Installations- und Konfigurationshandbuch

NetIQ Sentinel 7.0.1

March 2012

Rechtliche Hinweise

Weitere Informationen erhalten Sie von NetIQ unter folgender Anschrift:

1233 West Loop South, Houston, Texas 77027

USA

www.netiq.com

Inhalt

Allgemeines zu diesem Handbuch

Dieses Handbuch enthält eine Einführung in NetIQ Sentinel sowie Erklärungen zur Installation, Migration und Konfiguration von Sentinel.

Zielgruppe

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

Rückmeldungen

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

Aktualisierungen der Dokumentation

Die jeweils neueste Version des *Installations- und Konfigurationshandbuchs für NetIQ Sentinel 7.0.1* finden Sie auf der Sentinel-Dokumentationswebsite (http://www.novell.com/documentation/sentinel70).

Weitere Dokumentation

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

- Sentinel Overview Guide (Sentinel-Übersichtshandbuch) (http://www.novell.com/documentation/sentinel70/s70_overview/data/bookinfo.html)
- Sentinel Quick Start Guide (Kurzanleitung für Sentinel) (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Sentinel Administration Guide (Sentinel-Administrationshandbuch) (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Sentinel User Guide (Sentinel-Benutzerhandbuch) (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Sentinel Link Overview Guide (Sentinel Link-Übersichtshandbuch) (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Sentinel Internal Audit Events (Sentinel-interne Auditereignisse) (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  Auf der Sentinel SDK-Website finden Sie Informationen zum Erstellen eigener Plugins.

Anfragen an Novell und NetIQ

Sentinel ist nun ein Produkt von NetIQ. Novell leistet jedoch noch viele der Supportfunktionen.

- Novell-Website (http://www.novell.com)
- NetIQ-Website (http://www.netiq.com)
- Technischer Support (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Self-Support (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Patch Download Site (http://download.novell.com/index.jsp)
- Sentinel Community Support Forum (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sentinel TIDS (http://support.novell.com/products/sentinel)
- Sentinel-Plugin-Website (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **EMail-Liste für Benachrichtigungen:** Registrieren Sie sich auf der Sentinel-Plugin-Website.

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: NetIQ-Standorte (http://www.netiq.com/about_netiq/officelocations.asp)

Vereinigte Staaten und Kanada: 888-323-6768

EMail: info@netiq.com

Website: www.netiq.com

Installieren

Beachten Sie folgende Informationen bei der Installation von Sentinel:

1 Erfüllen der Systemanforderungen

Der folgende Abschnitt beschreibt die Anforderungen in Bezug auf Hardware, Betriebssystem, Browser, unterstützte Connectors und Ereignisquellenkompatibilität für Sentinel.

1.1 Systemanforderungen und unterstützte Plattformen

NetIQ unterstützt Sentinel auf den in diesem Abschnitt beschriebenen Betriebssystemen. NetIQ unterstützt Sentinel außerdem auf Systemen mit geringfügigen Aktualisierungen dieser Betriebssysteme, beispielsweise Sicherheits-Patches oder Hotfixes. Das Ausführen von Sentinel auf Systemen mit wesentlichen Aktualisierungen dieser Betriebssysteme wird jedoch erst unterstützt, wenn NetIQ diese Aktualisierungen geprüft und zertifiziert hat.

1.1.1 Unterstützte Betriebssysteme und Plattformen

Der Sentinel-Server, der Collector-Manager und die Correlation Engine werden auf folgenden Betriebssystemen und Plattformen unterstützt:

Kategorie	Anforderung
Betriebssystem	Sentinel wird auf folgenden Betriebssystemen unterstützt: ◆ SUSE Linux Enterprise Server (SLES) 11 SP1, 64-Bit * ◆ Red Hat Enterprise Linux für Server (RHEL) 6, 64-Bit * Auf Open Enterprise Server-Installationen von SLES wird Sentinel 7 nicht unterstützt.
Virtuelle Plattform	Für folgende virtuelle Plattformen stellt NetIQ Appliances zur Verfügung, die einen 64-Bit-SLES 11 SP1-Server und Sentinel installieren: ◆ VMWare ESX 4.0 ◆ Xen 4.0
ISO-DVD	Für folgende Systeme stellt NetIQ zur Installation des 64-Bit-SLES 11 SP1-Servers und von Sentinel eine DVD-ISO-Datei zur Verfügung: ◆ Hyper-V Server 2008 R2 ◆ Hardware ohne installiertes Betriebssystem

1.1.2 Hardwareanforderungen

Die Hardwareempfehlungen für eine Sentinel-Implementierung können je nach Implementierungstyp unterschiedlich ausfallen. Ziehen Sie daher vor der Fertigstellung der Sentinel-Architektur die NetIQ Consulting Services oder einen der NetIQ Sentinel-Partner zu Rate.

- „Sentinel-Server“, auf Seite 12
- „Collector-Manager“, auf Seite 13
- „Correlation Engine“, auf Seite 14

Sentinel-Server

Dieser Abschnitt enthält Informationen zu den Hardwareempfehlungen für ein Produktionssystem, das 90 Tage Online-Daten speichert. Die Empfehlungen basieren auf einer angenommenen durchschnittlichen Ereignisgröße von 600 Byte. Die Empfehlungen für den lokalen Speicher und den Netzwerkspeicher enthalten zusätzlich zum geschätzten tatsächlichen Speicherbedarf 20 % Puffer. NetIQ empfiehlt, einen Puffer zu integrieren, da die Schätzungen ungenau sein können und bestimmte Server mit der Zeit möglicherweise stärker ausgelastet sind.

Beachten Sie folgende Hardwareempfehlungen, um den Sentinel-Server mit allen Sentinel-Komponenten auf einem einzelnen Server auszuführen:

Kategorie	100 EPS	2500 EPS	5000 EPS
Prozessor	Ein Intel Xeon X5570 2,93 GHz (4 CPU-Kerne)	2 Intel Xeon X5470 3,33 GHz (4 Core)-CPUs (insgesamt 8 Cores)	2 Intel Xeon X5470 3,33 GHz (4 Core)-CPUs (insgesamt 8 Cores)
Lokaler Speicher (30 Tage)	2 x 256 GB, 7200-RPM-Laufwerke (Hardware-RAID 1 mit 256 MB Cache)	8 x 1,2 TB, 7200-RPM-Laufwerke (Hardware-RAID 10 mit 256 MB Cache)	16 x 1,2 TB, 15000-RPM-Laufwerke (Hardware-RAID 10 mit 512 MB Cache) oder ein gleichwertiges Storage Area Network (SAN)
Netzwerkspeicher (90 Tage)	2 x 128 GB	4 x 1 TB	8 x 1 TB
Arbeitsspeicher	**Sonstige Installationen:** 4 GB **DVD-ISO-Installation:** 4,5 GB	16 GB	24 GB

NOTE: Sentinel wird auf X86-64-Bit-Intel Xeon- und AMD Opteron-Prozessoren unterstützt, nicht jedoch auf reinen 64-Bit-Prozessoren wie Itanium.

