonzeption bis hin zur Bereitstellung IT-Lösungen benötigen, die richtig funktionieren und nahtlos mit Ihren vorhandenen Investitionen integriert werden können. Sie benötigen fortlaufenden Support, Schulungen nach der Bereitstellung und jemanden, mit dem Sie unkompliziert arbeiten können. Ihr Erfolg ist auch unser Erfolg.

Unsere Lösungen

- Identitäts- und Zugriffsregelung
- Zugriffsverwaltung
- Sicherheitsverwaltung
- System- und Anwendungsverwaltung

- Workload-Management
- Serviceverwaltung

Anfragen an die Verkaufsunterstützung

Bei Fragen zu Produkten, Preisen und Funktionen wenden Sie sich an Ihren Händler vor Ort. Wenn dies nicht möglich ist, wenden Sie sich an unser Verkaufsunterstützungsteam.

Weltweit:	www.netiq.com/about_netiq/officelocations.asp
Vereinigte Staaten und Kanada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Kontakt zum technischen Support

Bei spezifischen Produktproblemen, wenden Sie sich an unseren technischen Support.

Weltweit:	www.netiq.com/support/contactinfo.asp
Nord- und Südamerika:	1-713-418-5555
Europa, Naher Osten und Afrika:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Kontakt zum Dokumentationssupport

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Wenn Sie uns einen Verbesserungsvorschlag mitteilen möchten, nutzen Sie die Schaltfläche **Kommentar hinzufügen**, die unten auf jeder Seite der unter www.netiq.com/documentation veröffentlichten HTML-Versionen unserer Dokumentation verfügbar ist. Sie können Verbesserungsvorschläge auch per Email an Documentation-Feedback@netiq.com senden. Wir freuen uns auf Ihre Rückmeldung.

Kontakt zur Online-Benutzer-Community

Qmunity, die NetIQ-Online-Community, ist ein Netzwerk zur Zusammenarbeit mit anderen NetIQ-Benutzern und -Experten. Qmunity bietet Ihnen aktuellste Informationen, nützliche Links zu hilfreichen Ressourcen und Kontakt zu NetIQ-Experten, damit Sie über alle Voraussetzungen verfügen, um das meiste aus den IT-Investitionen zu holen, auf die Sie sich verlassen. Weitere Informationen hierzu finden Sie im Internet unter http://community.netiq.com.

Sentinel

In diesem Abschnitt finden Sie detaillierte Informationen darüber, was Sentinel ist und wie Sie mit Sentinel eine Ereignisverwaltungslösung in Ihrem Unternehmen bereitstellen können.

1 Was ist Sentinel?

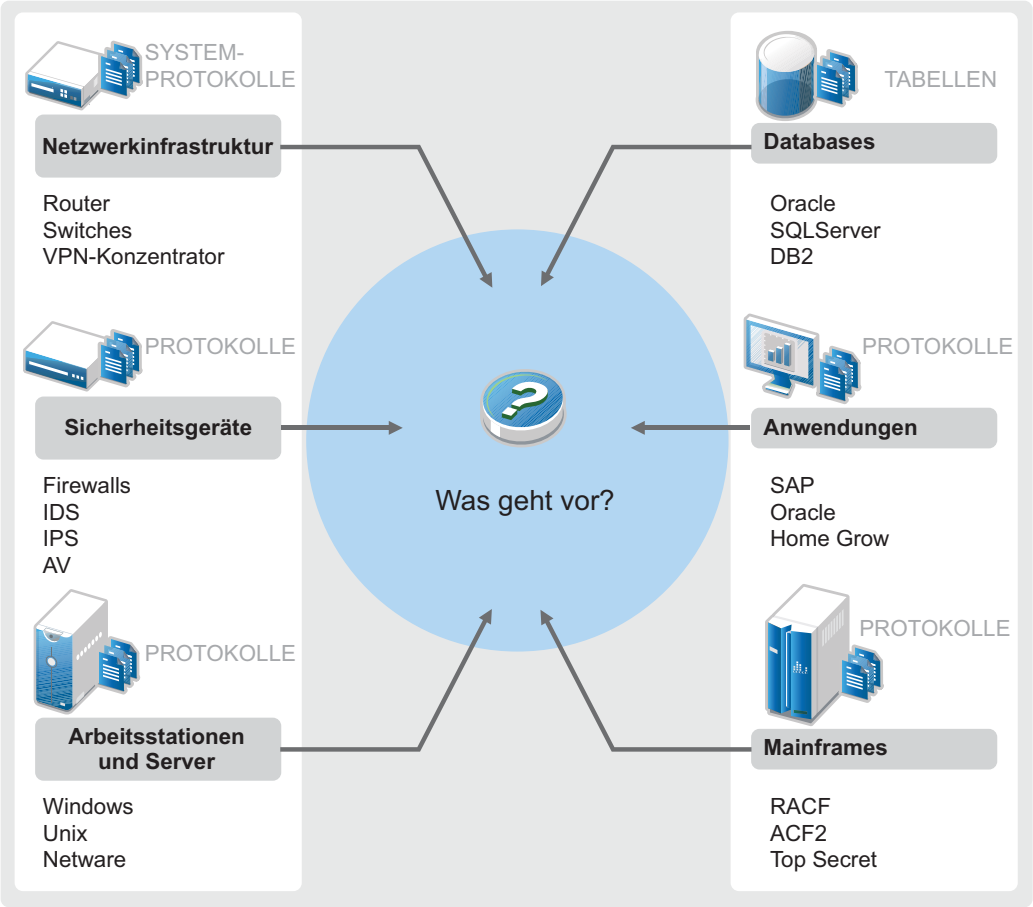
Sentinel ist eine Lösung für das Sicherheitsinformations- und Ereignismanagement (SIEM) und die Compliance-Überwachung. Sentinel überwacht die komplexesten IT-Umgebungen automatisch und stellt die für den Schutz der IT-Umgebung erforderliche Sicherheit bereit.

- Abschnitt 1.1, „Herausforderungen bei der Absicherung einer IT-Umgebung“, auf Seite 15
- Abschnitt 1.2, „Die Lösung, die Sentinel bietet“, auf Seite 16

1.1 Herausforderungen bei der Absicherung einer IT-Umgebung

Aufgrund der Komplexität Ihrer IT-Umgebung ist deren Absicherung eine Herausforderung. Zahlreiche Anwendungen, Datenbanken, Mainframes, Arbeitsstationen und Server zeichnen Protokolle der Ereignisse in Ihrer IT-Umgebung auf. Zusätzlich haben Sie Sicherheits- und Netzwerkinfrastrukturgeräte, die ebenfalls Protokoll über die Ereignisse in Ihrer IT-Umgebung führen.

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



Gründe für die Herausforderungen:

- Ihre IT-Umgebung besteht aus sehr vielen Geräten.
- Die Protokolle haben verschiedene Formate.
- Die Protokolle werden in Silos gespeichert.
- In den Protokollen wird eine große Menge an Informationen generiert.
- Ohne manuelle Analyse der Protokolle können Sie nicht feststellen, wer was getan hat.

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

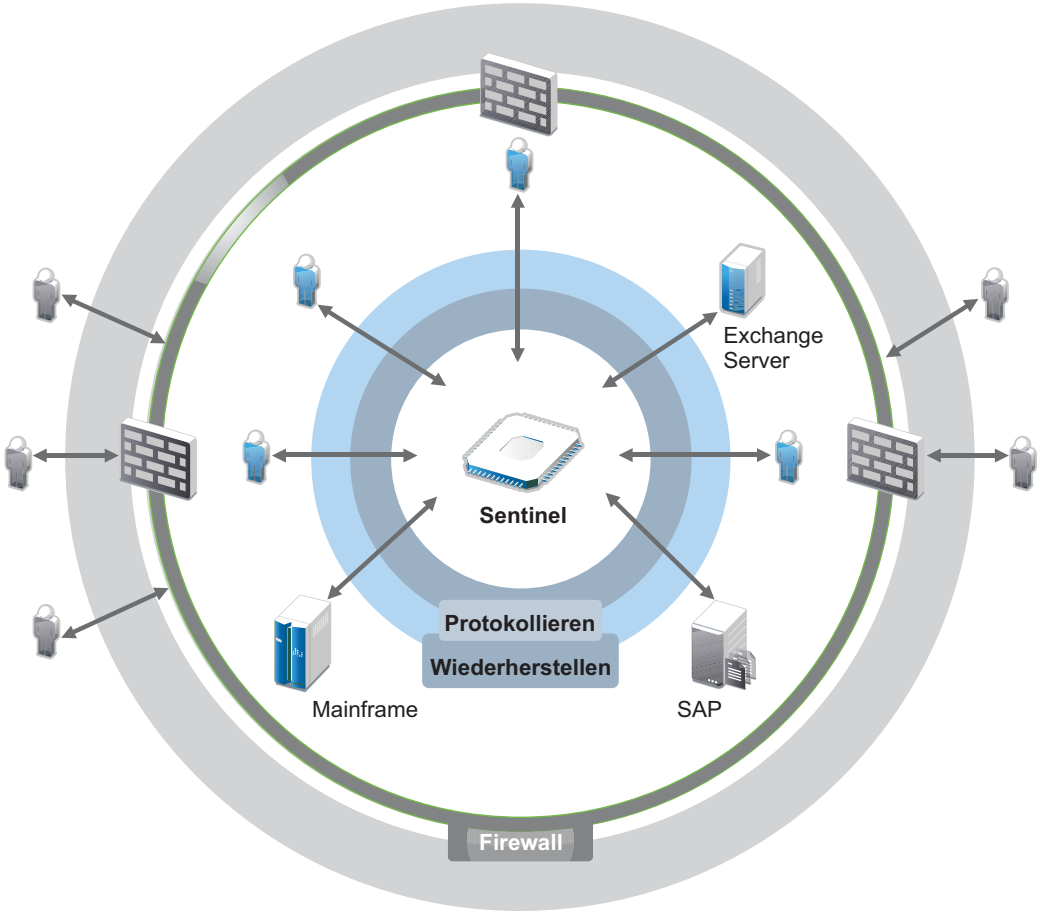
- Daten erfassen.
- Daten konsolidieren.
- Unterschiedliche Daten in Ereignissen normalisieren, die leicht verglichen werden können.
- Ereignisse Standardvorschriften zuordnen.
- Daten analysieren.
- Ereignisse aus mehreren Systemen vergleichen, um festzustellen, ob ein bestimmtes Muster auf ein Sicherheitsproblem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

Sie kennen nun die Herausforderungen, vor die Sie die Absicherung Ihrer IT-Umgebung stellt. Nun müssen Sie herausfinden, wie Sie Ihr Unternehmen für die Benutzer und vor den Benutzern schützen, ohne diese wie böswillige Benutzer zu behandeln oder sie bis zu einem Punkt zu belasten, an dem Produktivität unmöglich wird. Sentinel stellt die Lösung bereit.

1.2 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*



Sie wissen daher 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 lernen Sie das Verhalten der Benutzer kennen und können erforderliche Kontrollen einführen. Unabhängig davon, ob die Personen Mitarbeiter des Unternehmens oder Außenstehende sind, können Sie deren Aktionen zusammenführen, sodass nicht autorisierte Aktivitäten ersichtlich werden, bevor sie Schaden anrichten.

Dies ermöglicht Sentinel kostengünstig auf folgende Weise:

- Bereitstellen einer umfassenden Lösung für IT-Kontrollen zu mehreren Vorschriften gleichzeitig.
- Keine Diskrepanzen zwischen dem, was eigentlich passieren sollte, und dem, was tatsächlich in Ihrer vernetzten Umgebung passiert.
- Bereitstellen von Nachweisen für Auditoren und Prüfer, die belegen, dass Ihr Unternehmen Sicherheitskontrollen dokumentiert und überwacht sowie entsprechende Berichte erstellt.
- Bereitstellen eines einsatzbereiten Programms für die Compliance-Überwachung und Berichterstellung.
- Bereitstellen der Transparenz und Kontrolle, die Sie benötigen, um fortlaufend die Ergebnisse von Compliance- und Sicherheitsinitiativen Ihres Unternehmen zu bewerten.

Sentinel automatisiert die Erfassung und Analyse von Protokolldaten sowie die anschließende Berichterstellung und gewährleistet so, dass die Bedrohungserkennung und die Audit-Anforderungen durch die implementierten IT-Kontrollen effektiv unterstützt werden. Sentinel bietet eine automatische Überwachung von Sicherheitsereignissen und Compliance-Ereignissen sowie IT-Steuerelemente, damit Sie im Fall einer Sicherheitsverletzung oder eines regelwidrigen Ereignisses sofort Maßnahmen ergreifen können. Mit Sentinel können Sie außerdem auf einfache Weise zusammenfassende Informationen über die Umgebung sammeln, damit sie wichtigen Stakeholdern den allgemeinen Sicherheitsstand bekanntmachen können.

2 Funktionsweise von Sentinel

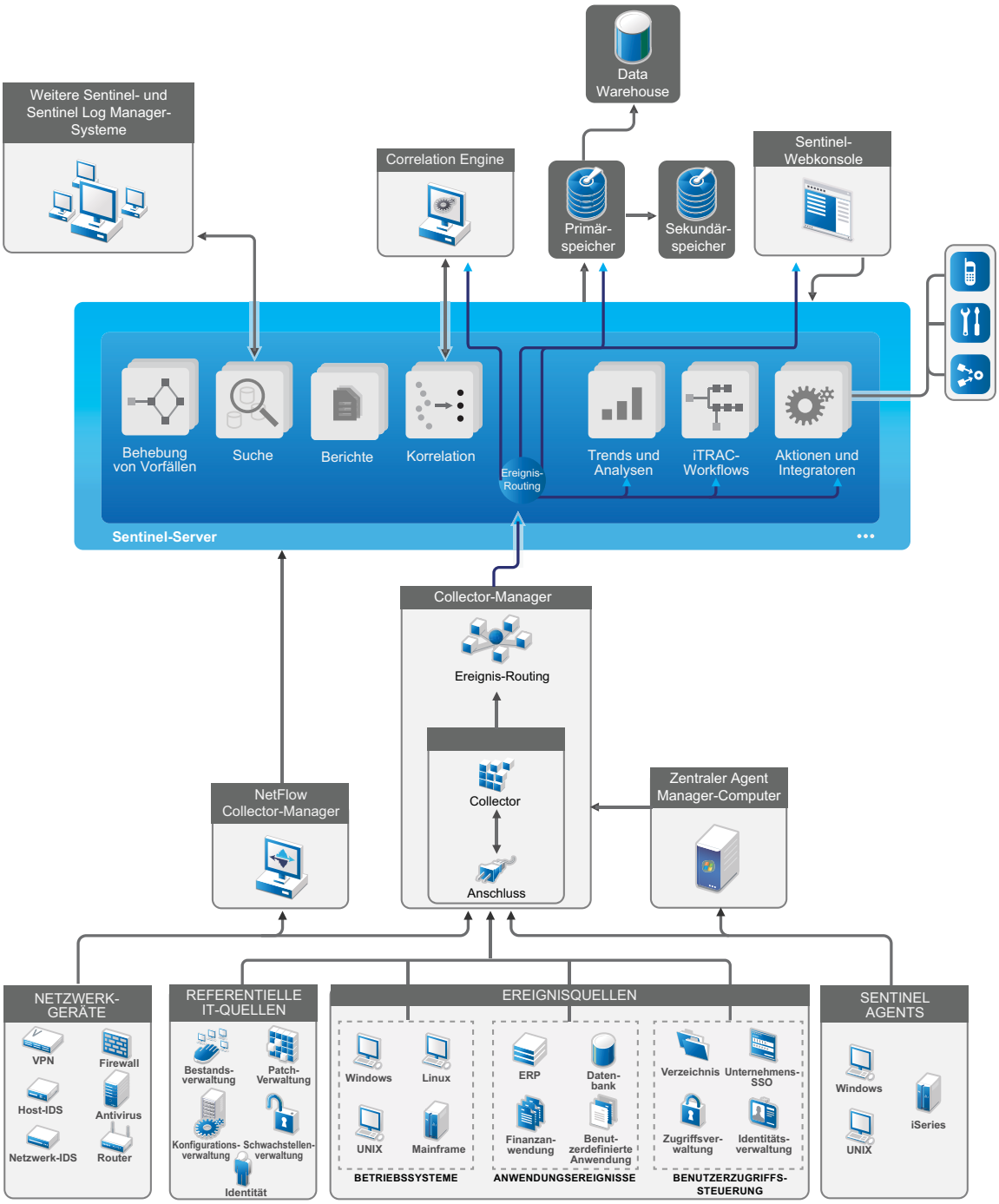
Sentinel verwaltet kontinuierlich sicherheitsrelevante Informationen und Ereignisse in Ihrer IT-Umgebung und bietet so eine vollständige Überwachungslösung.

Sentinel führt folgende Aufgaben aus:

- Erfassen von Protokoll-, Ereignis- und Sicherheitsinformationen aus allen Ereignisquellen Ihrer IT-Umgebung
- Konvertieren der erfassten Protokoll-, Ereignis- und Sicherheitsinformationen in ein Standardformat
- Speichern der Ereignisse in einem dateibasierten Datenspeicher mit flexiblen, benutzerdefinierbaren Datenbeibehaltungsrichtlinien
- Erfassen von Netzwerkablaufdaten und Hilfe bei der eingehenden Überwachung der Netzwerkaktivitäten.
- Fähigkeit zur hierarchischen Verknüpfung mehrerer Sentinel-Systeme, einschließlich Sentinel Log Manager
- Suche nach Ereignissen nicht nur auf dem lokalen, sondern auch auf weltweit verteilten Sentinel-Servern
- Durchführen statistischer Analysen zur Definition einer Baseline und Vergleich mit den aktuell einlaufenden Informationen, um verdeckte Probleme zu erkennen
- Korrelieren 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 wird dargestellt, wie Sentinel funktioniert:

Abbildung 2-1 *Sentinel-Architektur*



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

- Abschnitt 2.1, „Ereignisquellen“, auf Seite 21
- Abschnitt 2.2, „Sentinel-Ereignis“, auf Seite 21
- Abschnitt 2.3, „Collector-Manager“, auf Seite 23
- Abschnitt 2.4, „Agent Manager“, auf Seite 24

2.1 Ereignisquellen

Sentinel erfasst Sicherheitsinformationen und Ereignisse aus zahlreichen unterschiedlichen Quellen Ihrer IT-Umgebung. Diese Quellen werden als Ereignisquellen bezeichnet. Bei diesen Ereignisquellen kann es sich um zahlreiche verschiedene Komponenten in Ihrem Netzwerk handeln.

Sicherheitsbereich: Sicherheitsgeräte einschließlich Hardware und Software für die Erstellung eines Sicherheitsperimeters für Ihre Umgebung wie Firewalls, IDS und VPNs.

Betriebssysteme: Ereignisse aus den verschiedenen Betriebssystemen, die im Netzwerk ausgeführt werden.

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

Anwendungsereignisse: Ereignisse, die von den im Netzwerk installierten Anwendungen generiert werden.

Benutzerzugriffssteuerung: Ereignisse, die von Anwendungen oder Geräten generiert werden, über die Benutzer Zugriff auf Unternehmensressourcen erhalten.

Weitere Informationen zum Erfassen von Ereignissen aus Ereignisquellen finden Sie unter „Configuring Agentless Data Collection“ (Konfigurieren der agentlosen Datenerfassung).

2.2 Sentinel-Ereignis

Sentinel empfängt Informationen von Geräten, standardisiert diese Informationen in einer als Ereignis bezeichneten Struktur, klassifiziert das Ereignis und sendet es zur Verarbeitung. Durch Hinzufügen von Kategorieinformationen (Taxonomie) zu den Ereignissen können die Ereignisse leichter über verschiedene Systeme hinweg verglichen werden, die Ereignisse auf unterschiedliche Weise berichten. Ein Beispiel hierfür sind Authentifizierungsfehler. Ereignisse werden in der Echtzeitanzeige, von der Correlation Engine, von Dashboards sowie vom Back-End-Server verarbeitet.

Ein Ereignis umfasst über 200 Felder. Ereignisfelder weisen unterschiedliche Typen auf und dienen unterschiedlichen Zwecken. Es gibt einige vordefinierte Felder, beispielsweise zur Angabe des Schweregrads (severity), der Gefährlichkeit (criticality), der Ziel-IP (destination IP) und des Ziel-Ports

(destination port). Konfigurierbare Felder teilen sich in zwei Gruppen ein: Reservierte Felder sind für die interne Verwendung durch Sentinel vorgesehen (für künftige Erweiterungen), Kundenfelder sind für vom Kunden entwickelte Erweiterungen bestimmt.

Felder können durch Umbenennung einen neuen Zweck erfüllen. Die Quelle eines Felds kann entweder extern (die Festlegung erfolgt also explizit durch das Gerät oder den entsprechenden Collector) oder referenziell sein. Der Wert eines referenziellen Felds wird unter Verwendung des Zuordnungsservice als Funktion eines oder mehrerer weiterer Felder berechnet. Ein Feld kann beispielsweise der Gebäudecode des Gebäudes sein, in dem sich das Inventar befindet (die Angabe erfolgt als Ziel-IP eines Ereignisses). Ein Feld kann beispielsweise vom Zuordnungsservice als kundendefinierte Zuordnung berechnet werden (unter Verwendung der Ziel-IP aus dem Ereignis).