Beachten Sie für eine optimale Systemleistung folgende Richtlinien:

- Im lokalen Speicher muss mindestens ausreichend Speicherplatz für Daten der 5 letzten Tage vorhanden sein. Dies umfasst sowohl Ereignisdaten als auch Rohdaten. Weitere Details zur Berechnung der Datenspeicheranforderungen finden Sie unter Abschnitt 1.1.5, „Schätzung der Datenspeicheranforderung“, auf Seite 16.
- Der Netzwerkspeicher enthält die Daten der gesamten 90 Tage, einschließlich einer komprimierten Kopie der Ereignisdaten aus dem lokalen Speicher. Eine Kopie der Ereignisdaten wird im lokalen Speicher beibehalten, um bei Suchvorgängen und bei der Berichterstellung eine optimale Leistung zu gewährleisten. Wenn die Kosten für den Speicherplatz stärker berücksichtigt werden müssen, kann die Größe des lokalen Speichers reduziert werden. Dies führt jedoch aufgrund des Dekomprimierungs-Overheads zu schätzungsweise 70 % geringerer Leistung bei Suchvorgängen und bei der Berichterstellung mit Daten, die sonst im lokalen Speicher enthalten wären.
- Der Netzwerkspeicherort muss als externes SAN mit mehreren Laufwerken oder als NAS (Network Attached Storage) eingerichtet werden.
- Das empfohlene stationäre Speichervolumen beträgt 80 Prozent der maximal lizenzierten EPS. NetIQ empfiehlt, zusätzliche Sentinel-Instanzen zu erwerben, wenn diese Grenze erreicht wird.

Collector-Manager

Beachten Sie folgende Hardwareanforderungen, wenn der Collector-Manager auf einem anderen System als der Sentinel-Server in einer Produktionsumgebung ausgeführt werden soll:

Kategorie	Mindestanforderung	Empfehlung
Prozessor	Intel Xeon L5240 3 GHz (2 Core)	Ein Intel Xeon X5570 2,93 GHz (4 CPU-Kerne)
Festplattenspeicher	10 GB (RAID 1)	20 GB (RAID 1)
Arbeitsspeicher	1,5 GB	4 GB
Geschätzte Rate (EPS)	500	2000

Correlation Engine

Beachten Sie folgende Hardwareanforderungen, um die Correlation Engine auf einem separaten System vom Sentinel-Server in einer Produktionsumgebung auszuführen:

Kategorie	Mindestanforderung	Empfehlung
Prozessor	Intel Xeon L5240 3 GHz (2 Core)	Ein Intel Xeon X5570 2,93 GHz (4 CPU-Kerne)
Festplattenspeicher	10 GB (kein RAID erforderlich)	10 GB (kein RAID erforderlich)
Arbeitsspeicher	1,5 GB	4 GB
Geschätzte Rate (EPS)	500	2500

1.1.3 Unterstützte Datenbankplattformen

Sentinel enthält ein eingebettetes, dateibasiertes Speichersystem und eine Datenbank, die zum Ausführen von Sentinel erforderlich sind. Wenn Sie jedoch die optionale Datensynchronisierungsfunktion nutzen, um Daten in ein Data Warehouse zu kopieren, unterstützt Sentinel Oracle Version 11g R2 oder Microsoft SQL Server 2008 R2 als Data Warehouse.

1.1.4 Unterstützte Browser

Die Sentinel-Weboberfläche ist für eine Auflösung von 1280 x 1024 oder höher in den folgenden unterstützten Browsern optimiert:

NOTE: Zum ordnungsgemäßen Laden der Sentinel-Client-Anwendungen muss das Sun Java-Plugin auf dem System installiert sein.

Plattform	Browser
Windows 7	◆ Firefox 5, 6, 7, 8, 9 und 10 ◆ Internet Explorer 8 und 9* Informationen zu Internet Explorer 8 finden Sie unter „Voraussetzungen für Internet Explorer“, auf Seite 15.
SLES 11 SP1 und RHEL 6	◆ Firefox 5, 6, 7, 8, 9 und 10 Weitere Informationen finden Sie unter „Manuelles Aktualisieren der Firefox-Version“, auf Seite 15.

Voraussetzungen für Internet Explorer

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.

Manuelles Aktualisieren der Firefox-Version

Sentinel unterstützt die Firefox-Versionen 5 bis 10. Das SLES 11 SP1-System ist jedoch mit Firefox Version 3.6*x* gebündelt. Führen Sie folgende Schritte aus, um mittels manueller Aktualisierung der SLES 11 SP1-Installation eine unterstützte Version von Firefox hinzuzufügen:

1. Öffnen Sie YaST.
2. Wählen Sie *Software* > *Software-Repositorys*, um das Fenster für die konfigurierten Software-Repositorys anzuzeigen.
3. Klicken Sie auf *Hinzufügen*, um das Medientyp-Fenster zu öffnen.
4. Wählen Sie die Option *URL angeben* aus und klicken Sie dann auf *Weiter*.

   Das Fenster für die Repository-URL wird angezeigt.
5. Geben Sie den Link für das Software-Repository (http://download.opensuse.org/repositories/mozilla/SLE_11/) in das Textfeld für die URL ein und klicken Sie auf *Weiter*.

   Das Software-Repository wird heruntergeladen.
6. Klicken Sie auf *OK*, um das Software-Repository zu aktualisieren.
7. Klicken Sie auf *Softwareverwaltung*, um das YaST2-Fenster zu öffnen.
8. Geben Sie `Firefox` in das Textfeld *Suchen* ein.

   Die Liste der Firefox-Pakete wird angezeigt.

9 Wählen Sie die erforderlichen Pakete für die unterstützte Version von Firefox aus, die Sie installieren möchten.

   Wenn Sie ein Paket auswählen, das mit der bestehenden Version nicht vereinbar ist, wird ein Dialogfenster mit einem Warnhinweis angezeigt. Wählen Sie die geeignete Option aus und klicken Sie auf die Schaltfläche *OK, erneut versuchen*.

10 Klicken Sie auf *Akzeptieren*.

1.1.5 Schätzung der Datenspeicheranforderung

Mit Sentinel werden Rohdaten über einen längeren Zeitraum aufbewahrt, um rechtliche sowie andere Vorschriften zu erfüllen. Sentinel unterstützt Sie durch die Komprimierung der Daten dabei, den lokalen und vernetzten Speicherplatz effizient zu nutzen. Speicheranforderungen können jedoch über einen langen Zeitraum gesehen zu einem wichtigen Faktor werden.

Um Beschränkungen aufgrund von Kostenfaktoren zu überwinden, verwenden Sie kosteneffiziente Datenspeichersysteme zur langfristigen Speicherung von Daten. Bandbasierte Speichersysteme stellen die gängigste und kosteneffizienteste Lösung dar. Bänder ermöglichen jedoch keinen wahlfreien Zugriff auf gespeicherte Daten, der für schnelle Suchen erforderlich ist. Daher ist ein Hybridansatz zur langfristigen Datenspeicherung wünschenswert, bei dem die Daten für die Suche auf einem Speichersystem mit wahlfreiem Zugriff abgelegt werden und die Daten, die nur aufbewahrt und nicht gesucht werden müssen, auf einer kosteneffizienteren Alternative wie einem Band gespeichert werden. Anweisungen zur Bereitstellung dieses Hybridansatzes finden Sie unter "Using Sequential-Access Storage for Long Term Data Storage" (Verwendung der Speicherung mit sequenziellem Zugriff für die langfristige Datenaufbewahrung) im *NetIQ Sentinel 7.0.1 Administration Guide* (NetIQ Sentinel 7.0.1-Administrationshandbuch).

Um den für Sentinel erforderlichen Speicherplatz mit wahlfreiem Zugriff zu bestimmen, schätzen Sie die Anzahl der Tage ab, für deren Daten Sie regelmäßig Suchen ausführen oder Berichte erstellen. Sie sollten entweder lokal auf dem Sentinel-Computer oder remote im SMB (Server Message Block)-Protokoll oder CIFS-Protokoll, im NFS (Network File System) oder in einem SAN über ausreichend Festplattenspeicher verfügen, der von Sentinel zur Datenarchivierung verwendet werden kann.

Zusätzlich zu den Mindestanforderungen sollten Sie weiteren Festplattenspeicher für die folgenden Fälle bereithalten:

- Zum Auffangen von Datenraten, die höher ausfallen als erwartet
- Zum Zurückkopieren von auf Band archivierten Daten nach Sentinel für die Suche und Berichterstellung auf Basis historischer Daten

Verwenden Sie die folgenden Formeln, um den zum Speichern der Daten erforderlichen Speicherplatz zu ermitteln:

- **Lokaler Ereignis-Speicher (teilweise komprimiert):** {durchschnittliche Ereignisgröße in Byte} x {Anzahl der Tage} x {Ereignisanzahl pro Sekunde} x 0.00008 = erforderlicher Gesamtspeicherplatz in GB

  Ereignisgrößen bewegen sich üblicherweise in einem Bereich von 300 bis 1000 Byte.
- **Netzwerk-Ereignis-Speicher (vollständig komprimiert):** {durchschnittliche Ereignisgröße in Byte} x {Anzahl der Tage} x {Ereignisanzahl pro Sekunde} x 0,00001 = erforderlicher Gesamtspeicherplatz in GB
- **Rohdatenspeicher (vollständig komprimiert, sowohl im lokalen Speicher als auch im Netzwerkspeicher):** {durchschnittliche Größe eines Rohdatensatzes in Byte} x {Anzahl der Tage} x {Ereignisanzahl pro Sekunde} x 0,000003 = erforderlicher Gesamtspeicherplatz in GB

Die durchschnittliche Rohdatengröße für Syslog-Meldungen beträgt in der Regel 200 Byte.

- **Gesamtgröße des lokalen Speichers (bei aktiviertem Netzwerkspeicher):** {Größe des lokalen Ereignis-Speichers für die gewünschte Anzahl an Tagen} + {Größe des Rohdatenspeichers für einen Tag) = erforderlicher Gesamtspeicherplatz in GB

  Wenn der Netzwerkspeicher aktiviert ist, werden die Ereignisdaten üblicherweise nach 2 Tagen in den Netzwerkspeicher kopiert. Weitere Informationen finden Sie unter "Configuring Data Storage (Konfigurieren der Datenspeicherung)" im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.

- **Gesamtgröße des lokalen Speichers (bei deaktiviertem Netzwerkspeicher):** {Größe des lokalen Ereignis-Speichers für die Beibehaltungszeit} + {Größe des Rohdatenspeichers für die Beibehaltungszeit) = erforderlicher Gesamtspeicherplatz in GB
- **Gesamtgröße des Netzwerkspeichers:** {Größe des Netzwerkspeichers für die Beibehaltungszeit} + {Größe des Rohdatenspeichers für die Beibehaltungszeit} = erforderliche Gesamtspeichergröße in GB

NOTE:

- Die Koeffizienten in den Formeln ergeben sich aus ((Sekunden pro Tag) x (GB pro Byte) x Komprimierungsverhältnis).
- Diese Zahlen stellen lediglich Schätzungen dar und hängen von der Größe der Ereignisdaten sowie von der Größe der komprimierten Daten ab.
- „Teilweise komprimiert" bedeutet, dass die Daten komprimiert sind, der Index der Daten jedoch nicht komprimiert ist. „Vollständig komprimiert" bedeutet, dass sowohl die Ereignisdaten als auch die Indexdaten komprimiert sind. Das Komprimierungsverhältnis für Ereignisdaten ist üblicherweise 10:1. Das Komprimierungsverhältnis für Indexdaten ist üblicherweise 5:1. Der Index dient dem Optimieren der Suche in den Daten.

Anhand der oben genannten Formeln können Sie auch ermitteln, wie viel Speicherplatz für ein langfristiges Datenspeichersystem wie ein Band erforderlich ist.

1.1.6 Schätzung der Datenträger-E/A-Nutzung

Verwenden Sie die folgenden Formeln zur Schätzung der Datenträgernutzung auf dem Server bei unterschiedlichen EPS-Raten.

- **Auf den Datenträger geschriebene Daten (Kilobyte pro Sekunde):** (durchschnittliche Ereignisgröße in Byte + durchschnittliche Rohdatengröße in Byte) x (Ereignisanzahl pro Sekunde) x 0,002 Kompressionsverhältnis = pro Sekunde auf den Datenträger geschriebene Daten

  Bei beispielsweise 500 EPS, einer durchschnittlichen Ereignisgröße von 758 Byte und einer durchschnittlichen Rohdatengröße von 490 Byte in der Protokolldatei kann die Größe der auf den Datenträger geschriebenen Daten folgendermaßen ermittelt werden:

  (758 Byte + 490 Byte) x 500 EPS x 0,002 = 1100 KB

- **Anzahl der E/A-Anforderungen an den Datenträger (Übertragungen pro Sekunde):**

  (durchschnittliche Ereignisgröße in Byte + durchschnittliche Rohdatengröße in Byte) x (Ereignisanzahl pro Sekunde) x 0,00002 Kompressionsverhältnis = E/A-Anforderungen an Datenträger pro Sekunde

Bei beispielsweise 500 EPS, einer durchschnittlichen Ereignisgröße von 758 Byte und einer durchschnittlichen Rohdatengröße von 490 Byte in der Protokolldatei kann die Anzahl der E/A-Anforderungen an den Datenträger pro Sekunde folgendermaßen ermittelt werden:

(758 Byte + 490 Byte) x 500 EPS x 0,00002 = ca. 10 Übertragungen pro Sekunde

- **Anzahl der pro Sekunde auf den Datenträger geschriebenen Blöcke:** (durchschnittliche Ereignisgröße in Byte + durchschnittliche Rohdatengröße in Byte) x (Ereignisanzahl pro Sekunde) x 0,003 Kompressionsverhältnis = pro Sekunde auf den Datenträger geschriebene Blöcke