- Abschnitt 2.2.1, „Zuordnungsservice“, auf Seite 22
- Abschnitt 2.2.2, „Streaming von Zuordnungen“, auf Seite 22
- Abschnitt 2.2.3, „Exploit-Erkennung (Zuordnungsservice)“, auf Seite 23

2.2.1 Zuordnungsservice

Der Zuordnungsservice stellt einen fortschrittlichen Mechanismus zur Weiterleitung relevanter Geschäftsdaten im gesamten System bereit. Diese Daten können Ereignisse um referenzielle Informationen erweitern, die Kontextinformationen zur Verfügung stellen, die Analysten bei der Entscheidungsbildung und beim Erstellen nützlicher Berichte und gut durchdachter Korrelationsregeln unterstützen.

Sie können die Ereignisdaten bereichern, indem Sie über Zuordnungen zusätzliche Informationen wie Host und Identitätsdetails zu den von den Ursprungsgeräten eingehenden Ereignissen hinzufügen. Diese zusätzlichen Informationen können für erweiterte Korrelationen und zur Berichterstellung genutzt werden. Das System unterstützt neben mehreren integrierten Zuordnungen auch benutzerdefinierte Zuordnungen.

In Sentinel definierte Zuordnungen werden auf zwei verschiedene Weisen gespeichert:

- Integrierte Zuordnungen werden in der Datenbank gespeichert, über APIs im Collector-Code aktualisiert und automatisch zum 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-Managers verteilt und lokal angewendet. Diese verteilte Verarbeitung gewährleistet, dass die Zuordnungsaktivität den Hauptserver nicht überlastet.

2.2.2 Streaming von Zuordnungen

Der Zuordnungsservice setzt ein Modell zur dynamischen Aktualisierung ein, wobei die Zuordnungen per Streaming von einem Punkt an den nächsten übertragen werden. Auf diese Weise wird verhindert, dass sich große Datenmengen an statischen Zuordnungen im dynamischen Speicher ansammeln. Der Wert dieser Streaming-Funktion erweist sich insbesondere in einem für das Unternehmen essenziellen Echtzeitsystem wie Sentinel, in dem Datenbewegungen unabhängig von einer möglichen temporären Systemauslastung zuverlässig, prädiktiv und flexibel erfolgen müssen.

2.2.3 Exploit-Erkennung (Zuordnungsservice)

In Sentinel können Querverweise zwischen den Signaturen von Ereignisdaten und den Daten von Anfälligkeitsabsuchen erstellt werden. Benutzer werden automatisch und umgehend benachrichtigt, wenn ein anfälliges System durch einen Angriff ausgenutzt zu werden droht. Hier kommt Folgendes zum Einsatz:

- Advisor-Feed
- Intrusion Detection
- Anfälligkeitsabsuchen
- Firewalls

Advisor stellt Querverweise zwischen den Signaturen von Ereignisdaten und den Daten von Anfälligkeitsabsuchen her. Advisor-Feed enthält Informationen zu Schwachstellen und Bedrohungen sowie eine Standardisierung von Ereignissignaturen und Schwachstellen-Plugins. Weitere Informationen zu Advisor finden Sie im Abschnitt „Detecting Vulnerabilities and Exploits“ (Erkennen von Schwachstellen und Exploits) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

2.3 Collector-Manager

Der Collector-Manager verwaltet die Datenerfassung, überwacht Meldungen zum Systemstatus und führt bei Bedarf eine Ereignisfilterung durch. Zu den Hauptaufgaben des Collector-Manager zählen die folgenden Funktionen:

- Umwandeln von Ereignissen.
- Hinzufügen einer Geschäftsrelevanz zu Ereignissen durch den Zuordnungsservice
- Weiterleiten der Ereignisse
- Ermitteln von Echtzeit- und Nicht-Echtzeit-Daten sowie von Anfälligkeits- und Inventardaten
- Senden von Statusmeldungen an den Sentinel-Server

2.3.1 Collectors

Collectors standardisieren und erfassen die Informationen von den Connectors. Collectors werden in JavaScript erstellt und definieren die Logik für Folgendes:

- Empfangen der Rohdaten von den Connectors
- Analysieren und Standardisieren der Daten
- Anwenden wiederholbarer Logik auf die Daten
- Konvertieren gerätespezifischer Daten in Sentinel-spezifische Daten
- Formatieren der Ereignisse
- Weiterleiten der standardisierten, analysierten und formatierten Daten an den Collector-Manager
- Gerätespezifisches Filtern der Ereignisse.

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

2.3.2 Connectors

Connectors stellen die Verbindungen zwischen den Ereignisquellen und dem Sentinel-System her. Connectors verwenden branchenübliche Protokolle zum Erfassen von Ereignissen, wie Syslog, JDBC zum Lesen von Datenbanktabellen, WMI zum Lesen von Windows-Ereignisprotokollen usw. Connectors stellen Folgendes bereit:

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

2.4 Agent Manager

Der Agent Manager bietet eine hostbasierte Datenerfassung zur Ergänzung der agentlosen Datenerfassung. Er ermöglicht Folgendes:

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

2.5 NetFlow Collector-Manager

Der NetFlow Collector-Manager erfasst Netzwerkablaufdaten (NetFlow, IPFIX usw.) von Netzwerkgeräten wie Routern, Switches und Firewalls. Die Netzwerkablaufdaten beschreiben grundlegende Informationen zu allen Netzwerkverbindungen zwischen den Hosts, beispielsweise die übertragenen Pakete und Byte, so dass Sie das Verhalten einzelner Hosts im gesamten Netzwerk visualisieren können.

Der NetFlow Collector-Manager bietet die folgenden Funktionen:

- Erfassen von Netzwerkablaufdaten (Byte, Flow und Paketen) von unterstützten Netzwerkgeräten.
- Aggregieren der erfassten Daten und Senden dieser Daten an den Sentinel-Server, auf dem die Netzwerkaktivitäten in Ihrer Umgebung dann visualisiert und analysiert werden.

Weitere Informationen zum Visualisieren und Analysieren der Netzwerkablaufdaten finden Sie unter „Visualizing and Analyzing Network Flow Data“ (Visualisieren und Analysieren der Netzwerkablaufdaten) im *NetIQ Sentinel User Guide* (NetIQ Sentinel-Benutzerhandbuch).

2.6 Daten-Routing und Datenspeicherung in Sentinel

Sentinel bietet mehrere Optionen zum Weiterleiten, Speichern und Extrahieren der erfassten Daten. Standardmäßig erhält Sentinel von den Collector-Managern zwei getrennte, aber verwandte Datenströme: die analysierten Ereignisdaten und die Rohdaten. Die Rohdaten werden sofort in geschützten Partitionen gespeichert, um eine sichere Beweiskette bereitzustellen. Die analysierten Ereignisdaten werden gemäß den von Ihnen definierten Regeln weitergeleitet. Sie können gefiltert,

zum Speicher oder zur Echtzeitanalyse gesendet oder an externe Systeme weitergeleitet werden. Alle zum Speicher gesendeten Ereignisdaten werden mit benutzerdefinierten Beibehaltungsrichtlinien abgeglichen, um zu ermitteln, in welcher Partition die Daten abgelegt werden. Diese Richtlinien umfassen auch die Bereinigungsrichtlinien zur Beibehaltung bzw. zum Löschen der Ereignisdaten.

Der Datenspeicher in Sentinel basiert auf einer Struktur mit drei Ebenen:

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	Wenn Partitionen geschlossen werden, können Sie sie auf einem Offlinespeicher wie Amazon Glacier sichern. Bei Bedarf können Sie die Partitionen vorübergehend wieder importieren, um sie in forensischen Langzeit-Analysen zu verwenden.

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 Storage“ (Konfigurieren der Datenspeicherung) im *NetIQ Sentinel Administration Guide (NetIQ Sentinel-Administrationshandbuch)*.

2.7 Korrelation

Ein einzelnes Ereignis mag unbedeutend erscheinen. In Verbindung mit anderen Ereignissen kann es jedoch vor potenziellen Problemen warnen. Sentinel unterstützt Sie bei der Ereigniskorrelation, indem es die Regeln anwendet, die Sie in der Correlation Engine erstellen und bereitstellen, und geeignete Maßnahmen zum Abschwächen des Problems ergreift.

Die Korrelation bietet zusätzliche Intelligenz bei der Verwaltung von Sicherheitsereignissen, indem sie die Analyse des eingehenden Ereignisstroms automatisiert und auf diese Weise sicherheitsrelevante Muster erkennt. 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 finden Sie unter „Correlating Event Data (Korrelation von Ereignisdaten) “ im *NetIQ Sentinel User Guide (NetIQ Sentinel 7.1-Benutzerhandbuch)*.

Um Ereignisse entsprechend den Korrelationsregeln zu überwachen, müssen die Regeln in der Correlation Engine bereitgestellt werden. Wenn ein Ereignis eintritt, das die Regelkriterien erfüllt, generiert die Correlation Engine ein Korrelationsereignis, das das Muster beschreibt. Weitere Informationen finden Sie unter „Correlation Engine“ im *NetIQ Sentinel User Guide (NetIQ Sentinel 7.1-Benutzerhandbuch)*.

2.8 Sicherheitsintelligenz

Die Korrelationsfunktion in Sentinel bietet die Möglichkeit, nach bekannten Aktivitätsmustern zu suchen, ob für Sicherheits-, Compliance- oder andere Gründe. Die Sicherheitsintelligenzfunktion sucht nach Aktivitäten, die ungewöhnlich und möglicherweise schädlich sind, aber mit keinem bekannten Muster übereinstimmen.

Die Sentinel-Funktion der Sicherheitsintelligenz setzt in erster Linie auf die statistische Analyse von Zeitreihendaten. Die Funktion ermöglicht Analysten die Erkennung und Analyse von Abweichungen (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 *NetIQ Sentinel User Guide* (NetIQ Sentinel 7.1-Benutzerhandbuch).

2.9 Problembehebung

Sentinel bietet eine automatisierte Vorfallsreaktions-Verwaltung, mit der Sie den Prozess der Verfolgung, Eskalation und Reaktion auf Vorfälle und Richtlinienverstöße dokumentieren und formalisieren können. Außerdem wird die bidirektionale Integration in Problemberichtssysteme ermöglicht. 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 *NetIQ Sentinel User Guide (NetIQ Sentinel 7.1-Benutzerhandbuch)*.

2.10 iTRAC-Workflows

iTRAC-Workflows bieten eine einfache, flexible Lösung für die Automatisierung und Nachverfolgung der Vorfallsbehandlungsprozesse in einem Unternehmen. iTRAC nutzt das interne Vorfallsystem von Sentinel zur Verfolgung von Sicherheits- und Systemproblemen von deren Identifizierung (mithilfe von Korrelationsregeln oder durch manuelle Erkennung) bis hin zu deren Behebung.

Workflows können aus manuellen und automatischen Schritten bestehen. Auch erweiterte Funktionen wie Verzweigungen, zeitgesteuerte Eskalation und lokale Variablen werden unterstützt. 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 *NetIQ Sentinel User Guide* (NetIQ Sentinel 7.1-Benutzerhandbuch).

2.11 Aktionen und Integratoren

Mit Aktionen wird entweder manuell oder automatisch eine bestimmte Aktion in Sentinel ausgeführt, beispielsweise das Senden einer Email. Aktionen können durch Routing-Regeln, durch das manuelle Ausführen 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 *NetIQ Sentinel Administration Guide (NetIQ Sentinel 7.1-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 *NetIQ Sentinel Administration Guide (NetIQ Sentinel 7.1-Administrationshandbuch)*.

2.12 Suchvorgänge

Sentinel bietet eine Option zum Suchen nach Ereignissen. Die Daten können dabei im Primärspeicher oder im Sekundärspeicher gesucht werden. 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 unter „Performing a Search“ (Ausführen einer Suche) im *NetIQ 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 *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

2.13 Berichte

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

Sie können PDF-Berichte ausführen, planen und per E-Mail versenden. Sie können jeden Bericht als Suche ausführen und das Ergebnis wie bei jeder Suche beeinflussen, 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 *NetIQ Sentinel User Guide (NetIQ Sentinel-Benutzerhandbuch)*.

2.14 Identitätsnachverfolgung

Sentinel bietet ein Integrations-Framework für Identitätsmanagementsysteme, um die Identitäten jedes Benutzerkontos und die von diesen Identitäten ausgeführten Ereignisse nachzuverfolgen. Sentinel stellt Benutzerinformationen bereit, beispielsweise Kontaktinformationen, Benutzerkonten, kürzlich erfolgte Authentifizierungs- und Zugriffsereignisse und Berechtigungsänderungen. Das Anzeigen von Informationen über Personen, die eine bestimmte Aktion initiieren oder von einer bestimmten Aktion betroffen sind, ermöglicht reduzierte Vorfallsantwortzeiten und eine verhaltensbasierte Analyse. Weitere Informationen finden Sie unter „Leveraging Identity Information“ (Nutzen von Identitätsinformationen) im *NetIQ Sentinel User Guide* (NetIQ Sentinel-Benutzerhandbuch).

2.15 Ereignisanalyse

Sentinel stellt leistungsfähige Tools zur Verfügung, um Sie beim Erkennen und Analysieren kritischer Ereignisdaten zu unterstützen. Das System ist auf höchste Effizienz für beliebige Analysetypen abgestimmt und optimiert und stellt Methoden zur Verfügung, die den nahtlosen Übergang von einer Analyseart zur anderen ermöglichen.

Das Untersuchen von Ereignissen in Sentinel beginnt meist mit den Active Views, die Daten in nahezu Echtzeit darstellen. Ergänzend zu ausgefeilteren Tools zeigen Active Views gefilterte Ereignisströme mit zusammenfassenden Diagrammen an, die zur einfachen, groben Analyse 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 Active Views als Dashboard verwenden, das den allgemeinen Betriebs- und Sicherheitsstand darstellt.

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

Wenn Sie Hunderte von Ereignissen analysieren, bieten die Berichtfunktionen von Sentinel eine benutzerdefinierte Steuerung des Ereignislayouts und die Möglichkeit zur Anzeige größerer Datenmengen. Sentinel erleichtert diesen Übergang durch die Möglichkeit, interaktive Suchen aus der Suchoberfläche in eine Berichtvorlage zu übertragen. Hier wird sofort ein Bericht erstellt, der die gleichen Daten anzeigt, jedoch in einem Format, das für eine große Anzahl an Ereignissen besser geeignet ist.

Für diesen Zweck enthält Sentinel viele verschiedene Vorlagen. Einige Vorlagen sind auf die Anzeige bestimmter Informationstypen abgestimmt, beispielsweise Authentifizierungsdaten oder Daten zur Benutzererstellung, andere sind Allzweckvorlagen, in denen Sie Gruppen und Spalten im Bericht interaktiv anpassen können.

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

II Planen der Sentinel-Installation

Dieser Abschnitt enthält Tipps zu den Überlegungen, die Sie bei der Planung einer Sentinel-Installation berücksichtigen sollten. Wenden Sie sich an den Technischen Support von NetIQ, wenn Sie eine Konfiguration installieren möchten, die in den folgenden Abschnitten nicht behandelt wird, oder wenn Sie Fragen haben.

3 Implementierungs-Checkliste

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

❒	Aufgaben	Erklärt in
❒	Sehen Sie sich die Informationen zur Produktarchitektur an, um die Sentinel-Komponenten kennenzulernen.	Teil I, „Sentinel“, auf Seite 13.
❒	Stellen Sie anhand der Sentinel-Lizenzierung fest, ob Sie die Evaluierungslizenz oder die Unternehmenslizenz von Sentinel verwenden sollten.	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.
❒	Prüfen Sie die Anzahl der Ereignisse pro Sekunde (EPS) des Collector-Managers und der Correlation Engine sowie die Datensätze pro Sekunde (RPS) vom NetFlow Collector-Manager. Ermitteln Sie die Anzahl der Collector-Manager, der Correlation Engines und der NetFlow Collector Manager, die zur Optimierung der Leistung und für den Lastenausgleich installiert werden müssen.	Abschnitt 6.1, „Vorteile von verteilten Bereitstellungen“, auf Seite 39.
❒	Lesen Sie die 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 63.
❒	Stellen Sie sicher, dass Sie die Uhrzeit am Sentinel-Server konfigurieren.	Kapitel 17, „Konfigurieren der Zeit“, auf Seite 101.
❒	Wenn Sie Sentinel installieren, werden alle zum Zeitpunkt der Veröffentlichung der Sentinel-Version verfügbaren Sentinel-Plugins standardmäßig installiert. Konfigurieren Sie die einsatzbereiten Plugins für die Datenerfassung und Berichterstellung.	Kapitel 19, „Konfigurieren von einsatzbereiten Plugins“, auf Seite 109.
❒	Sentinel enthält einsatzbereite 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.

❒	Aufgaben	Erklärt in
❒	Installieren Sie je nach den Anforderungen Ihrer Umgebung zusätzliche Collectors und Connectors.	Kapitel 15, „Installieren von zusätzlichen Collectors und Connectors“, auf Seite 95.
❒	Installieren Sie je nach den Anforderungen Ihrer Umgebung zusätzliche Collector-Manager und Correlation Engines.	Abschnitt 12.4, „Installieren von Collector-Managers und Correlation Engines“, auf Seite 74.

4 Lizenzinformationen

Die Sentinel-Plattform bietet ein breites Spektrum an Funktionen für die unterschiedlichsten Kundenanforderungen. Diese lassen sich mit den Lizenzierungsmodellen von NetIQ individuell erfüllen.

Bis Sentinel 7.3 war die grundlegende Sentinel-Plattform in Form von zwei Produkten verfügbar: Sentinel und Sentinel Log Manager. In Sentinel 7.3 vereint NetIQ diese beiden Produkte in einer zentralen Plattform, über die sich neue Funktionen, Patches und Dokumentationen einfacher zustellen lassen. Kunden erhalten über die neue Plattform einfacher Support und können genau die Lösungsmerkmale auswählen, die am besten zu ihren Anforderungen passen.

Die Sentinel-Plattform umfasst diese beiden Hauptlösungen:

- **Sentinel Enterprise:** Eine Lösung mit vollständiger Funktionalität, die alle Core-Funktionen für die visuelle Analyse in Echtzeit und vieles mehr umfasst. Sentinel Enterprise eignet sich besonders für SIEM-Anwendungsfälle wie die Bedrohungserfassung, Warnmeldung und Fehlerbehebung in Echtzeit.
- **Sentinel for Log Management:** Eine Protokollmanagementlösung zum Erfassen, Speichern und Durchsuchen von Daten sowie zum Erstellen von Datenberichten.

  Sentinel for Log Management 7.3 stellt eine deutliche Verbesserung der Funktionen von Sentinel Log Manager 1.2.2 dar. In einigen Aspekten wurde die Architektur erheblich verändert. Weitere Informationen zum Aufrüsten auf Sentinel for Log Management 7.3 finden Sie in den häufig gestellten Fragen unter https://www.netiq.com/products/sentinel/frequently-asked-questions/slm122-to-slm73-upgrade-faqs.html.

NetIQ lienziert diese beiden Lösungen unabhängig voneinander. Es wird jeweils die Lösung aktiviert, deren Lizenzschlüssel Sie hinzufügen. Andere Aspekte von Sentinel wie die EPS-Grenze, die maximale Geräteanzahl und die Plugins werden zusätzlich lizenziert. Weitere Details finden Sie in der Endbenutzer-Lizenzvereinbarung.

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	Ja	Ja
◆ Grundlegende Ereignissammlung		
◆ Sammlung von Nichtereignisdaten (Bestände, Schwachstellen, Identitäten)		
◆ Analyse und Standardisierung		
◆ Taxonomische Klassifikation von Ereignisdaten		
◆ Inline-Kontextzuordnung		
◆ NetFlow-Sammlung und -Speicherung		
◆ NetFlow-Echtzeitvisualisierung		
◆ Ereignisbasierte NetFlow-Visualisierung		
◆ Ereignissuche (lokal)		
◆ Ereignisberichterstellung		
◆ Ereignisfilterung		
◆ Echtzeit-Ereignisvisualisierung		
◆ Ereignisspeicherung		
◆ Datenaufbewahrungsrichtlinien		
◆ Ereignisspeicher-Verbindlichkeit		
◆ FIPS-Aktivierung		
◆ Manuell ausgelöste Aktionen		
◆ Manuelle Erstellung und Verwaltung von Vorfällen		
◆ Vorfallaktionen und -Workflows		
◆ iTRAC-Workflows		
Aktionen	Ja	Ja
◆ Korrelationsgesteuerte Aktionen (nur bei aktivierter Korrelation)		
◆ Routing regelgesteuerter Aktionen (nur bei aktivierten Regeln)		
◆ Manuell ausgelöste Aktionen		
Routing-Regeln	Ja	Ja
◆ Ereignis-Routing (extern)		
◆ Durch Routing-Regeln ausgelöste Aktionen (nur bei aktivierten Aktionen)		
Sentinel Link	Ja	Ja

Services und Funktionen	Sentinel Enterprise	Sentinel for Log Management
Korrelation ◆ Echtzeit-Schemakorrelation ◆ Durch Korrelationsregeln ausgelöste Aktionen (nur bei aktivierten Aktionen) ◆ Warnmeldungsselektierung ◆ Warnmeldungs-Dashboard	Ja	Nein
Datensynchronisierung	Ja	Ja
Wiederherstellung von archivierten Ereignisdaten	Ja	Ja
Datenverbund (verteilte Suche)	Ja	Ja
Sicherheitsintelligenz ◆ Anomalieregeln ◆ Statistische Echtzeitanalyse	Ja	Nein
Statistische Echtzeitanalyse	Ja	Nein
Lizenzablaufdatum	Nie	Nie
EPS-Grenze	Unbegrenzt	Unbegrenzt

4.1 Sentinel-Lizenzen

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

- Abschnitt 4.1.1, „Evaluierungslizenz“, auf Seite 35
- Abschnitt 4.1.2, „Freie Lizenz“, auf Seite 36
- Abschnitt 4.1.3, „Unternehmenslizenzen“, auf Seite 36

4.1.1 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, passt Sentinel das Ablaufdatum entsprechend an.

Nach Ablauf der Evaluierungslizenz gilt für das System ein Basislizenzschlüssel für einen begrenzten Funktionsumfang und eine EPS-Grenze von 25. Die Basislizenz wird auch als freie Lizenz bezeichnet.

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.

4.1.2 Freie Lizenz

Mit der freien Lizenz verfügt Ihr System über einen eingeschränkten Funktionsumfang und eine EPS-Grenze von 25. Die freie Lizenz hat kein Ablaufdatum.

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: Für die freie Sentinel-Version bietet NetIQ weder technischen Support noch Produkt-Updates.

4.1.3 Unternehmenslizenzen

Beim Kauf von Sentinel erhalten Sie über das Kundenportal einen Lizenzschlüssel. Je nach der erworbenen Lizenz aktiviert der Lizenzschlüssel bestimmte Funktionen, Datensammlungsraten und Ereignisquellen. 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 *NetIQ Sentinel Administration Guide* (NetIQ-Sentinel-Administrationshandbuch).

5 Erfüllen der Systemanforderungen

Eine Sentinel-Implementierung kann je nach den Anforderungen Ihrer Umgebung unterschiedlich ausfallen. Ziehen Sie daher vor der Fertigstellung der Sentinel-Architektur die NetIQ Consulting Services oder einen der NetIQ Sentinel-Partner zu Rate.

Die Hardwarevoraussetzungen sowie die unterstützten Betriebssysteme, Appliance-Plattformen und Browser sind auf der Website mit technischen Daten zu NetIQ Sentinel aufgeführt.

5.1 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 Sentinel-Plugins-Website.

5.2 Virtuelle Umgebung

Sentinel ist eingehend getestet und wird auf einem VMware ESX-Server vollständig unterstützt. Wenn Sie eine virtuelle Umgebung einrichten, müssen die virtuellen Maschinen über mindestens 2 CPUs verfügen. Um auf ESX oder in anderen virtuellen Umgebungen Ergebnisse zu erzielen, die mit den Testergebnissen auf physischen Computern vergleichbar sind, sollte die virtuelle Umgebung dieselben Anforderungen an Arbeitsspeicher, CPU, Speicherplatz und E/A erfüllen, die auch für physische Computer gelten.

Weitere Informationen zu Empfehlungen für physische Computer finden Sie unter Kapitel 5, „Erfüllen der Systemanforderungen“, auf Seite 37.

6 Überlegungen zur Bereitstellung

Sentinel verfügt über eine skalierbare Architektur, die je nach zutreffender Last angepasst werden kann. Die auf Sentinel angewendete Last kann unterschiedlicher Art sein. Dieses Kapitel enthält einen Überblick der wichtigsten Punkte, die bei der Skalierung einer Sentinel-Bereitstellung berücksichtigt werden sollten. Ein Experte von NetIQ Services oder NetIQ Partner Services kann Sie dabei unterstützen, ein System für Ihre individuelle Umgebung zu entwerfen.

6.1 Vorteile von verteilten Bereitstellungen

Standardmäßig beinhaltet der Sentinel-Server die folgenden Komponenten:

- **Collector Manager:** Der Collector-Manager stellt eine flexible Datenerfassungsstelle für Sentinel bereit. Das Sentinel-Installationsprogramm installiert während der Installation standardmäßig einen Collector-Manager.
- **Correlation Engine:** Die Correlation Engine verarbeitet Ereignisse aus dem Echtzeit-Ereignisstrom, um zu ermitteln, ob Korrelationsregeln ausgelöst werden sollen.
- **NetFlow Collector-Manager:** Der NetFlow Collector-Manager erfasst Netzwerkablaufdaten (NetFlow, IPFIX usw.) von Netzwerkgeräten wie Routern, Switches und Firewalls. Die Netzwerkablaufdaten beschreiben grundlegende Informationen zu allen Netzwerkverbindungen zwischen den Hosts, beispielsweise die übertragenen Pakete und Byte, so dass Sie das Verhalten einzelner Hosts im gesamten Netzwerk visualisieren können.

WICHTIG: Für Produktionsumgebungen empfiehlt die NetIQ Corporation das Einrichten einer verteilten Bereitstellung, da hierbei die Datensammlungskomponenten 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.

6.1.1 Vorteile zusätzlicher Collector-Manager-Instanzen

Der Sentinel-Server umfasst standardmäßig einen Collector-Manager. Für Produktionsumgebungen bieten verteilte Collector-Manager 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 mehrere Vorteile:

- **Verbesserte Systemleistung:** Zusätzliche Collector-Manager 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 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 an den geeigneten Speicherorten in Ihrem Netzwerk installieren. Diese Remote-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 Abschnitt 12.4, „Installieren von Collector-Managers und Correlation Engines“, auf Seite 74.

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

6.1.2 Vorteile zusätzlicher Correlation Engines

Sie können mehrere Correlation Engines (jede auf einem eigenen Server) bereitstellen, ohne dass Konfigurationen repliziert oder Datenbanken hinzugefügt werden müssen. Für Umgebungen mit vielen Korrelationsregeln oder extrem hohen Ereignisraten kann es von Vorteil sein, mehr als eine Correlation Engine zu installieren und einige Regeln auf der neuen Correlation Engine erneut bereitzustellen. Mehrere Correlation Engines bieten die Möglichkeit der Skalierung, weil das Sentinel-System zusätzliche Datenquellen umfasst oder weil die Ereignisrate steigt. Informationen zur Installation von zusätzlichen Correlation Engines finden Sie unter Abschnitt 12.4, „Installieren von Collector-Managers und Correlation Engines“, auf Seite 74.

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

6.1.3 Vorteile zusätzlicher NetFlow Collector-Manager-Instanzen

Der NetFlow Collector-Manager erfasst Netzwerkablaufdaten von Netzwerkgeräten. Um Systemressourcen für andere wichtige Funktionen freizugeben, beispielsweise für das Speichern und Suchen von Ereignissen, installieren Sie bevorzugt weitere NetFlow Collector-Manager, statt den NetFlow Collector-Manager auf dem Sentinel-Server zu nutzen.

In den folgenden Szenarien können Sie zusätzliche NetFlow Collector-Manager installieren:

- In Umgebungen mit zahlreichen Netzwerkgeräten und großen Mengen an Netzwerkablaufdaten können Sie mehrere NetFlow Collector-Manager installieren und so die Belastung verteilen.
- In einer multimandantenfähigen Umgebung sollten Sie je einen NetFlow Collector-Manager für jeden Mandanten installieren, damit separate Netzwerkablaufdaten für die einzelnen Mandanten erfasst werden.

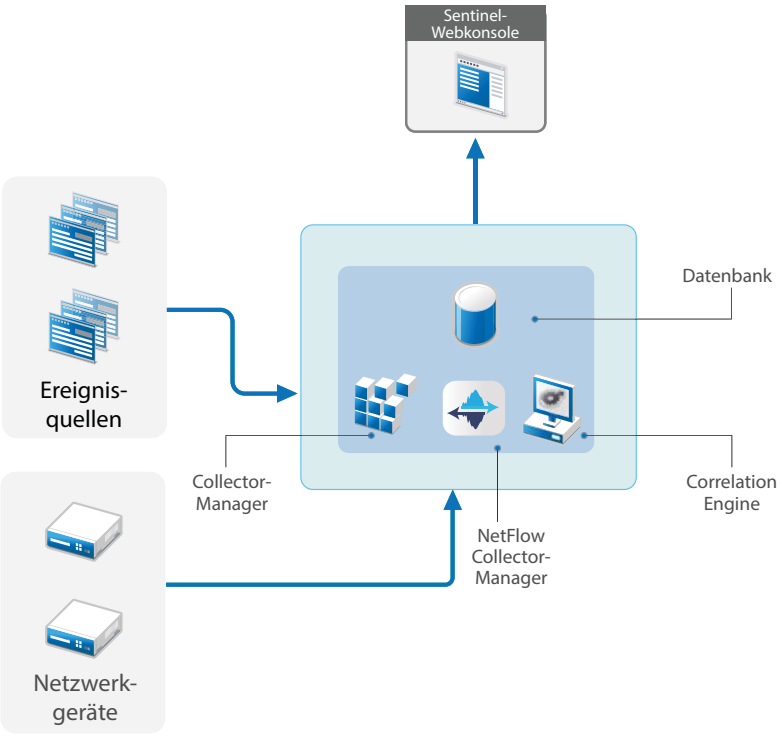
Weitere Informationen zum Installieren von zusätzlichen NetFlow Collector-Managern finden Sie unter Kapitel 14, „Installation des NetFlow Collector-Managers“, auf Seite 91.

6.2 All-In-One-Bereitstellung

Die einfachste Bereitstellungsoption ist ein All-In-One-System, bei dem alle Sentinel-Komponenten auf einem einzigen 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 geringfügige Ressourcenkonflikte zwischen den Komponenten Leistungsprobleme verursachen.

WICHTIG: Für Produktionsumgebungen empfiehlt die NetIQ Corporation das Einrichten einer verteilten Bereitstellung, da hierbei die Datensammlungskomponenten auf einem separaten Computer isoliert werden. Dies ist für die Bewältigung von Spitzenlasten und anderen Anomalien mit größtmöglicher Systemstabilität wichtig.

Abbildung 6-1 All-In-One-Bereitstellung

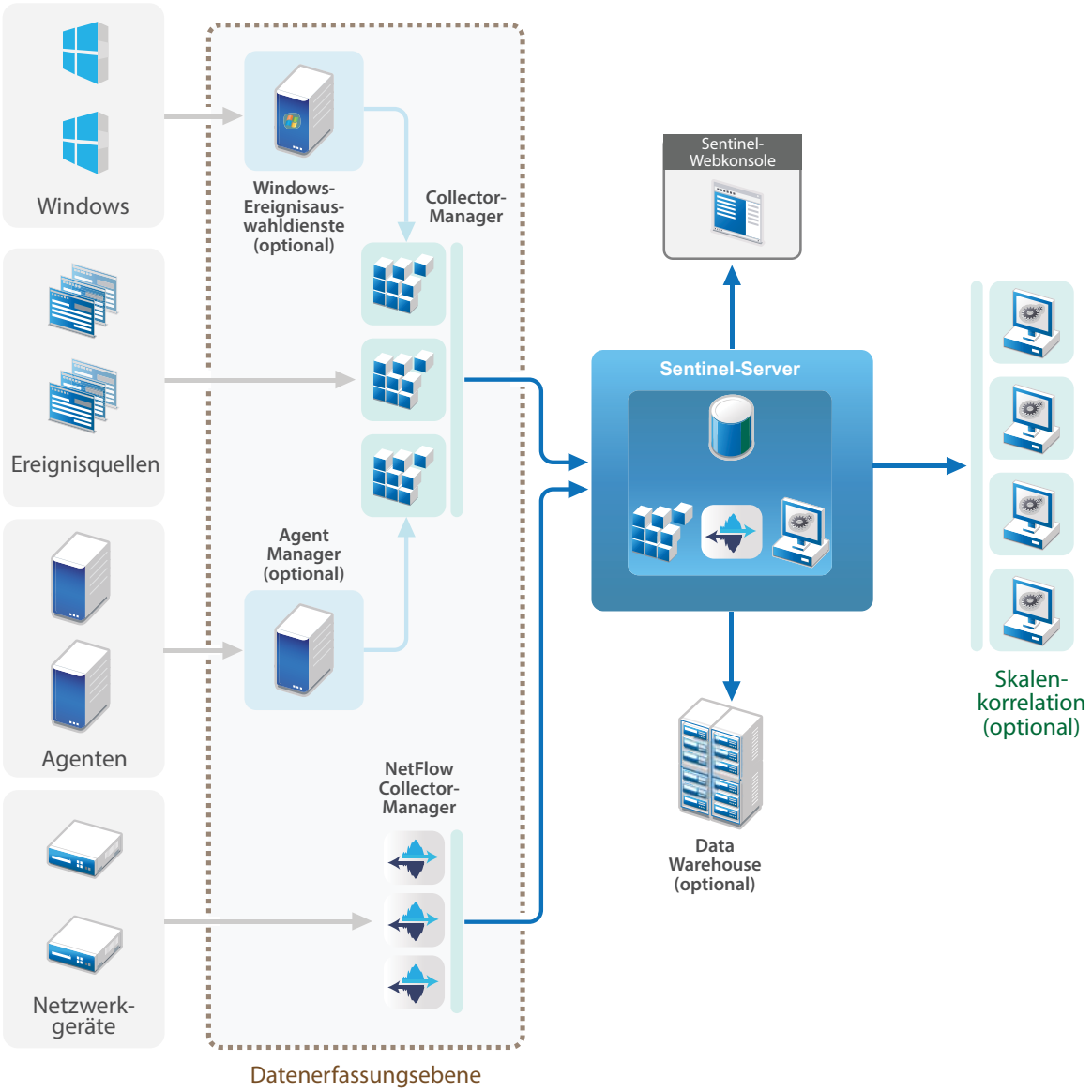


6.3 Verteilte Ein-Ebenen-Bereitstellung

Die Ein-Ebenen-Bereitstellung bietet die Möglichkeit, Windows-Computer zu überwachen und eine höhere Last als mit der All-In-One-Bereitstellung zu verarbeiten. Die Datenerfassung und Korrelation kann durch Hinzufügen von Collector-Manager-, NetFlow Collector-Manager- und Correlation Engine-Computern skaliert werden, die die Verarbeitungslast vom zentralen Sentinel-Server nehmen. Remote-Collector-Manager, Remote-Correlation Engines und Remote-NetFlow Collector-Manager übernehmen die Last der Ereignisse, Korrelationsregeln und Netzwerkablaufdaten und geben außerdem Ressourcen auf dem zentralen Sentinel-Server frei, sodass er 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.

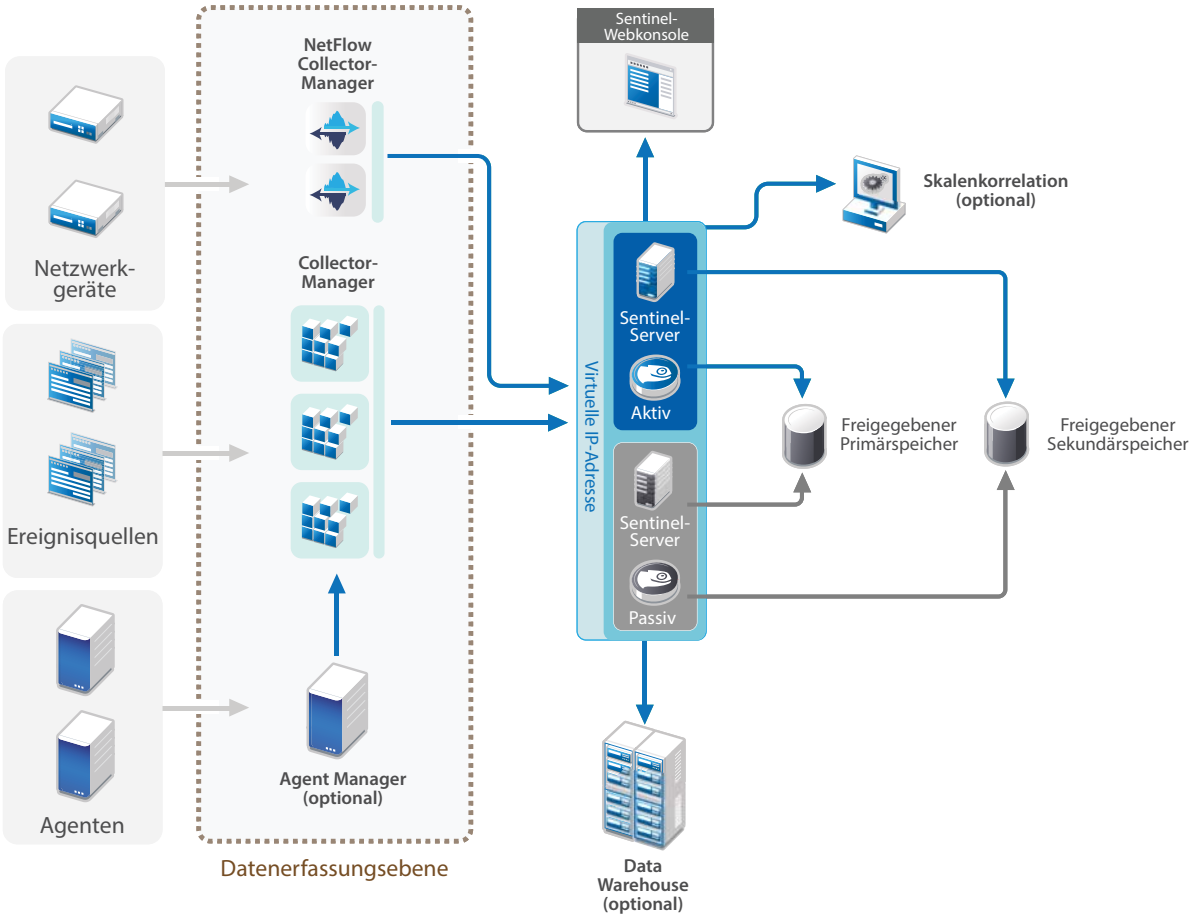
Abbildung 6-2 *Verteilte Ein-Ebenen-Bereitstellung*



6.4 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 VI, „Bereitstellen von Sentinel für Hochverfügbarkeitssysteme“, auf Seite 145.

Abbildung 6-3 *Verteilte Ein-Ebenen-Bereitstellung mit hoher Verfügbarkeit*

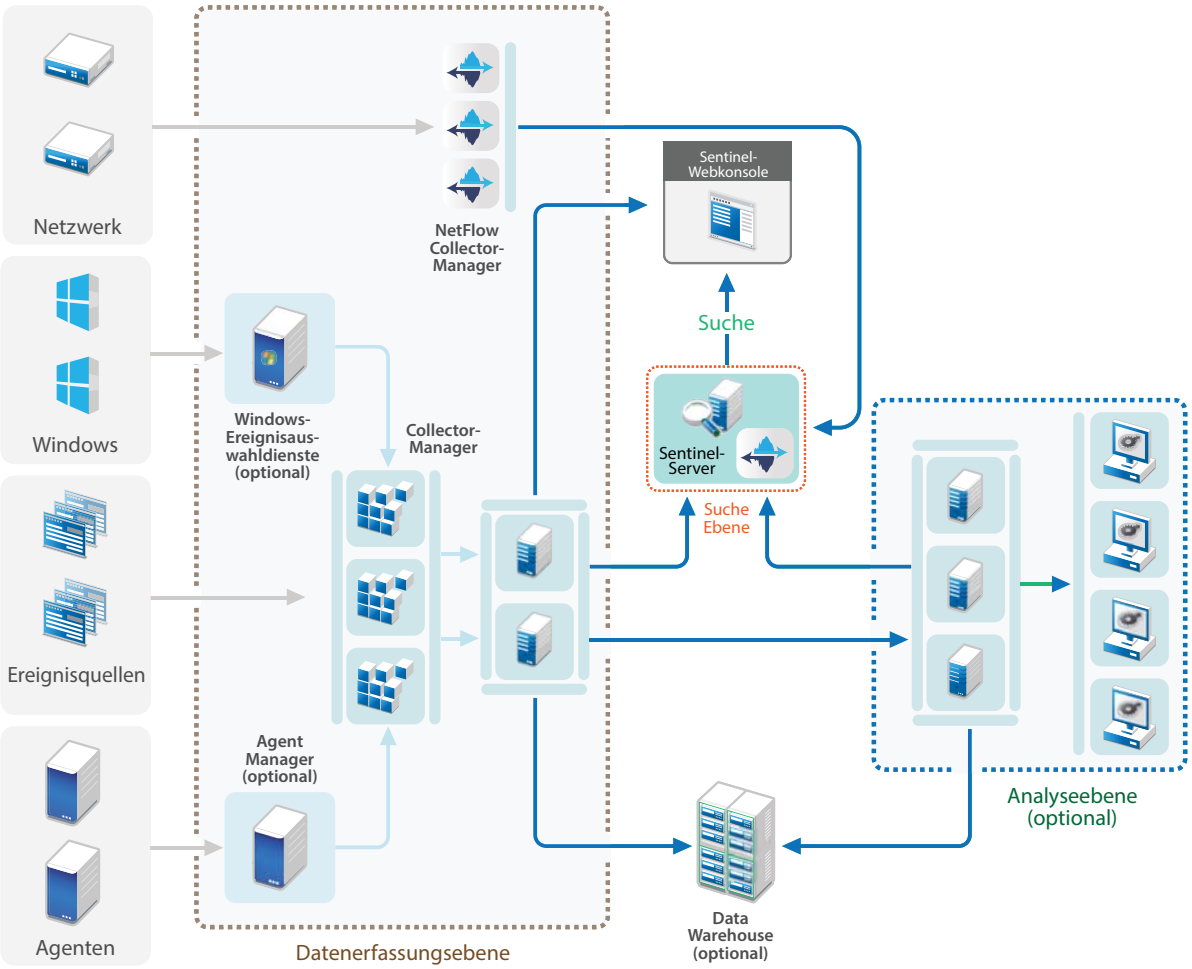


6.5 Verteilte Zwei-Ebenen- und Drei-Ebenen-Bereitstellung

Mit dieser Art der Bereitstellung kann die Lastverarbeitungskapazität eines einzelnen, zentralen Sentinel-Servers übertroffen werden. Die Verarbeitungslast wird über mehrere Sentinel-Instanzen verteilt, indem die Funktion von Sentinel Link und der verteilten Sentinel-Suche optimal ausgenutzt werden. Die Last der Datenerfassung wird über mehrere Sentinel-Server verteilt, die jeweils über mehrere Collector-Manager 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 Zugriffspunkt für Suchen über Sentinel Link im gesamten System und in allen Ebenen dar. Da die Suchanforderung über mehrere Instanzen von Sentinel verbündet wird, bietet diese Art der Bereitstellung auch eine Lastverteilung bei Suchen, die zur Verarbeitung einer hohen Suchlast nützlich ist.