  Bei beispielsweise 500 EPS, einer durchschnittlichen Ereignisgröße von 758 Byte und einer durchschnittlichen Rohdatengröße von 490 Byte in der Protokolldatei kann die Anzahl der pro Sekunde auf den Datenträger geschriebenen Blöcke folgendermaßen ermittelt werden:

  (758 Byte + 490 Byte) x 500 EPS x 0,003 = ca. 1800 Blöcke pro Sekunde

- **Beim Ausführen eines Suchvorgangs pro Sekunde vom Datenträger gelesene Daten:**

  (durchschnittliche Ereignisgröße in Byte + durchschnittliche Rohdatengröße n Byte) x (Anzahl der mit der Suchabfrage übereinstimmenden Ereignisse in Millionen) x 0,40 Kompressionsverhältnis = pro Sekunde vom Datenträger gelesene Kilobyte

  Bei beispielsweise einer Anzahl von 5 Millionen Ereignisse, die mit der Suchabfrage übereinstimmen, einer durchschnittlichen Ereignisgröße von 758 Byte und einer durchschnittlichen Rohdatengröße von 490 Byte in der Protokolldatei kann die Größe der pro Sekunde vom Datenträger gelesenen Daten folgendermaßen ermittelt werden:

  (758 Byte + 490 Byte) x 5 x 0,40 = ca. 500 KB

1.1.7 Schätzung der Netzwerkbandbreitennutzung

Verwenden Sie folgende Formeln zur Schätzung der genutzten Netzwerkbandbreite zwischen dem Sentinel-Server und dem Remote-Collector-Manager bei verschiedenen EPS-Raten:

{durchschnittliche Ereignisgröße in Byte + durchschnittliche Rohdatengröße in Byte} x {Ereignisanzahl pro Sekunde} x 0,0003 Kompressionsverhältnis = Netzwerkbandbreite in KBit/s (Kilobit pro Sekunde)

Bei beispielsweise 500 EPS, einer durchschnittlichen Ereignisgröße von 758 Byte und einer durchschnittlichen Rohdatengröße von 490 Byte in der Protokolldatei kann die Netzwerkbandbreitennutzung folgendermaßen ermittelt werden:

(758 Byte + 490 Byte} x 500 EPS x 0,0003 = ca. 175 KBit/s

1.1.8 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 Abschnitt 1.1, „Systemanforderungen und unterstützte Plattformen“, auf Seite 11.

1.2 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-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

1.3 Verwendete Ports

1.3.1 Sentinel-Server

Lokale Ports

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

Ports	Beschreibung
TCP 5432	Wird für die PostgreSQL-Datenbank verwendet. Dieser Port muss standardmäßig nicht geöffnet werden. Wenn Sie jedoch Berichte unter Verwendung von Sentinel SDK erstellen, muss dieser Port geöffnet werden. Weitere Informationen finden Sie auf der Sentinel-Plugin-SDK-Website (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).
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.

Netzwerkports

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 Standardinstallation müssen Sie jedoch das Betriebssystem, auf dem Sie Sentinel installieren, so konfigurieren, dass die entsprechenden Ports in der Firewall geöffnet sind.

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

Ports	Beschreibung
TCP 1099 und 2000	Werden gemeinsam von Überwachungswerkzeugen verwendet, um mit Java Management Extensions (JMX) eine Verbindung zum Sentinel-Serverprozess herzustellen.
TCP 1289	Wird für Audit-Verbindungen verwendet.
UDP 1514	Wird für Syslog-Meldungen verwendet.
TCP 8443	Wird für die HTTPS-Kommunikation verwendet.
TCP 1443	Wird für SSL-verschlüsselte Syslog-Meldungen verwendet.
TCP 61616	Dient zur Kommunikation zwischen Collector-Manager-Instanzen und dem Server.
TCP 10013	Wird von Sentinel Control Center und Solution Designer verwendet.
TCP 1468	Wird für Syslog-Meldungen verwendet.
TCP 10014	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.

Spezifische Ports für die Sentinel-Server-Appliance

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

Ports	Beschreibung
TCP 22	Wird für sicheren Shell-Zugriff auf die Sentinel Appliance verwendet.
TCP 54984	Wird von der Verwaltungskonsole der Sentinel-Appliance (WebYaST) verwendet. Wird außerdem von der Sentinel-Appliance für den Aktualisierungsservice verwendet.
TCP 289	Wird für Audit-Verbindungen an 1289 weitergeleitet.
UDP 443	Wird für die HTTPS-Kommunikation an 8443 weitergeleitet.
UDP 514	Wird für Syslog-Meldungen an 1514 weitergeleitet.
TCP 1290	Dies ist der Sentinel Link-Port, der eine Verbindung über die SuSE-Firewall erstellen darf.
UDP und TCP 40000–41000	Ports die bei der Konfiguration von Datensammlungsservern verwendet werden können, beispielsweise eines Syslog-Servers. Standardmäßig überwacht Sentinel diese Ports nicht.

1.3.2 Collector-Manager

Netzwerkports

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

Ports	Beschreibung
TCP 1289	Wird für Audit-Verbindungen verwendet.
UDP 1514	Wird für Syslog-Meldungen verwendet.
TCP 1443	Wird für SSL-verschlüsselte Syslog-Meldungen verwendet.
TCP 1468	Wird für Syslog-Meldungen verwendet.
TCP 1099 und 2000	Werden gemeinsam von Überwachungswerkzeugen verwendet, um mit Java Management Extensions (JMX) eine Verbindung zum Sentinel-Serverprozess herzustellen.

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	Beschreibung
TCP 22	Wird für sicheren Shell-Zugriff auf die Sentinel Appliance verwendet.
TCP 54984	Wird von der Verwaltungskonsole der Sentinel-Appliance (WebYaST) verwendet. Wird außerdem von der Sentinel-Appliance für den Aktualisierungsservice verwendet.
TCP 289	Wird für Audit-Verbindungen an 1289 weitergeleitet.
UDP 514	Wird für Syslog-Meldungen an 1514 weitergeleitet.
TCP 1290	Dies ist der Sentinel Link-Port, der eine Verbindung über die SuSE-Firewall erstellen darf.
UDP und TCP 40000–41000	Ports die bei der Konfiguration von Datensammlungsservern verwendet werden können, beispielsweise eines Syslog-Servers. Standardmäßig überwacht Sentinel diese Ports nicht.

1.3.3 Correlation Engine

Netzwerkports

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

Ports	Beschreibung
TCP 1099 und 2000	Werden gemeinsam von Überwachungswerkzeugen verwendet, um mit Java Management Extensions (JMX) eine Verbindung zum Sentinel-Serverprozess herzustellen.

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	Beschreibung
TCP 22	Wird für sicheren Shell-Zugriff auf die Sentinel Appliance verwendet.
TCP 54984	Wird von der Verwaltungskonsole der Sentinel-Appliance (WebYaST) verwendet. Wird außerdem von der Sentinel-Appliance für den Aktualisierungsservice verwendet.