Die Netzwerkablaufdaten werden in der Suchebene gespeichert, was die einfache Navigation von den Suchergebnissen zur kontextabhängigen Netzwerkdatenverkehrsanalyse ermöglicht.

Abbildung 6-4 *Verteilte Zwei-Ebenen- und Drei-Ebenen-Bereitstellung*



6.6 Planen von Partitionen für die Datenspeicherung

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

Die gesamte Verzeichnisstruktur unter dem Verzeichnis `/var/opt/novell/sentinel` muss sich in einer einzigen Datenträgerpartition befinden, um eine richtige Berechnung der Datenträgerauslastung zu gewährleisten. Andernfalls werden Ereignisdaten möglicherweise vorzeitig durch die automatische Datenverwaltung gelöscht. Weitere Informationen zur Sentinel-Verzeichnisstruktur finden Sie unter Abschnitt 6.6.4, „Sentinel-Verzeichnisstruktur“, auf Seite 47.

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 Festplattenpartitionierung.

6.6.1 Partitionen in herkömmlichen Installationen

In herkömmlichen Partitionen können Sie das Layout der Datenträgerpartition des Betriebssystems vor der Installation von Sentinel bearbeiten. Der Administrator muss hierzu die gewünschten Partitionen erstellen und in den entsprechenden Verzeichnissen einhängen. Beachten Sie hierzu die in Abschnitt 6.6.4, „Sentinel-Verzeichnisstruktur“, auf Seite 47 detailliert dargestellte Verzeichnisstruktur. 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`.

6.6.2 Partitionen in einer Appliance-Installation

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 Abschnitt 13.3.2, „Erstellen von Partitionen“, auf Seite 87.

6.6.3 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
Temp	`/tmp`	30 GB	Standort der Betriebssystemdateien und temporären Sentinel-Dateien. Die Abgrenzung dieser Dateien in einer separaten Partition schützt die Anwendungsdaten vor Beschädigung, falls ein Endlosprozess den temporären Speicher ausfüllt.
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.

6.6.4 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`.
- Die Konfigurationsdateien befinden sich im Verzeichnis `/etc/opt/novell/sentinel/`.
- Die Prozess-ID-Datei (PID-Datei) befindet sich im Verzeichnis `/var/run/sentinel/server.pid`

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

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

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

Durch die Aktivierung des Sentinel FIPS 140-2-Modus wird für die Kommunikation zwischen dem Sentinel-Server, den Sentinel-Remote-Collector-Managern, den Sentinel-Remote-Correlation Engines, der Sentinel-Weboberfläche, dem Sentinel Control Center und dem Sentinel-Advisor-Service die FIPS 140-2-validierte Verschlüsselung verwendet.

7.1 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 bereitgestellt wird, ist FIPS 140-2-validiert. Das von SLES 11 SP3 bereitgestellte 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 6.2 finden Sie im Abschnitt *FIPS 140-1- und FIPS 140-2-validierte Verschlüsselungsmodule*.

7.1.1 RHEL-NSS-Pakete

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

- nspr-4.9-1.el6.x86_64
- nss-sysinit-3.13.3-6.el6.x86_64
- nss-util-3.13.3-2.el6.x86_64
- nss-softokn-freebl-3.12.9-11.el6.x86_64
- nss-softokn-3.12.9-11.el6.x86_64
- nss-3.13.3-6.el6.x86_64
- nss-tools-3.13.3-6.el6.x86_64

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

7.1.2 SLES-NSS-Pakete

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

- libfreebl3-3.13.1-0.2.1
- mozilla-nspr-4.8.9-1.2.2.1
- mozilla-nss-3.13.1-0.2.1
- mozilla-nss-tools-3.13.1-0.2.1

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

7.2 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, wenn der Dateiereignistyp „lokal“ oder NFS ist.
  - 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

  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 116.

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. Anweisungen 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 121.

- 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.

- NetIQ 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 Sie möchten, dass eines der Plugins, das noch nicht aktualisiert wurde, mit FIPS-Unterstützung bereitgestellt werden soll, können Sie eine Anforderung über Bugzilla senden.

7.3 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.	Abschnitt 7.4, „Bereitstellungsszenarien“, auf Seite 52.
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.	Abschnitt 12.2.2, „Angepasste Installation“, auf Seite 71. Abschnitt 12.3, „Ausführen einer automatischen Installation“, auf Seite 73 Kapitel 20, „Aktivieren des FIPS 140-2-Modus in einer vorhandenen Sentinel-Installation“, auf Seite 111
Konfigurieren Sie die Sentinel-Plugins zur Ausführung im FIPS 140-2-Modus.	Abschnitt 21.5, „Konfigurieren der Sentinel-Plugins zur Ausführung im FIPS 140-2-Modus“, auf Seite 116.
Importieren Sie Zertifikate in den Sentinel-FIPS-Keystore.	Abschnitt 21.6, „Importieren von Zertifikaten in die FIPS-Keystore-Datenbank“, auf Seite 122

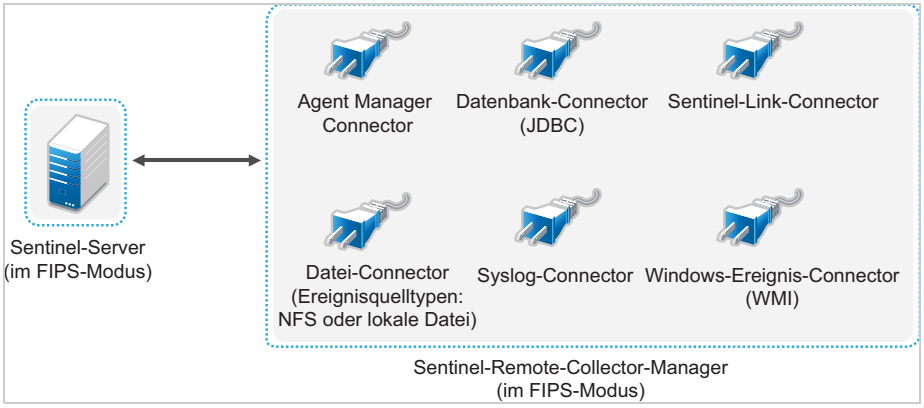
HINWEIS: NetIQ rät Ihnen dringend, eine Sicherung Ihres Sentinel-Systems zu erstellen bevor Sie mit der Umstellung auf den FIPS-Modus beginnen. Falls der Server aus irgendeinem Grund in den Nicht-FIPS-Modus zurückgesetzt werden muss, ist die Wiederherstellung aus einer Sicherung die einzige unterstützte Methode dafür. Weitere Informationen zum Zurücksetzen in den Nicht-FIPS-Modus finden Sie unter „Zurücksetzen von Sentinel in den Nicht-FIPS-Modus“, auf Seite 122.

7.4 Bereitstellungsszenarien

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

7.4.1 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 einen Remote-Collector-Manager erfasst werden. Sie können einen oder mehrere Remote-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 111.

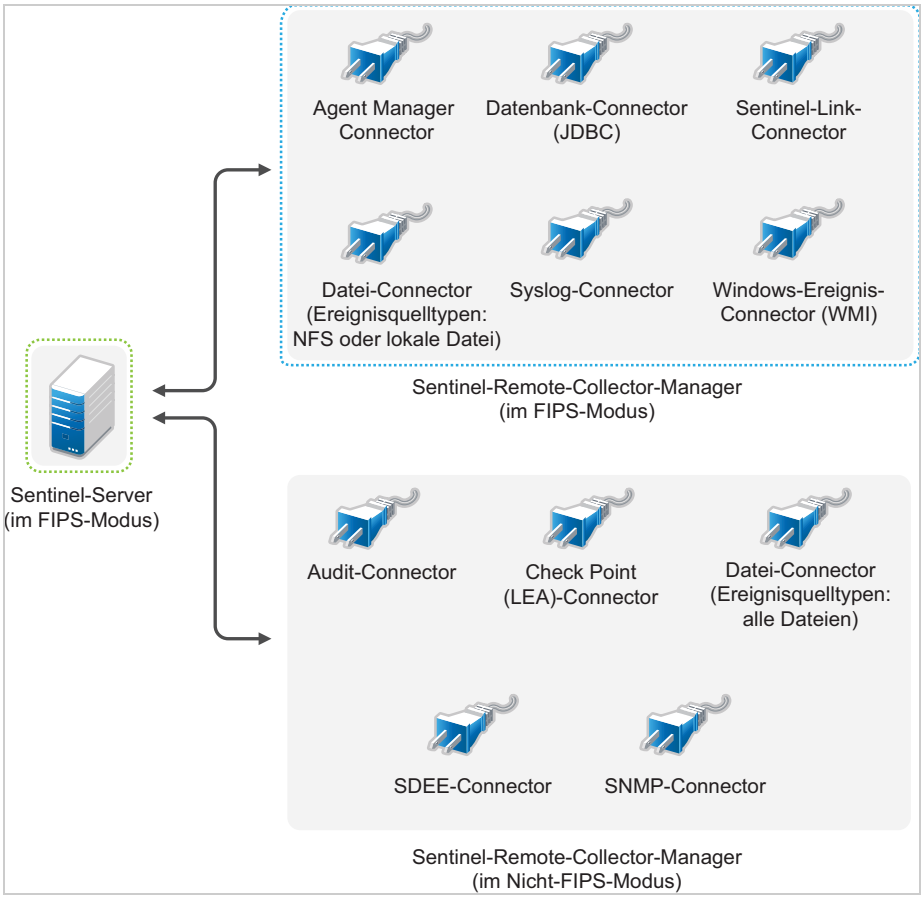
2. Sie müssen über einen Sentinel-Remote-Collector-Manager verfügen, der im FIPS 140-2-Modus ausgeführt wird.

   HINWEIS: Wenn Ihr (neu installierter oder aktualisierter) Remote-Collector-Manager im Nicht-FIPS-Modus ausgeführt wird, müssen sie FIPS am Remote-Collector-Manager aktivieren. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus auf Remote-Collector-Managern und Remote-Correlation Engines“, auf Seite 111.

3. Vergewissern Sie sich, dass der FIPS-Server und die Remote-Collector-Manager miteinander kommunizieren.
4. Stellen Sie eventuell vorhandene Remote-Correlation Engines auf den FIPS-Modus um. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus auf Remote-Collector-Managern und Remote-Correlation Engines“, auf Seite 111.
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 116.

7.4.2 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 nehmen an, dass in dieser Umgebung ein Server vorhanden ist und die Daten durch einen Remote-Collector-Manager erfasst werden. Sie können einen oder mehrere Remote-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-Collector-Manager verwenden. Der eine wird im FIPS 140-2-Modus ausgeführt für Connectors, die FIPS unterstützen. Der andere wird im Nicht-FIPS-Modus (normalen Modus) ausgeführt für Connectors, die den FIPS 140-2-Modus nicht unterstützen.

Sie müssen die folgende Prozedur ausführen, wenn in Ihrer Umgebung Daten von Ereignisquellen mit Connectors erfasst werden, die den FIPS 140-2-Modus unterstützen, und 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 111.

---

2 Stellen Sie sicher, dass ein Remote-Collector-Manager im FIPS 140-2-Modus ausgeführt wird und ein anderer Remote-Collector-Manager weiterhin im Nicht-FIPS-Modus.

   2a Wenn Sie über keinen Remote-Collector-Manager verfügen, der für den FIPS 140-2-Modus aktiviert wurde, müssen Sie den FIPS-Modus auf einem Remote-Collector-Manager aktivieren. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus auf Remote-Collector-Managern und Remote-Correlation Engines“, auf Seite 111.

   2b Aktualisieren Sie das Serverzertifikat auf dem Remote-Collector-Manager im Nicht-FIPS-Modus. Weitere Informationen finden Sie unter „Aktualisieren der Serverzertifikate in Remote-Collector-Managern und Remote-Correlation Engines“, auf Seite 115.

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

4 Stellen Sie eventuell vorhandene Remote-Correlation Engines auf den FIPS-Modus um. Weitere Informationen finden Sie unter „Aktivieren des FIPS 140-2-Modus auf Remote-Collector-Managern und Remote-Correlation Engines“, auf Seite 111.

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 116.

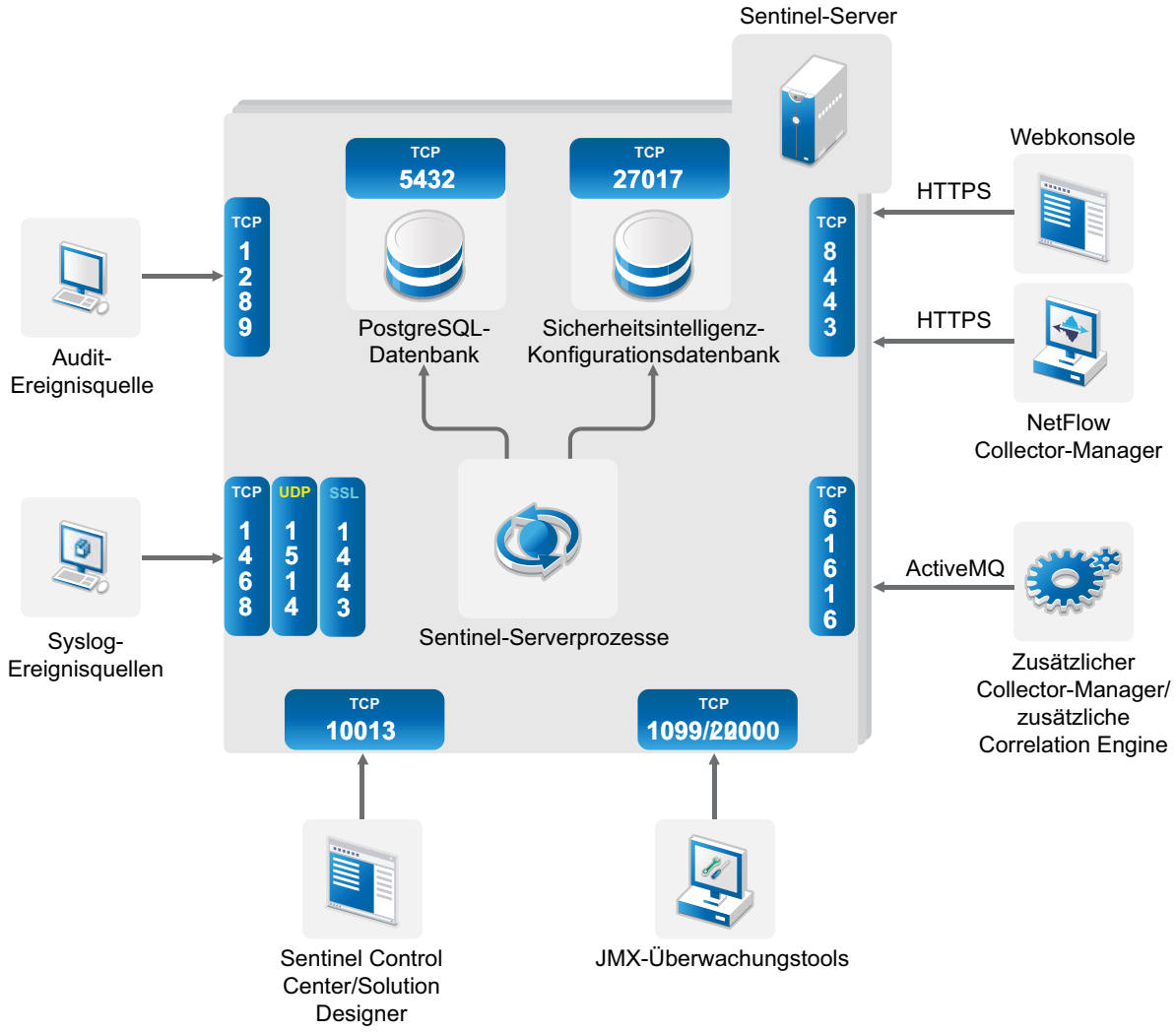
   5a Stellen Sie Connectors, die den FIPS 140-2-Modus unterstützen, im Remote-Collector-Manager bereit, der im FIPS-Modus ausgeführt wird.

   5b Stellen Sie Connectors, die den FIPS 140-2-Modus nicht unterstützen, im Remote-Collector-Manager bereit, der 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. In der folgenden Abbildung sind die in Sentinel verwendeten Ports dargestellt:

Abbildung 8-1 *In Sentinel verwendete Ports*



- Abschnitt 8.1, „Sentinel-Server-Ports“, auf Seite 56
- Abschnitt 8.2, „Collector-Manager-Ports“, auf Seite 58
- Abschnitt 8.3, „Correlation Engine-Ports“, auf Seite 59
- Abschnitt 8.4, „NetFlow Collector-Manager-Ports“, auf Seite 60

8.1 Sentinel-Server-Ports

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

8.1.1 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 Weboberfläche 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.

8.1.2 Netzwerkports

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

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	Optional	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	Für die HTTPS-Kommunikation und eingehende Verbindungen von NetFlow Collector-Managern.
TCP 1443	Eingehend	Optional	Wird für SSL-verschlüsselte Syslog-Meldungen verwendet.
TCP 61616	Eingehend	Optional	Wird für eingehende Verbindungen von den Collector-Managern und den Correlation Engines verwendet.

Ports	Richtung	Erforderlich/ optional	Beschreibung
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-Collector-Manager-Instanzen verwendet, um über den SSL-Proxy eine Verbindung zum Server herzustellen. Dies ist jedoch ungewöhnlich. Standardmäßig verwenden die Remote-Collector-Manager-Instanzen für die Verbindung zum Server den SSL-Port 61616.
TCP 443	Ausgehend	Optional	Wenn Advisor verwendet wird, initiiert der Port eine Verbindung zum Advisor-Dienst über das Internet mit der Advisor-Aktualisierungs-URL (https://secure-www.novell.com/sentinel/download/advisor/).
TCP 8443	Ausgehend	Optional	Wenn die verteilte Suche 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.
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.

8.1.3 Spezifische Ports für die 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 die Sentinel Appliance verwendet.
TCP 4984	Eingehend	Erforderlich	Wird von der Verwaltungskonsole der Sentinel-Appliance (WebYaST) verwendet. Wird außerdem von der 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 Datensammlungsservern verwendet werden können, beispielsweise eines Syslog-Servers. Standardmäßig überwacht Sentinel diese Ports nicht.
TCP 443 oder 80	Ausgehend	Erforderlich	Initiiert eine Verbindung zum NetIQ-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.

8.2 Collector-Manager-Ports

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

8.2.1 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.

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 1099 und 2000	Eingehend	Optional	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.

8.2.2 Spezifische Ports für die Collector-Manager-Appliance

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

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 22	Eingehend	Erforderlich	Wird für sicheren Shell-Zugriff auf die Sentinel Appliance verwendet.
TCP 4984	Eingehend	Erforderlich	Wird von der Verwaltungskonsole der Sentinel-Appliance (WebYaST) verwendet. Wird außerdem von der 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	Ports die bei der Konfiguration von Datensammlungsservern verwendet werden können, beispielsweise eines Syslog-Servers. Standardmäßig überwacht Sentinel diese Ports nicht.
TCP 443	Ausgehend	Erforderlich	Initiiert eine Verbindung zum NetIQ-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.

8.3 Correlation Engine-Ports

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

8.3.1 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	Optional	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.

8.3.2 Spezifische Ports für die Correlation Engine-Appliance

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

Ports	Richtung	Erforderlich/ optional	Beschreibung
TCP 22	Eingehend	Erforderlich	Wird für sicheren Shell-Zugriff auf die Sentinel Appliance verwendet.
TCP 4984	Eingehend	Erforderlich	Wird von der Verwaltungskonsole der Sentinel-Appliance (WebYaST) verwendet. Wird außerdem von der Sentinel-Appliance für den Aktualisierungsservice verwendet.
TCP 443	Ausgehend	Erforderlich	Initiiert eine Verbindung zum NetIQ-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.

8.4 NetFlow Collector-Manager-Ports

Der NetFlow Collector-Manager verwendet die folgenden Ports für die Kommunikation mit anderen Komponenten:

Ports	Richtung	Erforderlich/ optional	Beschreibung
HTTPS 8443	Ausgehend	Erforderlich	Initiiert eine Verbindung zum Sentinel-Server.
3578	Eingehend	Erforderlich	Empfängt Netzwerkablaufdaten von Netzwerkgeräten.

9 Installationsoptionen

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

9.1 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.
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 Abschnitt 12.2, „Durchführen der interaktiven Installation“, auf Seite 70.

- **Automatisch:** Wenn Sie mehrere Sentinel-Server in Ihrer Bereitstellung installieren möchten, können Sie die Installationsoptionen während der Standardinstallation oder benutzerdefinierten Installation in einer Konfigurationsdatei aufzeichnen und anhand dieser Datei eine unbeaufsichtigte Installation ausführen. Weitere Informationen zur automatischen Installation finden Sie unter Abschnitt 12.3, „Ausführen einer automatischen Installation“, auf Seite 73.