2 Installieren von Sentinel

Sentinel kann als eigenständige Installation oder als Appliance installiert werden. Das Installationsprogramm für die eigenständige Installation installiert Sentinel auf einem vorhandenen SUSE Linux Enterprise Server (SLES) 11 SP1- oder einem Red Hat Enterprise Linux (RHEL) 6-Betriebssystem. Das Appliance-Installationsprogramm installiert sowohl das 64-Bit-SLES 11 SP1-Betriebssystem als auch Sentinel.

Dieser Abschnitt beschreibt die Prozedur für eine eigenständige Installation des Sentinel-Servers auf einem vorhandenen SLES 11 SP1- bzw. RHEL 6-System. Anweisungen zur Installation der Appliance finden Sie in Kapitel 5, „Installieren der Appliance“, auf Seite 41.

2.1 Installationsmethoden

Für die eigenständige Installation stehen folgende Methoden zur Verfügung:

- **Interaktiv:** Zum Fortführen der Installation sind Benutzereingaben erforderlich. Während der Installation können Sie die Installationsoptionen (Benutzereingaben oder Standardwerte) in einer Datei speichern, die später für eine automatische Installation verwendet werden kann.
- **Automatisch:** Diese Option ist verfügbar, wenn die Installationsoptionen zuvor aufgezeichnet wurden. Die automatische Installation verwendet die Angaben aus der Datei mit den aufgezeichneten Installationseingaben und führt die Installation mit den in dieser Datei erfassten Werten aus. Der Automatikmodus ist sinnvoll, wenn Sie viele Reproduktionen der gleichen Konfiguration in einer Umgebung installieren möchten. Weitere Informationen finden Sie unter Abschnitt 2.5, „Automatische Installation“, auf Seite 29.

Sowohl die interaktive als auch die automatische Installation von Sentinel kann entweder mit dem Benutzer `root` oder mit einem Nicht-root-Benutzer ausgeführt werden.

2.1.1 Standardinstallation und benutzerdefinierte Installation

Bei der Installation von Sentinel sind folgende Konfigurationen verfügbar:

- **Standard:** In dieser Konfiguration wird die Installation mit Standardwerten für die Konfigurationseinrichtung ausgeführt. Eine Benutzereingabe ist lediglich für das Passwort erforderlich. Weitere Informationen zur Installation von Sentinel mit der Standardkonfiguration finden Sie in Abschnitt 2.4.1, „Standardkonfiguration“, auf Seite 26.
- **Benutzerdefiniert:** In dieser Konfiguration werden Sie während der Installation zur Eingabe von Werten für die Konfigurationseinrichtung aufgefordert. Sie können die Standardwerte auswählen oder die gewünschten Werte angeben. Weitere Informationen zur Installation von Sentinel mit einer benutzerdefinierten Konfiguration finden Sie in Abschnitt 2.4.2, „Benutzerdefinierte Konfiguration“, auf Seite 28.

Standardkonfiguration	Benutzerdefinierte Konfiguration
Verwendet den standardmäßigen 90-Tage-Evaluierungsschlüssel.	Bietet die Möglichkeit, den 90-Tage-Lizenzschlüssel 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.
Authentifiziert die Benutzer mit der internen Datenbank.	Bietet die Möglichkeit, Benutzer entweder mit der internen Datenbank oder über LDAP-Authentifizierung zu authentifizieren.

2.1.2 Installierte Komponenten

Sentinel enthält mehrere Komponenten. Standardmäßig werden alle folgenden Komponenten installiert:

- Sentinel-Server
- Correlation Engine
- Collector-Manager

Zusätzliche Correlation Engines oder Collector-Manager-Instanzen können auf verschiedenen Systemen installiert werden.

2.2 Vor dem Beginn

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

- Vergewissern Sie sich, dass die Hardware und Software die in Abschnitt 1.1, „Systemanforderungen und unterstützte Plattformen“, auf Seite 11 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 Teil V, „Deinstallation“, auf Seite 103.

- Um eine optimale Leistung, Stabilität und Zuverlässigkeit des Sentinel-Servers zu gewährleisten, nutzen Sie unter SLES das ext3-Dateisystem und unter RHEL das ext4-Dateisystem. Weitere Informationen zu Dateisystemen finden Sie unter Overview of File Systems in Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) (Überblick über Dateisysteme in Linux) im *Storage Administration Guide* (Handbuch zur Speicherungsverwaltung).
- Konfigurieren Sie die Netzwerkeinstellungen so, dass das System über eine gültige IP-Adresse und einen gültigen Hostnamen verfügt.
- Wenn Sie eine lizenzierte Version installieren möchten, wenden Sie sich an den Novell Kundenservice (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22), um Ihren Lizenzschlüssel zu erhalten.
- Synchronisieren Sie die Zeit mit NTP (Network Time Protocol).
- Vergewissern Sie sich, dass die in Abschnitt 1.3, „Verwendete Ports“, auf Seite 19 aufgeführten Ports in der Firewall geöffnet sind.
- Um eine optimale Leistung zu ermöglichen, müssen die Speichereinstellungen für die PostgreSQL-Datenbank geeignet sein:

  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 eine minimale oder monitorlose Installation muss das Betriebssystem für den Sentinel-Server mindestens die Basisserver-Komponenten des SLES- bzw. RHEL 6-Servers enthalten. Sentinel erfordert die 64-Bit-Versionen folgender RPMs:
  - bash
  - bc
  - coreutils
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof
  - net-tools
  - openssl
  - python-libs
  - sed
  - zlib

2.3 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

2.4 Interaktive Installation

2.4.1 Standardkonfiguration

1. Laden Sie die Sentinel-Installationsdatei von der Novell Downloads-Webseite (http://download.novell.com/index.jsp) 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 7.0 Evaluation (Sentinel 7.0-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 sentinel_server-7.0.0.0.x86_64
```

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 90-Tage-Evaluierungsschlüssel, der im Installationsprogramm enthalten ist, fortgesetzt. Dieser Lizenzschlüssel aktiviert den vollständigen Satz an Produktfunktionen für einen Testzeitraum von 90 Tagen. 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.

2.4.2 Benutzerdefinierte Konfiguration

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 Novell Downloads-Webseite (http://download.novell.com/index.jsp) 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 7.0 Evaluation (Sentinel 7.0-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 90-Tage-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`.

   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.

2.5 Automatische Installation

Die automatische oder unbeaufsichtigte Installation von Sentinel 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 2.4.1, „Standardkonfiguration“, auf Seite 26 oder Abschnitt 2.4.2, „Benutzerdefinierte Konfiguration“, auf Seite 28.

1 Laden Sie die Installationsdateien von der Novell Downloads-Webseite (http://download.novell.com/index.jsp) 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*> durch den 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.

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.

2.6 Installieren von Sentinel mit einem Nicht-root-Benutzer

Wenn Ihre Unternehmensrichtlinie nicht zulässt, dass Sie die gesamte Sentinel-Installation mit dem Benutzer `root` ausführen, können Sie Sentinel mit einem anderen Benutzer installieren. Bei dieser Installationsart werden die einige wenige Schritte mit dem Benutzer `root` ausgeführt. Anschließend stellen Sie die Sentinel-Installation mit einem anderen Benutzer fertig, der mit dem Benutzer `root` erstellt wurde. Danach wird die Installation mit dem Benutzer `root` fertig gestellt.

1 Laden Sie die Installationsdateien von der Novell Downloads-Webseite (http://download.novell.com/index.jsp) 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: `novell`:

```
su novell
```

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

7a Geben Sie folgenden Befehl ein:

```
./install-sentinel
```

Um Sentinel an einem anderen als dem Standardstandort zu installieren, geben Sie zusammen mit dem Befehl die Option „--location“ an. Beispiel:.