9.2 Appliance-Installation

Bei der Appliance-Installation werden sowohl SLES 11 SP3 (64 Bit) als Betriebssystem als auch Sentinel installiert.

Die Sentinel-Appliance steht in den folgenden Formaten zur Verfügung:

- OVF-Appliance-Image
- Hardware-Appliance-Live-DVD-Image, das direkt für einen Hardware-Server bereitgestellt werden kann

Weitere Informationen zur Appliance-Installation finden Sie unter Kapitel 13, „Appliance-Installation“, auf Seite 81.

III Installieren von Sentinel

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

10 Installationsüberblick

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

- **Sentinel-Server-Prozess:** Dies ist die primäre Komponente von Sentinel. 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.
- **Webserver:** Für eine sichere Verbindung zur Weboberfläche von Sentinel wird Jetty als Webserver verwendet.
- **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:** In ihr werden die Sicherheitsintelligenzdaten gespeichert.
- **Collector Manager:** Der Collector-Manager stellt eine flexible Datenerfassungsstelle für Sentinel bereit. Das Sentinel-Installationsprogramm installiert während der Installation standardmäßig einen Collector-Manager.
- **NetFlow Collector-Manager:** Der NetFlow Collector-Manager erfasst Netzwerkablaufdaten (NetFlow, IPFIX usw.) von Netzwerkgeräten wie Routern, Switches und Firewalls. Die Netzwerkablaufdaten beschreiben grundlegende Informationen zu allen Netzwerkverbindungen zwischen den Hosts, beispielsweise die übertragenen Pakete und Byte, so dass Sie das Verhalten einzelner Hosts im gesamten Netzwerk visualisieren können.
- **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 *NetIQ 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

Sentinel weist eine hochgradig skalierbare Architektur auf. Wenn ein großes Ereignisaufkommen erwartet wird, können Komponenten auf mehrere Computer verteilt werden, um die optimale Leistung des Systems zu erzielen. Für Produktionsumgebungen empfiehlt die NetIQ Corporation das

Einrichten einer verteilten Bereitstellung, da hierbei die Datensammlungskomponenten auf einem separaten Computer isoliert werden. Dies ist für die Bewältigung von Spitzenlasten und anderen Anomalien mit größtmöglicher Systemstabilität wichtig. Weitere Informationen finden Sie unter Abschnitt 6.1, „Vorteile von verteilten Bereitstellungen“, auf Seite 39.

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 181.
- ❒ Wenn Sie die lizenzierte Version installieren möchten, geben Sie Ihren Lizenzschlüssel vom NetIQ-Kundenservicezentrum an.
- ❒ Vergewissern Sie sich, dass die in Kapitel 8, „Verwendete Ports“, auf Seite 55 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).
- ❒ **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

12 Herkömmliche Installation

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

12.1 Installationsoptionen

`./install-sentinel --help` zeigt folgende Optionen an:

Optionen	Wert	Beschreibung
--location	Verzeichnis	Angabe eines anderen Verzeichnisses als das Stammverzeichnis (/) zur Installation von Sentinel
-m, --manifest	Dateiname	Angabe einer Produkt-Manifestdatei, die anstelle der Standard-Manifestdatei verwendet werden soll
--no-configure		Gibt an, dass das Produkt nach der Installation nicht konfiguriert werden soll
-n, --no-start		Gibt an, dass Sentinel nach der Installation oder Konfiguration nicht gestartet bzw. nicht neu gestartet werden soll
-r, --recordunattended	Dateiname	Angabe einer Datei zur Aufzeichnung der Parameter für eine unbeaufsichtigte Installation
-u, --unattended	Dateiname	Verwendung der Parameter aus der angegebenen Datei zur unbeaufsichtigten Installation von Sentinel
-h, --help		Zeigt die Optionen für die Installation von Sentinel an
-l, --log-file	Dateiname	Zeichnet Protokollmeldungen in einer Datei auf
--no-banner		Unterdrückt die Anzeige von Banner-Nachrichten
-q, --quiet		Zeigt weniger Meldungen an
-v, --verbose		Zeigt während der Installation alle Meldungen an

12.2 Durchführen der interaktiven Installation

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

- Abschnitt 12.2.1, „Standardinstallation“, auf Seite 70
- Abschnitt 12.2.2, „Angepasste Installation“, auf Seite 71

12.2.1 Standardinstallation

Gehen Sie folgendermaßen vor, um eine Standardinstallation durchzuführen:

1. Laden Sie die Sentinel-Installationsdatei von der NetIQ Downloads-Website herunter:
   - **1a** Wählen Sie im Feld **Product or Technology (Produkt bzw. Technologie)** den Eintrag **SIEM-Sentinel** aus.
   - **1b** Klicken Sie auf **Suchen**.
   - **1c** Klicken Sie in der Spalte mit dem Titel **Download** auf die Schaltfläche zum Herunterladen von **Sentinel Evaluation (Sentinel 7.2-Evaluierung)**.
   - **1d** Klicken Sie auf **proceed to download (weiter zum Herunterladen)** und geben Sie dann Ihren Kundennamen und Ihr Passwort an.
   - **1e** Klicken Sie neben der Installationsversion für Ihre Plattform auf **download (herunterladen)**.
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 Sentinel-Weboberfläche zuzugreifen:

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

<IP_Address_Sentinel_server> ist die IP-Adresse oder der DNS-Name des Sentinel-Servers. „8443“ ist der Standardport für den Sentinel-Server.

12.2.2 Angepasste Installation

Wenn Sie Sentinel mit einer benutzerdefinierten Konfiguration installieren, können Sie den Lizenzschlüssel angeben, das Passwort für verschiedene Benutzer ändern und Werte für die verschiedenen Ports angeben, die zur Interaktion mit internen Komponenten verwendet werden.

1 Laden Sie die Sentinel-Installationsdatei von der NetIQ Downloads-Website herunter:

1a Wählen Sie im Feld **Product or Technology (Produkt bzw. Technologie)** den Eintrag **SIEM-Sentinel** aus.

1b Klicken Sie auf **Suchen**.

1c Klicken Sie in der Spalte mit dem Titel **Download** auf die Schaltfläche zum Herunterladen von **Sentinel 7.2 Evaluation (Sentinel 7.2-Evaluierung)**.

1d Klicken Sie auf **proceed to download (weiter zum Herunterladen)** und geben Sie dann Ihren Kundennamen und Ihr Passwort an.

1e Klicken Sie neben der Installationsversion für Ihre Plattform auf **download (herunterladen)**.

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 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>
```

4 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.

5 Drücken Sie die Leertaste, um die Lizenzvereinbarung durchzulesen.

6 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.

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

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

   Alternativ:

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

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

10 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.

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

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

13 Geben Sie nach dem Ändern der Ports „7“ ein, um den Änderungsvorgang abzuschließen.

14 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`.

15 ***Wenn Sie Sentinel im FIPS 140-2-Modus aktivieren möchten***, drücken Sie `j`.

   15a 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.

   15b 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`.

   15c Konfigurieren Sie den FIPS 140-2-Modus, indem Sie die unter Kapitel 21, „Ausführen von Sentinel im FIPS 140-2-Modus“, auf Seite 113 genannten Aufgaben ausführen.

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 Sentinel-Weboberfläche zuzugreifen:

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

<IP_Address_Sentinel_server> ist die IP-Adresse oder der DNS-Name des Sentinel-Servers. „8443“ ist der Standardport für den Sentinel-Server.

12.3 Ausführen einer automatischen Installation

Die automatische oder unbeaufsichtigte Installation ist nützlich, wenn Sie mehr als einen Sentinel-Server 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. Sie können die Installationsparameter sowohl bei einer Sentinel-Installation mit Standardkonfiguration als auch bei einer Installation mit benutzerdefinierter Konfiguration aufzeichnen.

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 Abschnitt 12.2.1, „Standardinstallation“, auf Seite 70 oder Abschnitt 12.2.2, „Angepasste Installation“, auf Seite 71.

Zur Aktivierung von Sentinel im 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 NetIQ Downloads-Website herunter:
2. Melden Sie sich am Server, auf dem Sentinel installiert werden soll, als `root` an.
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:

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

   Die Installation wird mit den Werten fortgesetzt, die in der Antwortdatei gespeichert sind.
5. **(Bedingt) Wenn Sie den FIPS 140-2-Modus aktivieren möchten,** konfigurieren Sie den FIPS 140-2-Modus, indem Sie die unter Kapitel 21, „Ausführen von Sentinel im FIPS 140-2-Modus“, auf Seite 113 genannten Aufgaben ausführen.

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.

12.4 Installieren von Collector-Managers und Correlation Engines

Standardmäßig installiert Sentinel einen Collector-Manager und eine Correlation Engine. Für Produktionsumgebungen empfiehlt die NetIQ Corporation das Einrichten einer verteilten Bereitstellung, da hierbei die Datensammlungskomponenten 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 Abschnitt 6.1, „Vorteile von verteilten Bereitstellungen“, auf Seite 39.

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.

12.4.1 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.

12.4.2 Installieren von Collector-Managers und Correlation Engines

1. Starten Sie die Sentinel-Weboberfläche, indem Sie in einem Webbrowser folgende URL eingeben:

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

   <IP_Address_Sentinel_server> ist die IP-Adresse oder der DNS-Name des Sentinel-Servers. „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
```

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 der Eingabeaufforderung „1“ an, um mit der Standardkonfiguration fortzufahren.

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

Das Sentinel-Serverzertifikat wird angezeigt.

13 Geben Sie die ActiveMQ-Anmeldedaten für den Collector-Manager oder die Correlation Engine an.

Die ActiveMQ-Anmeldedaten werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

14 Wenn Sie aufgefordert werden, das Zertifikat zu akzeptieren, überprüfen Sie das Zertifikat mit dem folgenden Befehl:

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

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

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

16 Geben Sie `ja` oder `j` ein, um den FIPS 140-2-Modus in Sentinel zu aktivieren, und fahren Sie mit der FIPS-Konfiguration fort.

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

12.4.3 Hinzufügen eines benutzerdefinierten ActiveMQ-Benutzers für den Collector-Manager oder die Correlation Engine

Sentinel empfiehlt die Verwendung der ActiveMQ-Standardbenutzernamen für den Remote-Collector-Manager und die Remote-Correlation Engine. Wenn Sie jedoch mehrere Remote-Collector-Manager-Instanzen installiert haben und sie einzeln identifizieren möchten, können Sie neue ActiveMQ-Benutzer erstellen:

1. Melden Sie sich am Server mit dem Sentinel-Benutzer an, der Zugriff auf die Installationsdateien hat.
2. Öffnen Sie die Datei `activemqgroups.properties`.

   Die Datei befindet sich im Verzeichnis `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/`.
3. Fügen Sie die neuen ActiveMQ-Benutzernamen durch Komma getrennt wie folgt hinzu:

   Fügen Sie die neuen Benutzer für den Collector-Manager im Abschnitt „cm“ hinzu. Beispiel:

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

   Fügen Sie die neuen Benutzer für den Collector-Manager im Abschnitt „admins“ hinzu. Beispiel:

   ```
   admins=system,correlationengine,ceuser1,ceuser2,...
   ```
4. Speichern und schließen Sie die Datei.
5. Öffnen Sie die Datei `activemqusers.properties`.

   Die Datei befindet sich im Verzeichnis `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/`.
6. Fügen Sie das Passwort für den in Schritt 3 erstellten ActiveMQ-Benutzer hinzu.

   Das Passwort kann eine beliebige Zufallszeichenkette sein. Beispiel:

   Für Collector-Manager-Benutzer:

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

   Für Correlation Engine-Benutzer:

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   correlationengine=68790d7a
   ceuser1=69700c6d
   ceuser2=70701b5c
   ```
7. Speichern und schließen Sie die Datei.
8. Starten Sie den Sentinel-Server neu.

12.5 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. NetIQ Corporation unterstützt keine Nicht-Root-Installationen mit einem anderen Benutzer als „novell“, auch wenn die Installation erfolgreich fortgeführt werden kann.

1. Laden Sie die Installationsdateien von der NetIQ 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`
NetFlow Collector-Manager	**Standardstandort:** `./install-netflow`
	Anderer Standort: `./install-netflow --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 Abschnitt 12.2.1, „Standardinstallation“, auf Seite 70 oder Abschnitt 12.2.2, „Angepasste Installation“, auf Seite 71.

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>`
NetFlow Collector-Manager	**Standardstandort:** `./install-netflow -u <Antwortdatei>`
	Anderer Standort: `./install-netflow --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 Abschnitt 12.2.1, „Standardinstallation“, auf Seite 70.
- Wenn Sie die benutzerdefinierte Konfiguration auswählen, fahren Sie fort mit Schritt 7 bis Schritt 14 in Abschnitt 12.2.2, „Angepasste Installation“, auf Seite 71.

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 Sentinel-Weboberfläche zuzugreifen:

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

<IP_Address_Sentinel_server> ist die IP-Adresse oder der DNS-Name des Sentinel-Servers. „8443“ ist der Standardport für den Sentinel-Server.

13 Appliance-Installation

Die Sentinel-Appliance ist eine ausführungsbereite, auf SUSE Studio aufgebaute Software-Appliance. Die Appliance vereint ein verstärktes SLES -Betriebssystem und den in die Sentinel-Software integrierten Aktualisierungsservice. Sie bietet eine einfache und nahtlose Benutzererfahrung und ermöglicht unseren Kunden, vorhandene Investitionen besser zu nutzen. Lesen Sie vor der Installation der Sentinel-Appliance die Versionshinweise des unterstützten SLES, um sich über die neuen Funktionen und bekannten Probleme zu informieren.

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

13.1 Installieren der Sentinel-ISO-Appliance

In diesem Abschnitt wird erklärt, wie Sie Sentinel, Collector-Manager und Correlation Engines 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.

13.1.1 Voraussetzungen

Die Installationsumgebung für die Sentinel-ISO-Appliance muss die folgenden Voraussetzungen erfüllen:

- (Bedingt) Wenn Sie die Sentinel-ISO-Appliance auf Bare-Metal-Hardware installieren, laden Sie sich das ISO-Datenträger-Image der Appliance von der Support-Website herunter, entpacken Sie es und erstellen Sie eine DVD.
- Stellen Sie sicher, dass das System, auf dem Sie das ISO-Datenträger-Image installieren möchten, über mindestens 4,5 GB freien Speicher für die Installation verfügt.
- Vergewissern Sie sich, dass auf der Festplatte mindestens 50 GB freier Speicherplatz zur Verfügung steht, damit das Installationsprogramm einen automatischen Partitionierungsvorschlag erstellen kann.

13.1.2 Installieren von Sentinel

So installieren Sie die Sentinel-ISO-Appliance:

1. Laden Sie das virtuelle ISO-Appliance-Image von der NetIQ-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:

   Kopieren Sie das ISO-Image auf eine DVD, richten Sie die virtuelle Maschine damit ein und schalten Sie sie ein.
3. (Bedingt) Wenn Sie die 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 Führen Sie das Live DVD-Appliance-Image aus, indem Sie das obere Element im Bootmenü auswählen.

   Das Installationsskript prüft zunächst, ob genügend Arbeitsspeicher und Plattenspeicherplatz zur Verfügung stehen. Bei weniger als 2.5 GB verfügbarem Arbeitsspeicher wird die Installation automatisch beendet. Bei mehr als 2.5 GB, jedoch weniger als 6.7 GB Arbeitsspeicher meldet die Installation, dass weniger Arbeitsspeicher als empfohlen zur Verfügung steht. Geben Sie „y“ ein, wenn die Installation fortgesetzt werden soll, und „n“, wenn Sie nicht fortfahren möchten.
4. Wählen Sie die gewünschte Sprache aus und klicken Sie auf **Weiter**.
5. Wählen Sie die Tastaturkonfiguration aus, und klicken Sie auf **Weiter**.
6. Lesen und akzeptieren Sie die SUSE Enterprise Server Software-Lizenzvereinbarung. Klicken Sie auf **Weiter**
7. Lesen und akzeptieren Sie die NetIQ Sentinel-Endbenutzer-Lizenzvereinbarung. Klicken Sie auf **Weiter**
8. Geben Sie auf der Seite für den Hostnamen und den Domänennamen die entsprechenden Namen ein. Deaktivieren Sie die Option **Hostnamen zu Loopback-IP zuweisen**.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie eine der beiden folgenden Optionen für die Verbindungseinstellung aus:
    - Um die aktuellen Netzwerkeinstellungen zu verwenden, wählen Sie auf der Seite „Netzwerkkonfiguration II“ die Option **Folgende Konfiguration verwenden** aus.
    - Um die Netzwerkeinstellungen zu ändern, klicken Sie auf **Ändern**, und nehmen Sie die gewünschten Änderungen vor.
11. Klicken Sie auf **Weiter**.
12. Legen Sie Uhrzeit und Datum fest und klicken Sie auf **Weiter**.

    Zum Ändern der NTP-Konfiguration nach der Installation rufen Sie YaST von der Befehlszeile der Appliance aus auf. Mit WebYast können Sie zwar die Einstellungen für die Uhrzeit und das Datum ändern, nicht jedoch die NTP-Konfiguration.

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

    ```
    rcntp restart
    ```
13. Legen Sie das `root`-Passwort fest und klicken Sie auf **Weiter**.

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

Zur Installation der Appliance auf dem physischen Server muss die Option **Sentinel-Appliance auf der Festplatte installieren (nur für Live DVD-Image)** ausgewählt sein. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Appliance nicht auf dem physischen Server installiert und nur im LIVE-DVD-Modus ausgeführt. Weiter mit Schritt 21.

15 Wählen Sie in der YaST2-Live-Installationsprogrammkonsole **Weiter**.

Die YaST2-Live-Installationsprogrammkonsole installiert die Appliance auf die Festplatte. Die YaST2-Live-Installationsprogrammkonsole wiederholt einen Teil der vorangegangenen Installationsschritte.

16 Im Bildschirm **Suggested Partitioning** (Vorgeschlagene Partitionierung) wird die empfohlene Einrichtung der Partitionen angezeigt. Prüfen Sie die Partitionseinrichtung, konfigurieren Sie die Einrichtung (bei Bedarf), und wählen Sie **Weiter**. Bearbeiten Sie diese Einstellungen nur dann, wenn Sie mit dem Konfigurieren von Partitionen in SLES vertraut sind.

Sie können die Partitionseinrichtung mithilfe der verschiedenen Partitionierungsoptionen auf dem Bildschirm konfigurieren. Weitere Informationen zum Konfigurieren von Partitionen finden Sie unter Using the YaST Partitioner (Verwenden des YaST-Partitionierungsprogramms) in der *SLES-Dokumentation* und unter Abschnitt 6.6, „Planen von Partitionen für die Datenspeicherung“, auf Seite 45.

17 Geben Sie das Root-Passwort ein, und wählen Sie **Weiter**.

18 Im Bildschirm **Live Installation Settings** (Live-Installationseinstellungen) werden die ausgewählten Installationseinstellungen angezeigt. Prüfen Sie die Einstellungen, konfigurieren Sie die Einstellungen (sofern erforderlich), und wählen Sie **Install** (Installieren).

19 Klicken Sie auf **Installieren**, um die Installation zu bestätigen.

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

20 Wählen Sie **OK**. Das System wird neu gebootet.

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

22 Geben Sie den Root-Benutzernamen und das Passwort an der Konsole ein, um sich an der Appliance anzumelden.

Der Standardwert für den Benutzernamen lautet `root`, und das Passwort ist das in Schritt 17 festgelegte Passwort.

23 Fahren Sie mit Abschnitt 13.3, „Konfiguration der Appliance im Anschluss an die Installation“, auf Seite 87 fort.

13.1.3 Installieren von Collector-Managers und Correlation Engines

Die Vorgehensweisen zur Installation von Collector-Manager und Correlation Engine sind gleich und unterscheiden sich nur dadurch, dass Sie die entsprechende ISO-Appliance-Datei von der NetIQ-Download-Website herunterladen müssen.

1. Führen Sie die Schritte 1 bis Schritt 13 aus, die unter Abschnitt 13.1.2, „Installieren von Sentinel“, auf Seite 82 aufgeführt sind.
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`.
   - **Benutzername für den Kommunikationskanal:** Geben Sie den Benutzernamen für den Kommunikationskanal an, der den Collector-Manager- oder Correlation Engine-Benutzernamen darstellt.
   - **Passwort für den Kommunikationskanalbenutzer:** Geben Sie das Passwort für den Kommunikationskanalbenutzer an.

     Die Anmeldedaten für den Kommunikationskanal werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

     Über folgende Zeile in der Datei `activemqusers.properties` können Sie die Anmeldedaten überprüfen:

     Für den Collector-Manager:

     ```
     collectormanager=<password>
     ```

     In diesem Beispiel ist `collectormanager` der Benutzername und der entsprechende Wert ist das Passwort.

     Für die Correlation Engine:

     ```
     correlationengine=<password>
     ```

     In diesem Beispiel ist `correlationengine` der Benutzername und der entsprechende Wert ist das Passwort.
   - **Sentinel-Appliance auf der Festplatte installieren (nur für Live DVD-Image):** Zur Installation der Appliance auf dem physischen Server muss dieses Kontrollkästchen aktiviert werden.

     Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Appliance nicht auf dem physischen Server installiert und nur im Live-DVD-Modus ausgeführt.
3. Klicken Sie auf **Weiter**.
4. Akzeptieren Sie das Zertifikat, wenn Sie dazu aufgefordert werden.
5. Führen Sie Schritt 15 bis Schritt 20 in Abschnitt 13.1.2, „Installieren von Sentinel“, auf Seite 82 aus.
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 22 bis Schritt 23 in Abschnitt 13.1.2, „Installieren von Sentinel“, auf Seite 82 aus.

13.2 Installieren der Sentinel-OVF-Appliance

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 die Sentinel-OVF-Appliance sind zwei Hypervisoren zertifiziert, aber sie kann auch mit anderen Hypervisoren verwendet werden.

13.2.1 Installieren von Sentinel

So installieren Sie die Sentinel-OVF-Appliance:

1 Laden Sie das virtuelle OVF-Appliance-Image von der NetIQ-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 und klicken Sie auf **Weiter**.

6 Wählen Sie das Tastatur-Layout aus und klicken Sie auf **Weiter**.

7 Lesen und akzeptieren Sie die Software-Lizenzvereinbarung für SUSE Linux Enterprise Server (SLES) 11 SP3.

8 Lesen und akzeptieren Sie die NetIQ Sentinel-Endbenutzer-Lizenzvereinbarung.

9 Geben Sie auf der Seite für den Hostnamen und den Domänennamen die entsprechenden Namen ein. Deaktivieren Sie die Option **Hostnamen zu Loopback-IP zuweisen**.

10 Klicken Sie auf **Weiter**. Die Konfigurationen für den Hostnamen werden gespeichert.

11 Wählen Sie eine der beiden folgenden Optionen für die Netzwerkverbindung aus:

- Um die aktuellen Netzwerkverbindungseinstellungen zu verwenden, wählen Sie auf der Seite „Netzwerkkonfiguration II“ die Option **Folgende Konfiguration verwenden** aus und klicken Sie auf **Weiter**.
- Um die Netzwerkeinstellungen zu ändern, wählen Sie **Ändern** aus, nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **Weiter**.

Die Netzwerkeinstellungen werden gespeichert.

12 Legen Sie Uhrzeit und Datum fest und klicken Sie auf **Weiter**.

Zum Ändern der NTP-Konfiguration nach der Installation rufen Sie YaST von der Befehlszeile der Appliance aus auf. Mit WebYast können Sie zwar die Uhrzeit und das Datum ändern, nicht jedoch die NTP-Konfiguration.

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

```
rcntp restart
```

13 Legen Sie das `root`-Passwort fest und klicken Sie auf **Weiter**.

Das Installationsskript prüft, ob genügend Arbeitsspeicher und Plattenspeicherplatz zur Verfügung stehen. Bei weniger als 2.5 GB verfügbarem Arbeitsspeicher wird die Installation nicht fortgeführt. Die Schaltfläche **Weiter** ist in diesem Fall nicht verfügbar.

Bei mehr als 2.5 GB, jedoch weniger als 6.7 GB Arbeitsspeicher meldet die Installation, dass weniger Arbeitsspeicher als empfohlen zur Verfügung steht. Wird diese Meldung angezeigt, klicken Sie auf **Weiter**, um die Installation fortzuführen.

14 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.

15 Notieren Sie sich die IP-Adresse der Appliance, die in der Konsole angezeigt wird. Greifen Sie über diese IP-Adresse auf die Sentinel-Webkonsole zu.

13.2.2 Installieren von Collector-Managers und Correlation Engines

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 10 aus, die unter Abschnitt 13.2.1, „Installieren von Sentinel“, auf Seite 85 aufgeführt sind.

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 ActiveMQ-Benutzernamen an, der den Collector-Manager- oder Correlation Engine-Benutzernamen darstellt. Der Standardbenutzername lautet `collectormanager` für den Collector-Manager und `correlationengine` für die Correlation Engine.

5 Geben Sie das Passwort für den ActiveMQ-Benutzer an.

Die ActiveMQ-Anmeldedaten werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

6 (Optional) Über folgende Zeile in der Datei `activemqusers.properties` können Sie das Passwort überprüfen:

Für den Collector-Manager:

```
collectormanager=<password>
```

In diesem Beispiel ist `collectormanager` der Benutzername und der entsprechende Wert ist das Passwort.

Für die Correlation Engine:

```
correlationengine=<password>
```

In diesem Beispiel ist `correlationengine` der Benutzername und der entsprechende Wert ist das Passwort.

7 Klicken Sie auf **Weiter**.

8 Akzeptieren Sie das Zertifikat.

9 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, der Sentinel-Collector-Manager oder die Sentinel-Correlation Engine ist. Sie zeigt auch die IP-Adresse der Sentinel-Server-Benutzeroberfläche an.

13.3 Konfiguration der Appliance im Anschluss an die Installation

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

13.3.1 Konfigurieren von WebYaST

Die Sentinel-Appliance-Benutzeroberfläche ist mit WebYaSt ausgestattet. WebYaSt ist eine webbasierte Fernkonsole zur Steuerung von Appliances, die auf SUSE Linux Enterprise basieren. Mit WebYaST können Sie auf Sentinel Appliances zugreifen, diese konfigurieren und überwachen. Nachfolgend werden die Schritte zum Konfigurieren von WebYaST kurz beschrieben. Weitere Informationen zur ausführlichen Konfiguration finden Sie im *WebYaST User Guide (Benutzerhandbuch für WebYaST)* (http://www.novell.com/documentation/webyast/).

1 Melden Sie sich an der Sentinel-Appliance an.

2 Klicken Sie auf **Appliance**.

3 Konfigurieren Sie den Sentinel-Server wie in Abschnitt 13.3.3, „Registrieren für Aktualisierungen“, auf Seite 88 beschrieben zum Empfang von Aktualisierungen.

4 Klicken Sie auf **Weiter**, um die Ersteinrichtung fertig zu stellen.

13.3.2 Erstellen von Partitionen

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 Abschnitt 6.6, „Planen von Partitionen für die Datenspeicherung“, auf Seite 45. 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 die Sentinel-Appliance neu zu starten:

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

13.3.3 Registrieren für Aktualisierungen

Sie müssen die Sentinel-Appliance im Appliance-Aktualisierungskanal registrieren, um Patch-Aktualisierungen zu erhalten. Zur Registrierung der Appliance müssen Sie zunächst den Appliance-Registrierungscode oder den Appliance-Aktivierungsschlüssel vom NetIQ-Kundenservicezentrum abrufen.

Gehen Sie folgendermaßen vor, um die Appliance für Aktualisierungen zu registrieren:

1. Melden Sie sich an der Sentinel-Appliance an.
2. Klicken Sie auf **Appliance**, um WebYaST zu starten.
3. Klicken Sie auf **Registrierung**.
4. Geben Sie die Email-Adresse für den Empfang der Aktualisierungen an und geben Sie dann den Systemnamen und den Appliance-Registrierungscode an.
5. Klicken Sie auf **Speichern**.

13.3.4 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 NetIQ Customer Center integriert ist und Kernfunktionen des NetIQ Customer Centers zur Verfügung stellt.

- „Voraussetzungen“, auf Seite 89
- „Konfigurieren der Appliance“, auf Seite 90
- „Aufrüsten der Appliance“, auf Seite 90

Voraussetzungen

- Besorgen Sie die Anmeldedaten für das NetIQ Customer Center, damit Sentinel Aktualisierungen von NetIQ abrufen kann. Weitere Informationen zum Erhalt der Anmeldedaten erhalten Sie vom NetIQ Support.
- Stellen Sie sicher, dass SLES 11 SP3 mit folgenden Paketen auf dem Computer installiert ist, auf dem SMT installiert werden soll:
  - 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

Informationen zur Konfiguration der Appliance mit SMT finden Sie in der Dokumentation Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

Führen Sie folgenden Befehl 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
```

Aufrüsten der Appliance

Informationen zur Aufrüstung der Appliance finden Sie unter Abschnitt 25.3, „Aufrüsten der Appliance mit SMT“, auf Seite 140.

13.4 Stoppen und Starten des Servers mit WebYaST

Sie können den Sentinel-Server folgendermaßen über die Weboberfläche starten und stoppen:

1. Melden Sie sich an der Sentinel-Appliance an.
2. Klicken Sie auf **Appliance**, um WebYaST zu starten.
3. Klicken Sie auf **Systemdienste**.
4. Um den Sentinel-Server zu stoppen, klicken Sie auf **stop** („stoppen“).
5. Um den Sentinel-Server zu starten, klicken Sie auf **start** („starten“).

14 Installation des NetFlow Collector-Managers

Der NetFlow-Collector-Manager muss auf einem separaten Computer installiert werden, nicht auf demselben Computer, auf dem der Sentinel-Server, der Collector-Manager oder eine Correlation Engine installiert ist.

14.1 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).

14.2 Installieren des NetFlow Collector-Managers

Zum Installieren der NetFlow Collector-Manager stehen folgende Methoden zur Auswahl:

- **Standard:** Verwendet die Standardwerte für die NetFlow-Konfiguration.
- **Benutzerdefiniert:** Ermöglicht die Anpassung der Portnummer für den Sentinel-Server.

HINWEIS

- Zum Senden von Netzwerkablaufdaten an den Sentinel-Server müssen Sie als Administrator angemeldet sein, zur Rolle „NetFlow-Anbieter“ gehören oder die Berechtigung „NetFlow-Daten senden“ besitzen.
- Falls mehrere NetFlow Collector-Manager installiert werden sollen, legen Sie je ein neues Benutzerkonto für die einzelnen NetFlow Collector-Manager an, über das die Netzwerkablaufdaten an Sentinel gesendet werden. Wenn Sie verschiedene Benutzerkonten für die NetFlow Collector-Manager nutzen, erhalten Sie zusätzliche Kontrolle darüber, welche NetFlow Collector-Manager Daten an Sentinel senden dürfen.

So installieren Sie den NetFlow Collector-Manager:

1. Starten Sie die Sentinel-Weboberfläche, indem Sie auf der Weboberfläche folgende URL eingeben:

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

   <IP_Address_Sentinel_server> ist die IP-Adresse oder der DNS-Name des Sentinel-Servers. „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 dem Titel „NetFlow Collector-Manager“ auf **Installationsprogramm herunterladen**.

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

5 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.

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

```
cd <directory_name>
```

7 Geben Sie folgenden Befehl ein, um den NetFlow Collector-Manager zu installieren:

```
./install-netflow
```

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

9 Drücken Sie die Leertaste, um die Lizenzvereinbarung durchzulesen.

10 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.

11 Geben Sie an, ob die Standardinstallation oder die benutzerdefinierte Installation durchgeführt werden soll.

12 Geben Sie den Hostnamen oder die IP-Adresse des Sentinel-Servers an, der die Netzwerkablaufdaten empfangen soll.

13 (Bedingt) Bei der benutzerdefinierten Installation geben Sie die Portnummer des Sentinel-Servers an.

Die Standard-Portnummer lautet 8443.

14 Geben Sie den Benutzernamen und das Passwort an, um sich beim Sentinel-Server zu authentifizieren.

HINWEIS: Der angegebene Berechtigungsnachweis muss über die Berechtigung „NetFlow-Daten senden“ oder über Administratorrechte verfügen. Die Installation wird auch sonst ordnungsgemäß abgeschlossen, allerdings tritt dann bei der Authentifizierung ein Fehler auf, wenn der NetFlow Collector-Manager Daten an den Sentinel-Server sendet.

Die Installation wird abgeschlossen. Es kann einige Minuten dauern, bis die Verbindung des NetFlow Collector-Managers zum Sentinel-Server hergestellt ist.

15 (Optional) Sie können erkennen, ob die Installation des NetFlow Collector-Managers erfolgreich war, wenn Sie einen der folgenden Schritte ausführen:

- Überprüfen Sie, ob die NetFlow Collector-Manager-Dienste ausgeführt werden:

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

- Überprüfen Sie, ob der NetFlow Collector-Manager eine Verbindung zum Sentinel-Server hergestellt hat:

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

- Überprüfen Sie, ob der NetFlow Collector-Manager in der Sentinel-Webkonsole aufgeführt wird. Klicken Sie hierzu auf **Sammlung** > **NetFlow**.

16 Aktivieren Sie die Weiterleitung des Netzwerkdatenverkehrs auf dem Gerät, für das die Netzwerkablaufdaten erfasst werden sollen.

Beim Aktivieren von NetFlow auf dem Gerät müssen Sie die IP-Adresse des Sentinel-Servers und den Port, an dem der NetFlow Collector-Manager die Daten vom NetFlow-fähigen Gerät empfangen soll, angeben. Die Standardportnummer lautet 3578. Weitere Informationen hierzu finden Sie in der Dokumentation zum jeweiligen NetFlow-fähigen Gerät.

15 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.

15.1 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. Melden Sie sich unter https://*<IP-Adresse>*:8443 bei der Sentinel-Weboberfläche an. 8443 ist der Standardport für den Sentinel-Server.
3. Klicken Sie in der Symbolleiste auf **Anwendungen** und klicken Sie dann auf **Anwendungen**.
4. Klicken Sie auf **Control Center starten**, um das Sentinel Control Center zu starten.
5. Klicken Sie in der Symbolleiste auf **Ereignisquellenmanagement** > **Live-Ansicht**. Klicken Sie dann auf **Werkzeuge** > **Plugin importieren**.
6. Suchen Sie die Collector-Datei, die Sie in Schritt 1 heruntergeladen haben, und klicken Sie dann auf **Weiter**.
7. 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.

15.2 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. Melden Sie sich unter https://*<IP-Adresse>*:8443 bei der Sentinel-Weboberfläche an. 8443 ist der Standardport für den Sentinel-Server.
3. Klicken Sie in der Symbolleiste auf **Anwendung** und klicken Sie dann auf **Anwendungen**.
4. Klicken Sie auf **Control Center starten**, um das Sentinel Control Center zu starten.
5. Klicken Sie in der Symbolleiste auf **Ereignisquellenmanagement** > **Live-Ansicht**. Klicken Sie dann auf **Werkzeuge** > **Plugin importieren**.
6. Suchen Sie die Connector-Datei, die Sie in Schritt 1 heruntergeladen haben, und klicken Sie dann auf **Weiter**.
7. 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.

16 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-Dienste aktiv sind:

  ```
  /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.

- Greifen Sie auf die Sentinel-Weboberfläche zu:
  1. Rufen Sie einen unterstützten Webbrowser auf:
  2. Geben Sie die URL der Sentinel-Weboberfläche an:

     ```
     https://<IP_Address/DNS_Sentinel_server:8443>
     ```

     „IP_Address/DNS_Sentinel_server“ ist die IP-Adresse oder der DNS-Name des Sentinel-Servers. Der Standardport für den Sentinel-Server lautet 8443.
  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.

17 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.

17.1 Zeit in Sentinel

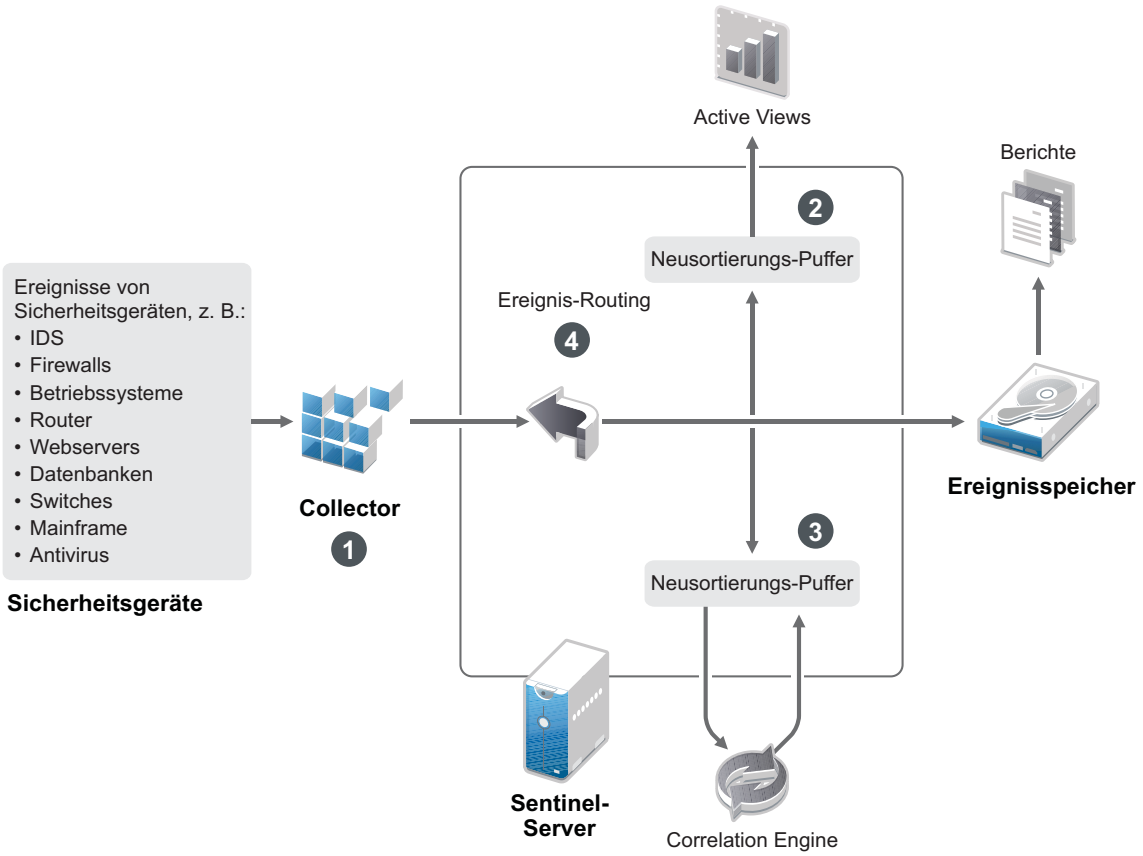
Sentinel ist ein verteiltes System, das aus verschiedenen Prozessen besteht, die im Netzwerk verteilt sind. Zudem kann es durch die Ereignisquelle zu einer gewissen Verzögerung kommen. Aus diesem Grund ordnen die Sentinel-Vorgänge die Ereignisse vor der Verarbeitung nach der Uhrzeit neu an.

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 erläutert, wie Sentinel hierzu vorgeht:

Abbildung 17-1 *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 Active Views verarbeitet. Ereignisse, deren Ereigniszeit mehr als 5 Minuten in der Zukunft liegen, werden in den Active Views nicht angezeigt, jedoch 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, Active Views und Sicherheitsintelligenz.

17.2 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 *NetIQ 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**.

17.3 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>
```

17.4 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 Client dargestellt werden. Über die Details in den ObserverTZ-Feldern kann der Benutzer die Ortszeit der Quelle anzeigen.

18 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 Sentinel-Webkonsole 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 Administratorpasworts, 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`.

19 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.

19.1 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 Sentinel-Weboberfläche an. 8443 ist der Standardport für den Sentinel-Server.
2. Klicken Sie auf **Plugins** > **Katalog**.

19.2 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 *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

19.3 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 „Verwenden von Lösungspaketen“ im *NetIQ 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 Sentinel-Webkonsole 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 *NetIQ Sentinel -Administrationshandbuch*.

19.4 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.

20 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.

20.1 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. Konfigurieren Sie den FIPS 140-2-Modus, indem Sie die unter Kapitel 21, „Ausführen von Sentinel im FIPS 140-2-Modus“, auf Seite 113 genannten Aufgaben ausführen.

20.2 Aktivieren des FIPS 140-2-Modus auf Remote-Collector-Managern und Remote-Correlation Engines

Sie müssen den FIPS 140-2-Modus auf dem Remote-Collector-Manager und der Remote-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 einen Remote-Collector-Manager oder eine Remote-Correlation Engine für den FIPS 140-2-Modus:

1. Melden Sie sich beim Remote-Collector-Manager- oder Remote-Correlation Engine-System 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 Konfigurieren Sie den FIPS 140-2-Modus, indem Sie die unter Kapitel 21, „Ausführen von Sentinel im FIPS 140-2-Modus“, auf Seite 113 genannten Aufgaben ausführen.

21 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.

21.1 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 122.

21.2 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 122.

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>/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 122.

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>/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 122.

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

21.3 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 122.

3 Melden Sie sich bei der Sentinel-Webkonsole als Benutzer in der Administratorrolle an und fahren sie mit der Konfiguration der LDAP-Authentifizierung fort.

Weitere Informationen finden Sie im Abschnitt „Konfigurieren der LDAP-Authentifizierung“ im *NetIQ Sentinel-Verwaltungshandbuch*.

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.

21.4 Aktualisieren der Serverzertifikate in Remote-Collector-Managern und Remote-Correlation Engines

Zur Konfiguration von vorhandenen Remote-Collector-Managern und Remote-Correlation Engines 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-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 dem Remote-Collector-Manager oder der Remote-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 im Remote-Collector-Manager oder der Remote-Correlation Engine:

1 Melden Sie sich beim Computer des Remote-Collector-Manager oder der Remote-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.

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

21.5.1 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 den 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 122.

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 des Remote-Collector-Managers (je nachdem, wo der Connector bereitgestellt ist) als verbürgt betrachten.

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

Speicherort des Remote-Collector-Manager-Zertifikats: `/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.

21.5.2 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 122.

3 Fahren Sie mit der Konfiguration des Connectors fort.

21.5.3 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 122.

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

21.5.4 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 122.

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 des Remote-Collector-Managers (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.

21.5.5 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 122.

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 des Remote-Collector-Managers (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.

---

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 122.

21.5.6 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 einem Remote-Collector-Manager bereitgestellt ist, kopieren Sie die Datei `/etc/opt/novell/sentinel/config/rcm.cer` vom empfangenden Remote-Collector-Manager-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 122.

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.

21.5.7 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 122.

3 Fahren Sie mit der Konfiguration der Integratorinstanz fort.

21.5.8 SMTP Integrator

Der SMTP-Integrator unterstützt FIPS 140-2 ab Version 2011.1r2. Es sind keine Änderungen an der Konfiguration erforderlich.

21.5.9 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 Remote-Collector-Manager im Nicht-FIPS-Modus, um eine Verbindung zum Sentinel-Server herzustellen, der sich im FIPS 140-2-Modus befindet.

Weitere Informationen finden Sie unter Abschnitt 12.4, „Installieren von Collector-Managers und Correlation Engines“, auf Seite 74.

2 Stellen Sie die Nicht-FIPS-Connectors explizit für den Remote-Collector-Manager bereit, der 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 einem Nicht-FIPS-Remote-Collector-Manager, der 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 7.1.

21.6 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 wie üblich bei der Aktivierung des FIPS 140-2-Modus in Sentinel über die Sentinel-Benutzeroberfläche hochladen. Sie müssen die Zertifikate manuell in die FIPS-Keystore-Datenbank importieren.

Für Ereignisquellen, die Connectors verwenden, die für einen Remote-Collector-Manager bereitgestellt wurden, müssen Sie die Zertifikate in der FIPS-Keystore-Datenbank des Remote-Collector-Managers 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 Remote-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 `ja` oder `j` ein, wenn Sie aufgefordert werden, den Sentinel-Server oder Remote-Collector-Manager neu zu starten.

21.7 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.

21.7.1 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-fips2013012419111359034887.tar.gz` lautet, führen Sie den folgenden Befehl aus:

   ```
   ./backup_util.sh -f non-fips2013012419111359034887.tar.gz -m 'restore'
   ```

5. Starten Sie den Sentinel-Server neu.

21.7.2 Zurücksetzen von Remote-Collector-Managern oder Remote-Correlation Engines in den Nicht-FIPS-Modus

Sie können Remote-Collector-Manager oder Remote-Correlation Engines in den Nicht-FIPS-Modus zurücksetzen.

So setzen Sie einen Remote-Collector-Manager oder eine Remote-Correlation Engine in den Nicht-FIPS-Modus zurück:

1. Melden Sie sich beim Remote-Collector-Manager- oder Remote-Correlation Engine-System 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 den Remote-Collector-Manager oder die Remote-Correlation Engine neu.

V Aufrüsten von Sentinel

In diesem Abschnitt finden Sie Informationen zur Aufrüstung von Sentinel und anderen Komponenten.

22 Implementierungs-Checkliste

Überprüfen Sie vor einer Aufrüstung von Sentinel die folgende Checkliste, um eine erfolgreiche Aufrüstung zu gewährleisten:

Tabelle 22-1 *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 mit technischen Informationen zu NetIQ 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

23 Voraussetzungen

23.1 Voraussetzung für Sentinel im FIPS-Modus

Wenn Sie die Java-Version mit JRE 7 Update 45 abgerüstet haben, um Verbindungsprobleme zwischen den Clients und Sentinel wie unter Sentinel 7.2.2 Release Notes – Known Issues (Sentinel 7.2.1-Versionshinweise – Bekannte Probleme) beschrieben zu beheben, muss die unten beschriebene Voraussetzung erfüllt werden.

Wenn in beliebigen Sentinel-Installationsverzeichnissen symbolische Links vorhanden sind, setzt das Sentinel-Installationsprogramm die Aufrüstung nicht fort. Wenn Sie JRE 7 Update 45 herunterladen und installieren, um die Java-Version abzurüsten, enthält der JRE-Ordner einen Unterordner mit dem Namen `man`, der symbolische Links enthält. Sie sollten daher den Ordner `man` löschen, um erfolgreich auf Sentinel 7.3 oder höher aufzurüsten. Wenn Sie jedoch JDK 7 Update 45 statt JRE 7 Update 45 heruntergeladen und installiert haben, enthält der Ordner `man` keine symbolischen Links und muss nicht gelöscht werden.

So löschen Sie den man-Ordner:

1. Melden Sie sich beim Sentinel-Server als der Benutzer „novell“ an.
2. Geben Sie den folgenden Befehl ein, um das Verzeichnis zu ändern:

   ```
   cd /opt/novell/sentinel/jre/
   ```

3. Löschen Sie den Ordner `man`:

   ```
   rm -rf man
   ```

23.2 Voraussetzung für Versionen unter Sentinel 7.1.1

Sentinel 7.1.1 und höher umfasst MongoDB Version 2.4.1. Für MongoDB 2.4 müssen doppelte Benutzernamen aus der Datenbank entfernt werden. Wenn Sie eine Sentinel-Version unter 7.1.1 aufrüsten, überprüfen Sie, ob doppelte Benutzer vorhanden sind. Wenn doppelte Benutzer vorhanden sind, entfernen Sie diese.

So ermitteln Sie doppelte Benutzer:

1. Melden Sie sich beim Sentinel-Server (Sentinel 7.1 oder früher) als der Benutzer novell an.
2. Wechseln Sie zu folgendem Verzeichnis:

   ```
   cd opt/novell/sentinel/3rdparty/mongodb/bin
   ```

3. Führen Sie die folgenden Befehle zur Überprüfung auf doppelte Benutzer aus:

   ```
   ./mongo --port 27017 --host "localhost"
   use analytics
   ```

```
db.system.users.find().count()
```

Ist die `Anzahl` größer als 1, so sind doppelte Benutzer vorhanden.

So entfernen Sie doppelte Benutzer:

1. Führen Sie den folgenden Befehl aus, um die Benutzer aufzulisten:

   ```
   db.system.users.find().pretty()
   ```

   Der Befehl gibt eine Liste der Benutzer zusammen mit den doppelten Einträgen zurück. Der erste Benutzer in dieser Liste ist der ursprüngliche Benutzer. Behalten Sie den ersten Benutzer bei, und löschen Sie die anderen Benutzer aus der Liste.

2. Führen Sie den folgenden Befehl aus, um doppelte Benutzer zu entfernen:

   ```
   db.system.users.remove({ _id : ObjectId("object_ID") })
   ```

3. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die doppelten Benutzer entfernt wurden:

   ```
   db.system.users.find().pretty()
   ```

4. Wechseln Sie zum Datenbank-Admin-Benutzer:

   ```
   use admin
   ```

5. Wiederholen Sie Schritt 1 bis Schritt 3, und suchen und entfernen Sie doppelte `dbausers` aus der Admin-Datenbank.

24 Aufrüsten einer herkömmlichen Sentinel-Installation

24.1 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 *NetIQ 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 unter „Maintaining Custom Settings in XML Files“ (Pflegen benutzerdefinierter Einstellungen in XML-Dateien) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

3. Laden Sie das aktuellste Installationsprogramm von der NetIQ-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 `ja` oder `j` 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 sehen zu können.

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 (Bedingt) Wenn Sie von Sentinel 7.1.1 oder einer früheren Version aufrüsten, migriert das Installationsprogramm nicht standardmäßig die Sicherheitsintelligenzdaten. Um Sicherheitsintelligenzdaten von Sentinel 7.1.1 oder einer früheren Version zu migrieren, aktivieren Sie manuell die Migration der Sicherheitsintelligenzdaten. Gehen Sie dazu folgendermaßen vor:

   14a Wechseln Sie zum novell-Benutzer.

   ```
   su novell
   ```

   14b Öffnen Sie die Datei `/etc/opt/novell/sentinel/config/server.xml`.

   14c Fügen Sie im Komponentenabschnitt `BaseliningRuntime` die folgende Eigenschaft hinzu:

   ```
   <property name="baselining.migration.check">true</property>
   ```

   14d Starten Sie den Sentinel-Server neu.

15 Informationen zur Aufrüstung von Collector-Manager- und Correlation Engine-Systemen finden Sie unter Abschnitt 24.3, „Aufrüsten des Collector-Managers oder der Correlation Engine“, auf Seite 134.

24.2 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 *NetIQ 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 unter „Maintaining Custom Settings in XML Files“ (Pflegen benutzerdefinierter Einstellungen in XML-Dateien) im *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

3 Laden Sie die Installationsdateien von der NetIQ-Download-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 `ja` oder `j` 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 sehen zu können.

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 von Sentinel 7.1.1 oder einer früheren Version aufrüsten, migriert das Installationsprogramm nicht standardmäßig die Sicherheitsintelligenzdaten. Um Sicherheitsintelligenzdaten von Sentinel 7.1.1 oder einer früheren Version zu migrieren, aktivieren Sie manuell die Migration der Sicherheitsintelligenzdaten. Gehen Sie dazu folgendermaßen vor:

16a Wechseln Sie zum novell-Benutzer.

```
su novell
```

16b Öffnen Sie die Datei `/etc/opt/novell/sentinel/config/server.xml`.

16c Fügen Sie im Komponentenabschnitt `BaseliningRuntime` die folgende Eigenschaft hinzu:

```
<property name="baselining.migration.check">true</property>
```

16d Starten Sie den Sentinel-Server neu.

24.3 Aufrüsten des Collector-Managers oder der 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 *NetIQ Sentinel -Administrationshandbuch*.

2 Melden Sie sich an der Sentinel-Weboberfläche als Benutzer mit Administratorrolle an.

3 Wählen Sie **Downloads** aus.

4 Klicken Sie im Abschnitt zum Collector-Manager-Installationsprogramm auf **Download Installer (Installationsprogramm herunterladen)**.

Es wird ein Fenster mit der Option angezeigt, die Installationsprogrammdatei entweder zu öffnen oder auf dem lokalen Computer zu speichern.

5 Speichern Sie die Datei.

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.

25 Aufrüsten der Sentinel-Appliance

Die Prozeduren in diesem Kapitel führen Sie durch die Aufrüstung der Sentinel-Appliance und der Collector-Manager- und Correlation Engine-Appliances.

25.1 Aufrüsten der Appliance mit zypper

So rüsten Sie die Appliance mit dem Zypper-Patch auf:

1. Sichern Sie die Konfiguration, und erstellen Sie einen ESM-Export. Weitere Informationen finden Sie im Abschnitt „Sichern und Wiederherstellen von Daten“ im *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 unter „Maintaining Custom Settings in XML Files“ (Pflegen benutzerdefinierter Einstellungen in XML-Dateien) im *NetIQ Sentinel Administration Guide* (NetIQ 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 Sie von Sentinel 7.0.1 oder einer früheren Version aufrüsten, geben Sie `1` ein, um den Herstellerwechsel von Novell zu NetIQ zu akzeptieren.
6. (Bedingt) Wenn Sie von einer Sentinel-Version unter 7.2 aufrüsten, zeigt das Installationsprogramm eine Meldung mit der Aufforderung an, die Abhängigkeit für bestimmte Appliance-Pakete aufzulösen. Geben Sie `1` ein, um abhängige Pakete zu deinstallieren.
7. Klicken Sie auf `J`, um fortzufahren.
8. Geben Sie `Ja` ein, um die Lizenzvereinbarung zu akzeptieren.
9. Starten Sie die Sentinel-Appliance neu.
10. Löschen Sie den Webbrowser-Cache, um die neueste Version von Sentinel sehen zu können.
11. 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.

12 (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.

12a Wechseln Sie zum novell-Benutzer.

```
su novell
```

12b Wechseln Sie zum Ordner `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

12c Löschen Sie mit folgendem Befehl alle alten PostgreSQL-Dateien:

```
./delete_old_cluster.sh
```

13 (Bedingt) Wenn Sie von Sentinel 7.1.1 oder einer früheren Version aufrüsten, migriert das Installationsprogramm nicht standardmäßig die Sicherheitsintelligenzdaten. Um Sicherheitsintelligenzdaten von Sentinel 7.1.1 oder einer früheren Version zu migrieren, aktivieren Sie manuell die Migration der Sicherheitsintelligenzdaten. Gehen Sie dazu folgendermaßen vor:

13a Wechseln Sie zum novell-Benutzer.

```
su novell
```

13b Öffnen Sie die Datei `/etc/opt/novell/sentinel/config/server.xml`.

13c Fügen Sie im Komponentenabschnitt `BaseliningRuntime` die folgende Eigenschaft hinzu:

```
<property name="baselining.migration.check">true</property>
```

13d Starten Sie den Sentinel-Server neu.

HINWEIS: Befolgen Sie zum Aufrüsten des Collector-Managers oder der Correlation Engine Schritt 3 bis Schritt 9.

25.2 Aufrüsten der Appliance über WebYaST

HINWEIS: Appliance-Aufrüstungen von Versionen unter Sentinel 7.2 müssen mit dem zypper-Befehlszeilenprogramm ausgeführt werden, weil zum Abschließen der Aufrüstung eine Benutzerinteraktion erforderlich ist. In WebYaST ist die hierfür erforderliche Benutzerinteraktion nicht möglich. Informationen zur Verwendung von zypper für die Aufrüstung der Appliance finden Sie unter Abschnitt 25.1, „Aufrüsten der Appliance mit zypper“, auf Seite 137..

---

1 Melden Sie sich an der Sentinel-Appliance als Benutzer mit Verwalterfunktion an.

2 Sichern Sie die Konfiguration, und erstellen Sie einen ESM-Export. Weitere Informationen finden Sie im Abschnitt „Sichern und Wiederherstellen von Daten“ im *NetIQ 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 *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

4 **Wenn Sie die Sentinel-Appliance aufrüsten möchten**, klicken Sie auf **Appliance**, um WebYaST zu starten.

5 **Wenn Sie eine Collector-Manager- oder Correlation Engine-Appliance aufrüsten möchten**, geben Sie die URL des Collector-Manager- bzw. Correlation Engine-Computers mit Port 4984 an, um WebYaST zu starten (`https://<IP-Adresse>:4984`, wobei `<IP-Adresse>` die IP-Adresse des Collector-Managers bzw. der Correlation Engine darstellt). Führen Sie Schritt 7 bis Schritt 10 aus.

6 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 *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

7 (Bedingt) Wenn Sie die Appliance noch nicht für automatische Aktualisierungen registriert haben, registrieren Sie sie jetzt.

   Weitere Informationen finden Sie unter Abschnitt 13.3.3, „Registrieren für Aktualisierungen“, auf Seite 88.

   Wenn die Appliance nicht registriert ist, zeigt Sentinel eine gelbe Warnmeldung in Bezug auf diesen Zustand an.

8 Klicken Sie auf **Aktualisieren**, um zu überprüfen, ob Aktualisierungen vorhanden sind.

   Die verfügbaren Aktualisierungen werden angezeigt.

9 Wählen Sie die Aktualisierungen aus und wenden Sie sie an.

   Das Abschließen der Aktualisierungen kann einige Minuten in Anspruch nehmen. Nach der erfolgreichen Aktualisierung wird die WebYaST-Anmeldeseite angezeigt.

   For dem Aufrüsten der Appliance stoppt WebYaST automatisch den Sentinel-Service. Nach dem Abschluss der Aufrüstung müssen Sie diesen Service manuell neu starten.

10 Starten Sie den Sentinel-Service über die Weboberfläche neu.

   Weitere Informationen finden Sie unter Abschnitt 13.4, „Stoppen und Starten des Servers mit WebYaST“, auf Seite 90.

11 Löschen Sie den Webbrowser-Cache, um die neueste Version von Sentinel sehen zu können.

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 novell-Benutzer.

   ```
   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 (Bedingt) Wenn Sie von Sentinel 7.1.1 oder einer früheren Version aufrüsten, migriert das Installationsprogramm nicht standardmäßig die Sicherheitsintelligenzdaten. Um Sicherheitsintelligenzdaten von Sentinel 7.1.1 oder einer früheren Version zu migrieren, aktivieren Sie manuell die Migration der Sicherheitsintelligenzdaten. Gehen Sie dazu folgendermaßen vor:

14a Wechseln Sie zum Benutzer „novell“:

```
su novell
```

14b Öffnen Sie die Datei `/etc/opt/novell/sentinel/config/server.xml`.

14c Fügen Sie im Komponentenabschnitt `BaseliningRuntime` die folgende Eigenschaft hinzu:

```
<property name="baselining.migration.check">true</property>
```

14d Starten Sie den Sentinel-Server neu.

25.3 Aufrüsten der Appliance mit 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 Abschnitt 13.3.4, „Konfigurieren der Appliance mit SMT“, auf Seite 89.

2 Sichern Sie die Konfiguration, und erstellen Sie einen ESM-Export. Weitere Informationen finden Sie im Abschnitt „Sichern und Wiederherstellen von Daten“ im *NetIQ 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 *NetIQ Sentinel Administration Guide* (NetIQ 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
```

26 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 Bereitstellen von Sentinel für Hochverfügbarkeitssysteme

Dieser Anhang unterstützt Sie bei der Installation von NetIQ Sentinel in einem Aktiv-Passiv-Hochverfügbarkeitsmodus, bei dem Sentinel ein Failover in einen redundanten Clusterknoten durchführen kann, falls Hardware- oder Softwarefehler auftreten. Wenden Sie sich an den NetIQ-Support, 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 Engines können jedoch weiter mit dem Sentinel-Hochverfügbarkeitsserver kommunizieren.

---

27 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.

27.1 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).

27.2 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.

HINWEIS: 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.

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.

27.3 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.

27.4 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.

28 Systemanforderungen

Bei der Zuweisung von Cluster-Ressourcen zur Unterstützung einer Hochverfügbarkeitsinstallation sind die folgenden Anforderungen zu erfüllen:

- ❒ **(Bedingt) Bei Hochverfügbarkeits-Appliance-Installationen** muss die Sentinel-Hochverfügbarkeits-Appliance mit einer gültigen Lizenz verfügbar sein. Die Sentinel-Hochverfügbarkeits-Appliance ist eine ISO-Appliance mit den folgenden Paketen:
  - Betriebssystem SUSE Linux Enterprise Server (SLES) 11 SP3
  - SUSE Linux Enterprise Server High Availability Extension (SLES HAE)-Paket
  - Sentinel-Software (mit Hochverfügbarkeits-RPM)
- ❒ **(Bedingt) Vergewissern Sie sich bei herkömmlichen Hochverfügbarkeits-Installationen, dass das Sentinel-Installationsprogramm (TAR-Datei) und das ISO-Abbild der SUSE Linux High Availability Extension (SLE HAE) mit gültigen Lizenzen verfügbar sind.**
- ❒ **(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:

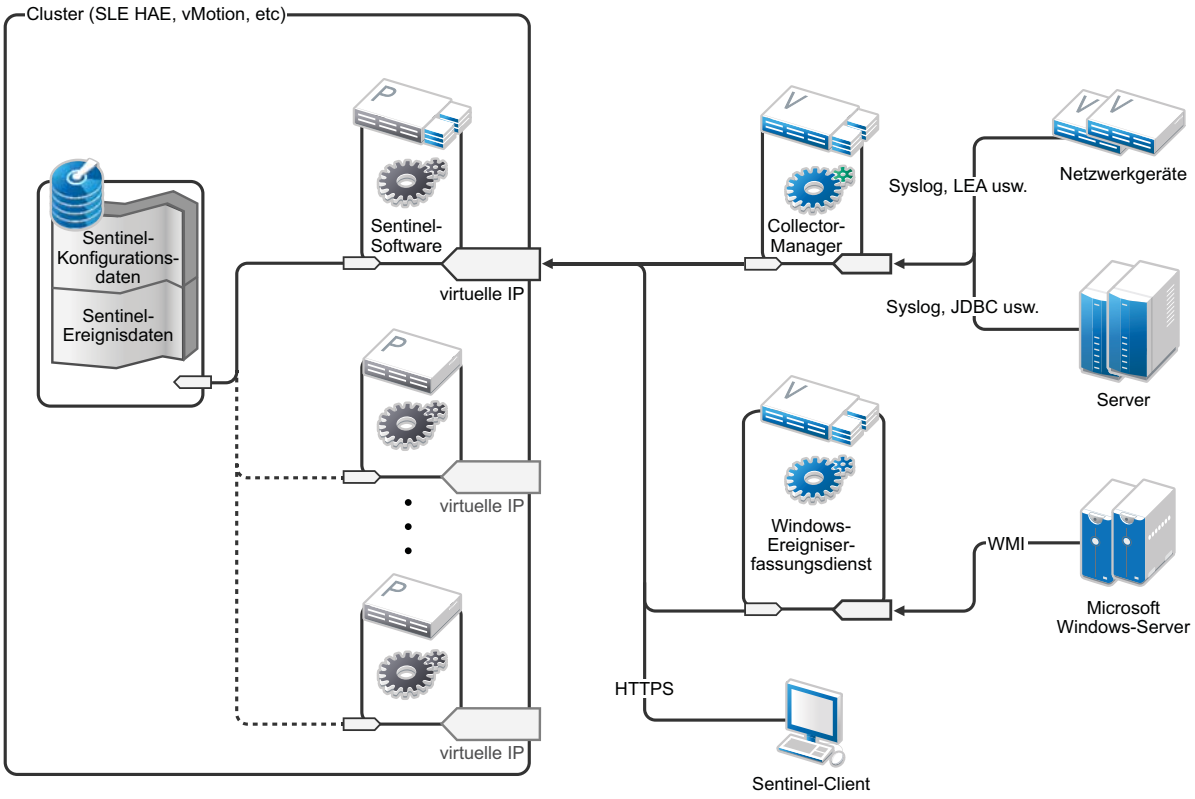
     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```
- ❒ Vergewissern Sie sich, dass jeder Clusterknoten, auf dem Sentinel-Services gehostet werden, die in Kapitel 5, „Erfüllen der Systemanforderungen“, auf Seite 37 angegebenen Anforderungen erfüllt.
- ❒ Stellen Sie sicher, dass 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. NetIQ empfiehlt eine mit iSCSI-Zielen konfigurierte SUSE Linux-Standard-VM als freigegebenen Speicher.
- ❒ Stellen Sie sicher, dass mindestens zwei Clusterknoten vorhanden sind, die die Ressourcenanforderungen zum Ausführen von Sentinel in einer Kundenumgebung erfüllen. NetIQ empfiehlt zwei SUSE Linux-VMs.
- ❒ Stellen Sie sicher, dass Sie eine Methode der Kommunikation zwischen den Clusterknoten und dem freigegebenen Speicher erstellen, beispielsweise FibreChannel für ein SAN. NetIQ empfiehlt die Verwendung einer dedizierten IP-Adresse für die Verbindung zum iSCSI-Ziel.

- ❒ Stellen Sie sicher, dass eine virtuelle IP 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. NetIQ empfiehlt eine einfache Unicast-IP-Adresse, für Produktionsumgebungen wird jedoch Multicast bevorzugt.

29 Installation und Konfiguration

In diesem Abschnitt finden Sie die Vorgehensweise zur Installation und Konfiguration von Sentinel in einer Hochverfügbarkeitsumgebung.

Im folgenden Diagramm ist eine Aktiv-Passiv-HA-Architektur dargestellt:



29.1 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 55.
❑	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.

NetIQ empfiehlt folgende Konfiguration:

- **(Bedingt) Bei herkömmlichen Hochverfügbarkeits-Installationen:**
  - Zwei virtuelle Computer mit SUSE Linux 11 SP3-Clusterknoten.
  - (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 der Basis der Hochverfügbarkeits-ISO-Appliance. Weitere Informationen zum Installieren der Hochverfügbarkeits-ISO-Appliance finden Sie unter Abschnitt 13.1.2, „Installieren von Sentinel“, auf Seite 82.
- 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. Sehen Sie sich die SUSE Linux- und SLE HAE-Systemanforderungen sowie die Sentinel-Anwendungsanforderungen an.
- Einen virtuellen Computer mit SUSE Linux 11 SP3, der mit iSCSI-Zielen für den 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. Sehen Sie sich die Systemanforderungen für SUSE Linux sowie die Anforderungen für den Sentinel-Ereignisdatenspeicher an.

HINWEIS: In einem Produktionscluster können Sie interne, nicht weiterleitbare IPs auf verschiedenen NICs (möglicherweise zwei, aus Redundanzgründen) für die interne Clusterkommunikation verwenden.

29.2 Einrichtung des freigegebenen Speichers

Richten Sie Ihren freigegebenen Speicher ein und vergewissern Sie sich, dass Sie ihn auf 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.

Beispiel für die Einrichtung eines freigegebenen Speichers

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: NetIQ empfiehlt, den freigegebenen Speicher zu konfigurieren und probehalber an jedem Clusterknoten einzuhängen. Die Clusterkonfiguration übernimmt dann jedoch das eigentliche Einhängen des Speichers.

NetIQ empfiehlt folgende Prozedur zum Erstellen von iSCSI-Zielen mit einer SUSE Linux-VM als Host:

1. Stellen Sie eine Verbindung zu `storage03` (der im Schritt Das System einrichten erstellten VM) her und starten Sie eine Konsolensitzung.
2. Erstellen Sie mit dem Befehl `dd` eine leere Datei jeder beliebigen Größe für den Sentinel-Primärspeicher:

   ```
   dd if=/dev/zero of=/localdata count=10240000 bs=1024
   ```

3. Erstellen Sie eine mit Nullen gefüllte, 10 GB große Datei durch Kopieren der Datei `/dev/zero pseudo-device`. Informationen zu den Befehlszeilenoptionen finden Sie auf der Informations- oder Hauptseite für den Befehl `dd`.
4. Wiederholen Sie Schritte 1 bis 3, um eine Datei für den Sekundärspeicher zu erstellen:

   ```
   dd if=/dev/zero of=/networkdata count=10240000 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.

29.2.1 Konfigurieren von iSCSI-Zielen

Konfigurieren Sie die Dateien `localdata` und `networkdata` als iSCSI-Ziele:

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 10.0.0.3 zu. Dies ist die IP für die interne iSCSI-Kommunikation.
6. Klicken Sie auf **Weiter** und anschließend auf **OK**.
7. Wählen Sie am Hauptbildschirm die Optionen **Netzwerkdienste** > **iSCSI-Ziel** aus.
8. Installieren Sie nach Aufforderung die erforderliche Software (`iscsitarget RPM`) vom SUSE Linux 11 SP3-Medium.
9. Klicken Sie auf **Dienst** und wählen Sie die Option **Beim Booten** aus, um sicherzustellen, dass der Dienst beim Booten des Betriebssystems gestartet wird.
10. Klicken Sie auf **Global** und wählen Sie anschließend **Keine Authentifizierung** aus, weil der aktuelle OCF Resource Agent für iSCSI keine Authentifizierung unterstützt.
11. 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.
12. Klicken Sie auf **Hinzufügen**, um ein neues LUN hinzuzufügen.
13. 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`.

14 Wiederholen Sie die Schritte 12 und 13 und fügen Sie diesmal LUN 1 und `/networkdata` hinzu.

15 Behalten Sie für die anderen Optionen die Standardwerte bei. Klicken Sie auf **OK** und anschließend auf **Weiter**.

16 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.

17 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.

29.2.2 Konfigurieren von iSCSI-Initiatoren

Formatieren Sie die Geräte mit folgender Prozedur:

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**, 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 nach Aufforderung die erforderliche Software (open-iscsi RPM) vom SUSE Linux 11 SP3-Medium.

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 iSCSI-Ziel-IP-Adresse (10.0.0.3) an, wählen Sie **Keine Authentifizierung** aus und klicken Sie anschließend 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 Wechseln Sie im Dropdown-Menü **Start** zu „Automatisch“, wählen Sie **Keine Authentifizierung** aus und klicken Sie anschließend 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 Systemanzeige sollten Sie nun in der Liste neue Festplatten sehen (wie `/dev/sdb` und `/dev/sdc`) mit dem Typ IET-VIRTUAL-DISK. 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 ext3-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. Angenommen Sie erstellen eine einzige große Partition auf diesem freigegebenen iSCSI-LUN, dann sollten Sie eine `/dev/sdb1` erhalten oder eine ähnliche formatierte Festplatte (weiter unten 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 Implementation):

```
# 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 5 jeweils durch eine andere IP-Adresse für jeden Clusterknoten.

29.3 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.

NetIQ empfiehlt, Sentinel auf jedem Clusterknoten zu installieren, 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.

29.3.1 Erste Installation im Knoten

- „Herkömmliche Hochverfügbarkeits-Installation“, auf Seite 159
- „Sentinel-Hochverfügbarkeits-Appliance-Installation“, auf Seite 159

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 folgende Befehle 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
   ```

4. Führen Sie eine Standardinstallation aus und konfigurieren Sie das Produkt entsprechend. Das Installationsprogramm installiert die Binärdaten, Datenbanken und Konfigurationsdateien. Außerdem richtet das Installationsprogramm die Anmeldeberechtigung, die Konfigurationseinstellungen und die Netzwerkanschlüsse ein.
5. Starten Sie Sentinel und prüfen Sie die Basisfunktionen. Sie können die standardmäßige externe Clusterknoten-IP 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
   ```

Sentinel-Hochverfügbarkeits-Appliance-Installation

Die Sentinel-Hochverfügbarkeits-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** Geben Sie die Option für den gewünschten Sentinel-Konfigurationstyp an.

3c Geben Sie `2` an, und geben Sie ein neues Passwort ein.

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/sentinel /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/
```

29.3.2 Nachfolgende Installation im Knoten

- „Herkömmliche Hochverfügbarkeits-Installation“, auf Seite 160
- „Sentinel-Hochverfügbarkeits-Appliance-Installation“, auf Seite 161

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
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props
cd /
insserv -r sentinel
```

Sentinel-Hochverfügbarkeits-Appliance-Installation

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/sentinel
   ```

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.

29.4 Clusterinstallation

Installieren Sie die Clustersoftware nur für herkömmliche Hochverfügbarkeitsinstallationen. Die Sentinel-Hochverfügbarkeits-Appliance umfasst die Cluster-Software und erfordert keine manuelle Installation.

NetIQ empfiehlt folgende Prozedur für die Einrichtung der SUSE Linux-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
```

29.5 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.

NetIQ empfiehlt 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 Maschine mit SUSE Linux konfiguriert ist, auf der auch der freigegebene Speicher gehostet wird, um als SBD-Gerät (Systemspaltungsdetektor) für Fencing-Zwecke zu dienen.

SBD-Einrichtung

1 Stellen Sie eine Verbindung zu `storage03` her und starten Sie eine Konsolensitzung. Erstellen Sie mit dem Befehl `dd` eine leere Datei von beliebiger Größe:

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```

2 Erstellen Sie eine mit Nullen gefüllte, 1 MB große Datei durch Kopieren der Datei `/dev/zero` pseudo-device.

3 Führen Sie YaST von der Befehlszeile oder der grafischen Benutzeroberfläche aus: `/sbin/yast`

4 Wählen Sie **Netzwerkdienste** > **iSCSI-Ziel** aus.

5 Klicken Sie auf **Ziele** und wählen Sie das vorhandene Ziel aus.

6 Wählen Sie **Bearbeiten** aus. Auf der Benutzeroberfläche wird eine Liste von verfügbaren LUNs (Laufwerken) angezeigt.

7 Wählen Sie **Hinzufügen** aus, um ein neues LUN hinzuzufügen.

8 Belassen Sie die LUN-Nummer bei 2. Durchsuchen Sie das Dialogfeld **Pfad** und wählen Sie die Datei `/sbd` aus, die Sie erstellt haben.

9 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.

10 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 und deren Hostname 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 Optionen **automatisch** und **Keine Authentifizierung** aktiviert).
6. Wählen Sie **OK** aus, um das iSCSI-Inititor-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. Führen Sie den Befehl `sleha-init` aus.
11. Wenn Sie aufgefordert werden, die Netzwerkadresse für die Verknüpfung 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 „j“ 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. Beenden Sie den Assistenten und vergewissern Sie sich, dass keine Fehler gemeldet wurden.
15. Starten Sie YaST.
16. Wählen Sie **Hochverfügbarkeit** > **Cluster** aus (oder bei einigen Systemen nur „Cluster“).
17. Vergewissern Sie sich, dass im Feld auf der linken Seite die Option **Kommunikationskanäle** ausgewählt ist.
18. 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).
19. 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.
20. Wählen Sie zum Beenden der Konfiguration **Fertig stellen** aus.
21. Beenden Sie YaST.
22. 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 Optionen **automatisch** und **Keine Authentifizierung** aktiviert).
6. Wählen Sie **OK** aus, um das iSCSI-Inititor-Werkzeug zu beenden.
7. Führen Sie den folgenden Befehl aus: `sleha-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. Kopieren Sie `/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 auf `node02` einrichten.
2. Führen Sie `/etc/rc.d/openais start im node02 aus`.

   (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 Skripts`leha-join` erneut aus.
3. 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`.

29.6 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 Dienste zugegriffen wird.
- Die PostgreSQL-Datenbanksoftware, die Konfigurations- und Ereignis-Metadaten speichert.

NetIQ empfiehlt für die Ressourcenkonfiguration Folgendes:

NetIQ stellt das Skript `crm` bereit, um die Clusterkonfiguration zu unterstützen. 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) Bei den neuen Ressourcen, die im Cluster auftauchen, könnten Probleme auftreten. Führen Sie `/etc/rc.d/openais restart` in node02 aus, wenn Sie ein Problem feststellen.
4. Das Skript `install-resources.sh` fordert Sie auf, einige Werte einzugeben, nämlich die virtuelle IP, 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 NetIQ 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.

29.7 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 Sentinel-Webkonsole auf **Speicher**.

2 Wählen Sie **Konfiguration** aus.

3 Wählen Sie eines der Optionsfelder unter „Sekundärspeicher nicht konfiguriert“ aus.

NetIQ empfiehlt, ein einfaches iSCSI-Ziel als freigegebenen Netzwerkspeicherort zu verwenden, 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: Da NetIQ ein iSCSI-Ziel für diese Lösung empfiehlt, wird das Ziel als Verzeichnis eingehängt, das als Sekundärspeicher verwendet wird. 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 die Webkonsole 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 Sentinel-Weboberfläche 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`.

NetIQ empfiehlt die Verwendung einfacher Versionen der erforderlichen Ressourcen, wie den einfachen Resource Agent für das Dateisystem. Kunden können komplexere Clusterressourcen wie cLVM (eine Version des logischen Volumes des Dateisystems) verwenden, falls sie es wünschen.

30 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.

30.1 Voraussetzungen

- Laden Sie das aktuellste Installationsprogramm von der NetIQ-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 <watchdog driver name>
     ```

  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 <watchdog driver name>
     ```

30.2 Aufrüsten einer herkömmlichen 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 die Ressourcen zugreifbar bleiben, und wird die Umgrenzung der Knoten 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 <install_filename>
```

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 *NetIQ Sentinel Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.

4b Stoppen Sie den Clusterstapel:

```
rcopenais stop
```

Durch Stoppen des Clusterstapels wird sichergestellt, dass die Ressourcen zugreifbar bleiben, und wird die Umgrenzung der Knoten 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 <install_filename>
```

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:

```
run 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
```

30.3 Aufrüsten einer Sentinel-Hochverfügbarkeits-Appliance-Installation

Sie können eine Sentinel-Hochverfügbarkeits-Appliance-Installation mit dem zypper-Patch und über WebYaST aufrüsten.

- Abschnitt 30.3.1, „Aufrüsten einer Sentinel-Hochverfügbarkeits-Appliance-Installation mit zypper“, auf Seite 171
- Abschnitt 30.3.2, „Aufrüsten einer Sentinel-Hochverfügbarkeits-Appliance-Installation über WebYaST“, auf Seite 173

30.3.1 Aufrüsten einer Sentinel-Hochverfügbarkeits-Appliance-Installation mit zypper

Vor dem Aufrüsten müssen Sie alle Appliance-Knoten über WebYast registrieren. Weitere Informationen finden Sie unter Abschnitt 13.3.3, „Registrieren für Aktualisierungen“, auf Seite 88. 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 Laden Sie die Aufrüstungen für die Sentinel-Hochverfügbarkeits-Appliance herunter.

```
zypper -v patch -d
```

Mit diesem Befehl werden die Aufrüstungen für die auf der Appliance installierten Pakete (auch Sentinel) in `/var/cache/zypp/packages` heruntergeladen.

3b Stoppen Sie den Clusterstapel.

```
rcopenais stop
```

Durch Stoppen des Clusterstapels wird sichergestellt, dass die Ressourcen zugreifbar bleiben, und wird die Umgrenzung der Knoten verhindert.

3c Nach dem Herunterladen der Aufrüstungen installieren Sie sie mit dem folgenden Befehl:

```
rpm -Uvh /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/rpm/
noarch/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/
rpm/x86_64/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-
Updates/rpm/i586/*.rpm --excludepath=/var/opt/novell/
```

3d Zum Abschluss des Aufrüstungsvorgangs führen Sie das folgende Skript aus:

```
/var/adm/update-scripts/sentinel_server_ha_x86_64-update-<version>-
overlay_files.sh
```

3e Starten Sie nach dem Abschluss der Aufrüstung den Clusterstapel neu.

```
rcopenais start
```

Wiederholen Sie Schritt 3 für alle passiven Clusterknoten.

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 *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

4b Stoppen Sie den Clusterstapel.

```
rcopenais stop
```

Durch Stoppen des Clusterstapels wird sichergestellt, dass die Ressourcen zugreifbar bleiben, und wird die Umgrenzung der Knoten verhindert.

4c Melden Sie sich als Administrator bei der Sentinel-Appliance an.

4d Zum Aufrüsten der Sentinel-Appliance klicken Sie auf **Appliance**, um WebYaST zu starten.

4e Klicken Sie auf **Aktualisieren**, um zu überprüfen, ob Aktualisierungen vorhanden sind.

4f Wählen Sie die Aktualisierungen aus und wenden Sie sie an.

Das Abschließen der Aktualisierungen kann einige Minuten in Anspruch nehmen. Nach der erfolgreichen Aktualisierung wird die WebYaST-Anmeldeseite angezeigt.

For dem Aufrüsten der Appliance stoppt WebYaST automatisch den Sentinel-Service. Nach dem Abschluss der Aufrüstung müssen Sie diesen Service manuell neu starten.

4g Löschen Sie den Webbrowser-Cache, um die neueste Version von Sentinel sehen zu können.

4h Starten Sie nach dem Abschluss der Aufrüstung den Clusterstapel neu.

```
rcopenais start
```

4i Führen Sie den folgenden Befehl aus, um alle Änderungen der Konfigurationsdateien zu synchronisieren:

```
run 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
```

30.3.2 Aufrüsten einer Sentinel-Hochverfügbarkeits-Appliance-Installation über WebYaST

Vor dem Aufrüsten müssen Sie alle Appliance-Knoten über WebYast registrieren. Weitere Informationen finden Sie unter Abschnitt 13.3.3, „Registrieren für Aktualisierungen“, auf Seite 88. 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 die passiven Clusterknoten auf:

3a Stoppen Sie den Clusterstapel.

```
rcopenais stop
```

Durch Stoppen des Clusterstapels wird sichergestellt, dass die Ressourcen zugreifbar bleiben, und wird die Umgrenzung der Knoten verhindert.

3b Geben Sie die URL des passiven Clusterknotens mit Port 4984 an, um WebYaST zu starten (`https://<IP-Adresse>:4984`, wobei `<IP-Adresse>` die IP-Adresse des Clusterknotens darstellt). Melden Sie sich als Administrator bei der Sentinel-Appliance an.

3c Klicken Sie auf **Aktualisieren**, um zu überprüfen, ob Aktualisierungen vorhanden sind.

3d Wählen Sie die Aktualisierungen aus und wenden Sie sie an.

Das Abschließen der Aktualisierungen kann einige Minuten in Anspruch nehmen. Nach der erfolgreichen Aktualisierung wird die WebYaST-Anmeldeseite angezeigt.

3e Starten Sie nach dem Abschluss der Aufrüstung den Clusterstapel neu.

```
rcopenais start
```

Wiederholen Sie Schritt 4 für alle passiven Clusterknoten.

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 *NetIQ Sentinel Administration Guide* (NetIQ Sentinel-Administrationshandbuch).

4b Stoppen Sie den Clusterstapel.

```
rcopenais stop
```

Durch Stoppen des Clusterstapels wird sichergestellt, dass die Ressourcen zugreifbar bleiben, und wird die Umgrenzung der Knoten verhindert.

4c Melden Sie sich als Administrator bei der Sentinel-Appliance an.

4d Zum Aufrüsten der Sentinel-Appliance klicken Sie auf **Appliance**, um WebYaST zu starten.

4e Klicken Sie auf **Aktualisieren**, um zu überprüfen, ob Aktualisierungen vorhanden sind.

4f Wählen Sie die Aktualisierungen aus und wenden Sie sie an.

Das Abschließen der Aktualisierungen kann einige Minuten in Anspruch nehmen. Nach der erfolgreichen Aktualisierung wird die WebYaST-Anmeldeseite angezeigt.

For dem Aufrüsten der Appliance stoppt WebYaST automatisch den Sentinel-Service. Nach dem Abschluss der Aufrüstung müssen Sie diesen Service manuell neu starten.

4g Löschen Sie den Webbrowser-Cache, um die neueste Version von Sentinel sehen zu können.

4h Starten Sie nach dem Abschluss der Aufrüstung den Clusterstapel neu.

```
rcopenais start
```

4i Führen Sie den folgenden Befehl aus, um alle Änderungen der Konfigurationsdateien zu synchronisieren:

```
run 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
```

31 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.

31.1 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 *NetIQ 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.

31.2 Recovery

31.2.1 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.

31.2.2 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.

31.2.3 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 *NetIQ 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.

VII Anhänge

A Fehlersuche

Dieser Abschnitt behandelt einige Probleme, die bei der Installation auftreten können, sowie die entsprechenden Abhilfemaßnahmen.

A.1 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.

A.2 Die UUID wird für Images von Collector-Managers oder Correlation Engines 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.

A.3 In Internet Explorer ist die Weboberfläche 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.

B Deinstallation

In diesem Anhang finden Sie Informationen über die Deinstallation von Sentinel und die Aufgaben nach der Deinstallation.

B.1 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.

B.2 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.

B.2.1 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:

   `/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.

B.2.2 Deinstallieren des Collector-Managers und der Correlation Engine

Gehen Sie folgendermaßen vor, um den Collector-Manager und die Correlation Engine zu deinstallieren:

1 Melden Sie sich als `root` beim Computer des Collector-Managers und der Correlation Engine an.

   HINWEIS: Sie können den Remote-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 „j“ 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 Weboberfläche angezeigt.

5 Führen Sie folgende zusätzliche Schritte aus, um den Collector-Manager und die Correlation Engine manuell aus der Weboberfläche 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-Weboberfläche an.
   2. Erweitern Sie den Abschnitt **Korrelation** und wählen Sie die zu löschende Correlation Engine aus.
   3. Klicken Sie auf die Schaltfläche **Löschen** (Papierkorbsymbol).

B.2.3 Deinstallieren des NetFlow Collector-Managers

Gehen Sie folgendermaßen vor, um den NetFlow Collector-Manager zu deinstallieren:

1 Melden Sie sich beim Computer des NetFlow Collector-Managers 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 `j` ein.

Das Skript stoppt den Dienst zunächst und deinstalliert ihn dann vollständig.

B.3 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.