```
./install-sentinel --location=/foo
```

7b Fahren Sie mit Schritt 9 fort.

8 (Bedingt) So führen Sie eine automatische Installation aus:

8a Geben Sie folgenden Befehl ein:

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

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 2.4.1, „Standardkonfiguration“, auf Seite 26.
- Wenn Sie die benutzerdefinierte Konfiguration auswählen, fahren Sie fort mit Schritt 7 bis Schritt 14 in Abschnitt 2.4.2, „Benutzerdefinierte Konfiguration“, auf Seite 28.

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.

2.7 Ändern der Konfiguration nach der Installation

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

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

```
./configure.sh
```

2. Geben Sie `1` ein, um die Standardkonfiguration durchzuführen, oder `2`, um Sentinel benutzerdefiniert zu konfigurieren.
3. Drücken Sie die Leertaste, um die Lizenzvereinbarung durchzulesen.
4. 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.
5. Geben Sie `1` ein, um den standardmäßigen 90-Tage-Evaluierungslizenzschlüssel zu verwenden.

   Alternativ:

   Geben Sie `2` ein, um einen erworbenen Lizenzschlüssel für Sentinel einzugeben.
6. 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 7.
   - 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 7.
7. 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 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.

   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.
8. 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 9.
   - Wenn Sie das Passwort ändern möchten, geben Sie `2` ein. Geben Sie dann das neue Passwort an, bestätigen Sie das Passwort und fahren Sie fort mit Schritt Schritt 9.

   Das `dbauser`-Konto wird von Sentinel zur Interaktion mit der Datenbank verwendet. Das hier eingegebene Passwort kann zum Ausführen von Datenbankwartungsaufgaben verwendet werden, unter anderem zum Zurücksetzen des Administratorpassworts, falls dieses vergessen wird bzw. nicht mehr auffindbar ist.
9. Ändern Sie die Portzuweisungen für die Sentinel-Services, indem Sie die entsprechende Nummer und dann die neue Portnummer angeben.
10. Geben Sie nach dem Ändern der Ports „7“ ein, um den Änderungsvorgang abzuschließen.
11. 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`.

3 Installieren zusätzlicher Collector-Manager-Instanzen

Standardmäßig installiert Sentinel einen Collector-Manager. Je nach Umgebung sind gegebenenfalls mehrere Collector-Manager-Instanzen erforderlich. Nachfolgend finden Sie Informationen zur Installation von Remote-Collector-Manager-Instanzen.

IMPORTANT: Es ist nicht möglich, auf dem Server, auf dem Sentinel ausgeführt wird, einen weiteren Collector-Manager oder eine weitere Correlation Engine zu installieren.

3.1 Vorteile zusätzlicher Collector-Manager-Instanzen

Die Installation von mehr als einem Collector-Manager in einem verteilten Netzwerk bietet mehrere Vorteile:

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

  Wenn die Collector-Manager-Instanzen gemeinsam mit Ereignisquellen installiert werden, können Filterung, Verschlüsselung und Datenkomprimierung an der Quelle ausgeführt werden.
- **Datei-Caching:** Der Remote-Collector-Manager kann 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.

3.2 Vor dem Beginn

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 Abschnitt 1.1, „Systemanforderungen und unterstützte Plattformen“, auf Seite 11.

- ❒ 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.

3.3 Installieren eines zusätzlichen Collector-Managers

Der Remote-Collector-Manager darf nicht auf dem System installiert werden, auf dem Sentinel oder die Remote-Correlation Engine installiert sind.

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 dem Titel „Collector-Manager“ 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. Beispiel:

   `cd sentinel_collector_mgr-7.0.0.0.x86_64`
7. Geben Sie folgenden Befehl ein, um den Sentinel-Collector-Manager zu installieren:

   `./install-cm`

   Das Installationsskript prüft zunächst, ob genügend Arbeitsspeicher und Plattenspeicherplatz zur Verfügung stehen. Bei weniger als 1.5 GB verfügbarem Arbeitsspeicher beendet das Skript automatisch die Installation.
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.

    Es kann einige Sekunden dauern, bis das Installationsprogramm Sie zur Auswahl des Konfigurationstyps auffordert.
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.
13. Geben Sie den Benutzernamen und das Passwort für den Collector-Manager an.

Der Benutzername und das Passwort werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

Beispiel:

```
collectormanager=1c51ae55
```

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

14 Akzeptieren Sie das Zertifikat dauerhaft, wenn Sie dazu aufgefordert werden.

Die Installation des Remote-Collector-Managers von Sentinel ist abgeschlossen.

3.4 Hinzufügen eines benutzerdefinierten Benutzers für einen Collector-Manager

Novell empfiehlt die Verwendung des standardmäßigen Collector-Manager-Benutzernamens `collectormanager`. Wenn Sie jedoch mehrere Remote-Collector-Manager-Instanzen installiert haben und diese einzeln identifizieren möchten, können Sie neue Benutzer erstellen:

1 Melden Sie sich am Server mit dem Benutzer an, der Zugriff auf die Installationsdateien für Sentinel hat.

2 Öffnen Sie die Datei `activemqgroups.properties`.

Die Datei befindet sich im Verzeichnis `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/`.

3 Fügen Sie den neuen Collector-Manager-Benutzer im Abschnitt `cm` hinzu. Trennen Sie die einzelnen Einträge mit Kommas. Beispiel:

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

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 Benutzer hinzu.

Das Passwort kann eine beliebige Zufallszeichenkette sein. Beispiel:

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

7 Speichern und schließen Sie die Datei.

8 Starten Sie den Sentinel-Server neu.

4 Installieren zusätzlicher Correlation Engines

Standardmäßig installiert Sentinel eine Correlation Engine. Für Umgebungen mit einer hohen Anzahl an Korrelationsregeln oder sehr hohen Ereignisraten kann es sinnvoll sein, mehrere Correlation Engines zu installieren. Weitere Informationen zu den empfohlenen Ereignisraten pro Correlation Engine finden Sie unter Correlation Engine in Kapitel 1, „Erfüllen der Systemanforderungen“, auf Seite 11.

IMPORTANT: Es ist nicht möglich, auf dem Server, auf dem Sentinel ausgeführt wird, einen weiteren Collector-Manager oder eine weitere Correlation Engine zu installieren.

4.1 Vor dem Beginn

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 Abschnitt 1.1, „Systemanforderungen und unterstützte Plattformen“, auf Seite 11.
- ❒ Synchronisieren Sie die Zeit mit NTP (Network Time Protocol).
- ❒ Eine Correlation Engine erfordert Netzwerkkonnektivität zum Port für den Nachrichtenbus (61616) auf dem Sentinel-Server. Stellen Sie vor der Installation der Correlation Engine sicher, dass alle Firewall- und Netzwerkeinstellungen über diesen Port kommunizieren dürfen.

4.2 Installieren einer zusätzlichen Correlation Engine

Die Remote-Correlation Engine kann nicht auf dem gleichen System installiert werden, auf dem bereits Sentinel oder ein Remote-Collector-Manager installiert ist.

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 dem Titel „Correlation Engine“ 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. Beispiel:

   ```
   cd sentinel_correlation_engine-7.0.0.0.x86_64
   ```
7. Geben Sie folgenden Befehl ein, um die Sentinel-Correlation Engine zu installieren:

   ```
   ./install-ce
   ```

   Das Installationsskript prüft zunächst, ob genügend Arbeitsspeicher und Plattenspeicherplatz zur Verfügung stehen. Bei weniger als 1.5 GB verfügbarem Arbeitsspeicher beendet das Skript automatisch die Installation.
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.
13. Geben Sie den Benutzernamen und das Passwort für die Correlation Engine an.

    Der Benutzername und das Passwort werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

    Beispiel:

    ```
    correlationengine=68790d7a
    ```

    In diesem Beispiel ist `correlationengine` der Benutzername und der entsprechende Wert ist das Passwort.
14. Akzeptieren Sie das Zertifikat dauerhaft, wenn Sie dazu aufgefordert werden.

    Die Installation der Remote-Correlation Engine von Sentinel ist abgeschlossen.

4.3 Hinzufügen eines benutzerdefinierten Benutzers für die Correlation Engine

Novell empfiehlt die Verwendung des standardmäßigen Correlation Engine-Benutzernamens `correlationengine`. Wenn Sie jedoch mehrere Remote-Correlation Engines installiert haben und diese einzeln identifizieren möchten, können Sie neue Benutzer erstellen:

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

   Die Datei befindet sich im Verzeichnis `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/`.
3. Fügen Sie den neuen Correlation Engine-Benutzer im Abschnitt `admin` hinzu. Trennen Sie dabei einzelne Einträge mit einem Komma. 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 Benutzer hinzu.

   Das Passwort kann eine beliebige Zufallszeichenkette sein. Beispiel:

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

5 Installieren der Appliance

Die Sentinel-Appliance ist eine ausführungsbereite, auf SUSE Studio aufgebaute Software-Appliance. Die Appliance vereint ein verstärktes SUSE Linux Enterprise Server (SLES) 11 SP1-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. Die Software-Appliance kann auf der Hardware oder in einer virtuellen Umgebung installiert werden.

5.1 Vor dem Beginn

Vergewissern Sie sich vor der Installation der Appliance, dass folgende Aufgaben abgeschlossen sind.

- ❒ Überprüfen Sie, ob die Hardwareanforderungen erfüllt sind. Weitere Informationen finden Sie unter Abschnitt 1.1, „Systemanforderungen und unterstützte Plattformen“, auf Seite 11.
- ❒ Wenn Sie eine lizenzierte Version installieren möchten, wenden Sie sich an den Novell Kundenservice (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22), um Ihren Lizenzschlüssel zu erhalten.
- ❒ Ihren Registrierungscode, mit dem Sie sich für Softwareaktualisierungen registrieren können, erhalten Sie ebenfalls vom Novell Kundenservice (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22).

5.2 Installieren der VMware-Appliance

5.2.1 Installieren von Sentinel

So importieren und installieren Sie das Sentinel-Appliance-Image auf einem VMware ESX-Server:

1. Laden Sie die Installationsdatei für die VMware-Appliance von der Novell-Download-Website (http://download.novell.com/index.jsp) herunter.

   Die korrekte Datei für die VMware-Appliance enthält `vmx` im Dateinamen. Beispiel: `sentinel_server_7.0.0.0.x86_64.vmx.tar.gz`
2. Richten Sie eine ESX-Datenablage ein, auf der das Appliance-Image installiert werden kann.
3. Melden Sie sich als Administrator an dem Server an, auf dem Sie die Appliance installieren möchten.
4. Extrahieren Sie mit folgendem Befehl das komprimierte Appliance-Image vom Computer, auf dem VM Converter installiert ist:

   ```
   tar zxvf <install_file>
   ```

   Ersetzen Sie <*install_file*> durch den tatsächlichen Dateinamen.
5. Um das VMware-Image auf den ESX-Server zu importieren, verwenden Sie den VMware Converter und folgen Sie den Anweisungen auf dem Bildschirm des Installationsassistenten.
6. Melden Sie sich am ESX-Server an.
7. Wählen Sie das importierte VMware-Image der Appliance und klicken Sie auf das Symbol *Einschalten*.
8. Wählen Sie die gewünschte Sprache aus und klicken Sie auf *Weiter*.
9. Wählen Sie das Tastatur-Layout aus und klicken Sie auf *Weiter*.
10. Lesen und akzeptieren Sie die Software-Lizenzvereinbarung für SUSE Linux Enterprise Server (SLES) 11 SP1.
11. Lesen und akzeptieren Sie die NetIQ Sentinel-Endbenutzer-Lizenzvereinbarung.
12. Geben Sie auf der Seite mit dem Hostnamen bzw. Domänennamen die entsprechenden Namen ein und stellen Sie sicher, dass die Option *Hostname zur Loopback-ID zuweisen* ausgewählt ist.
13. Klicken Sie auf *Weiter*. Die Konfigurationen für den Hostnamen werden gespeichert.
14. Führen Sie einen der folgenden Vorgänge 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.
15. 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
    ```
16. 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.

17 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.

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

19 Fahren Sie mit Abschnitt 5.5, „Konfiguration der Appliance im Anschluss an die Installation“, auf Seite 52 fort.

5.2.2 Installieren des Collector-Managers

So importieren und installieren Sie das Appliance-Image auf dem VMware ESX-Server:

1 Laden Sie die Installationsdatei für die VMware-Appliance von der Novell-Download-Website (http://download.novell.com/index.jsp) herunter.

Die korrekte Datei für die VMware-Appliance enthält `vmx` im Dateinamen. Beispiel: `sentinel_colletor_manager_7.0.0.0.x86_64.vmx.tar.gz`

2 Richten Sie eine ESX-Datenablage ein, auf der das Appliance-Image installiert werden kann.

3 Melden Sie sich als Administrator an dem Server an, auf dem Sie die Appliance installieren möchten.

4 Extrahieren Sie mit folgendem Befehl das komprimierte Appliance-Image vom Computer, auf dem VM Converter installiert ist:

```
tar zxvf <install_file>
```

Ersetzen Sie *<install_file>* durch den tatsächlichen Dateinamen.

5 Um das VMware-Image auf den ESX-Server zu importieren, verwenden Sie den VMware Converter und folgen Sie den Anweisungen auf dem Bildschirm des Installationsassistenten.

6 Melden Sie sich am ESX-Server an.

7 Wählen Sie das importierte VMware-Image der Appliance und klicken Sie auf das Symbol *Einschalten*.

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

9 Geben Sie die Portnummer des Communication Server an. Der Standardport für den Nachrichtenbus ist `61616`.

10 Geben Sie den JMS-Benutzernamen an, der den Collector-Manager-Benutzernamen darstellt. Der Standardbenutzername ist `collectormanager`.

11 Geben Sie das Passwort für den JMS-Benutzer an.

Der Benutzername und das Passwort werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

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

```
collectormanager=<password>
```

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

13 Klicken Sie auf *Weiter*.

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

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

Nach dem Abschluss der Installation wird eine Meldung angezeigt, die darauf hinweist, dass diese Appliance der Sentinel-Collector-Manager ist. Die Meldung enthält außerdem die IP-Adresse. Sie zeigt auch die IP-Adresse der Sentinel-Server-Benutzeroberfläche an.

5.2.3 Installieren der Correlation Engine

Die Installation der Correlation Engine-Appliance erfolgt auf ähnliche Weise wie die Installation der Collector-Manager-Appliance.

1 Laden Sie die Installationsdatei für die VMware-Appliance von der Novell-Download-Website (http://download.novell.com/index.jsp) herunter.

Die korrekte Datei für die VMware-Correlation Engine-Appliance enthält `vmx` im Dateinamen. Beispiel: `sentinel_correlation_engine_7.0.0.0.x86_64.vmx.tar.gz`

2 Richten Sie eine ESX-Datenablage ein, auf der das Appliance-Image installiert werden kann.

3 Melden Sie sich als Administrator an dem Server an, auf dem Sie die Appliance installieren möchten.

4 Geben Sie den folgenden Befehl ein, um das komprimierte Appliance-Image von dem Computer, auf dem VM Converter installiert ist, zu extrahieren:

```
tar zxvf <install_file>
```

Ersetzen Sie <*install_file*> durch den tatsächlichen Dateinamen.

5 Um das VMware-Image auf den ESX-Server zu importieren, verwenden Sie den VMware Converter und folgen Sie den Anweisungen auf dem Bildschirm des Installationsassistenten.

6 Melden Sie sich am ESX-Server an.

7 Wählen Sie das importierte VMware-Image der Appliance und klicken Sie auf das Symbol *Einschalten*.

8 Geben Sie den Hostnamen/die IP-Adresse des Sentinel-Servers an, mit dem die Correlation Engine eine Verbindung herstellen soll.

9 Geben Sie die Portnummer des Communication Server an. Der Standardport für den Nachrichtenbus ist `61616`.

10 Geben Sie den JMS-Benutzernamen an, der den Correlation Engine-Benutzernamen darstellt. Der Standardbenutzername ist `correlationengine`.

11 Geben Sie das Passwort für den JMS-Benutzer an.

Der Benutzername und das Passwort werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

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

```
correlationengine=<password>
```

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

13 Klicken Sie auf *Weiter*.

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

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

Nach dem Abschluss der Installation wird eine Meldung angezeigt, die darauf hinweist, dass diese Appliance die Sentinel-Correlation Engine ist. Die Meldung enthält außerdem die IP-Adresse. Sie zeigt auch die IP-Adresse der Sentinel-Server-Benutzeroberfläche an.

5.3 Installieren der Xen-Appliance

5.3.1 Installieren von Sentinel

1 Laden Sie die Installationsdatei für die virtuelle Xen-Appliance von der Novell-Download-Website (http://download.novell.com/index.jsp) in das Verzeichnis `/var/lib/xen/images` herunter.

Der korrekte Dateiname für die virtuelle Xen-Appliance enthält die Buchstaben `xen`. Beispiel: `Sentinel_7.0.0.0.x86_64.xen.tar.gz`

2 Geben Sie den folgenden Befehl ein, um die Datei zu entpacken:

```
tar -zxvf <install_file>
```

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

3 Wechseln Sie zum neuen Installationsverzeichnis. Dieses Verzeichnis enthält folgende Dateien:

- *<dateiname>*`.raw`
- *<dateiname>*`.xenconfig`

4 Öffnen Sie die Datei *<file_name>*`.xenconfig` in einem Texteditor.

5 Ändern Sie die Datei wie folgt:

- Geben Sie den vollständigen Pfad zur `.raw`-Datei in der Einstellung `Datenträger` ein.
- Geben Sie die Bridge-Einstellung für Ihre Netzwerkkonfiguration an. Beispiel: `"bridge=br0"` oder `"bridge=xenbr0"`.
- Geben Sie Werte für die Einstellungen `name` und `memory` ein.

Beispiel:

```
# -*- mode: python; -*-
name="Sentinel_7.0.0.0.x86_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/sentinel_7.0.0.0.x86_64/
sentinel_7.0.0.0.x86_64.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```

6 Nachdem Sie die Datei `<filename>.xenconfig` geändert haben, geben Sie folgenden Befehl ein, um die virtuelle Maschine (VM) zu erstellen:

```
xm create <file_name>.xenconfig
```

7 (Optional) Geben Sie folgenden Befehl ein, um zu überprüfen, ob die virtuelle Maschine erstellt wurde:

```
xm list
```

Die VM wird in der generierten Liste angezeigt.

Wenn Sie z. B. `name="Sentinel_7.0.0.0.x86_64"` in der Datei `.xenconfig` konfiguriert haben, wird die VM mit diesem Namen angezeigt.

8 Geben Sie den folgenden Befehl ein, um die Installation zu starten:

```
xm console <vm name>
```

Ersetzen Sie *<vm_name>* mit dem in der Namenseinstellung der Datei `.xenconfig` festgelegten Namen. Dieser entspricht außerdem dem in Schritt 7 zurückgegebenen Wert. Beispiel:

```
xm console Sentinel_7.0.0.0.x86_64
```

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.

9 Wählen Sie die gewünschte Sprache aus und klicken Sie auf *Weiter*.

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

11 Lesen und akzeptieren Sie die Software-Lizenzvereinbarung für SUSE Linux Enterprise Server (SLES) 11 SP1.

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

13 Geben Sie auf der Seite mit dem Hostnamen bzw. Domänennamen die entsprechenden Namen ein und stellen Sie sicher, dass die Option *Hostname zur Loopback-ID zuweisen* ausgewählt ist.

14 Wählen Sie *Weiter*. Die Konfigurationen für den Hostnamen werden gespeichert.

15 Führen Sie einen der folgenden Vorgänge 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, wählen Sie *Ändern* aus und nehmen Sie die gewünschten Änderungen vor.

16 Wählen Sie *Weiter*. Die Netzwerkeinstellungen werden gespeichert.

17 Legen Sie Uhrzeit und Datum fest, klicken Sie auf *Weiter* und anschließend auf *Fertig stellen*

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
```

18 Legen Sie das `root`-Passwort für SUSE Enterprise Server fest und klicken Sie auf *Weiter*.

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

Die Sentinel-Installation wird fortgesetzt und abgeschlossen. 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.

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

20 Fahren Sie mit Abschnitt 5.5, „Konfiguration der Appliance im Anschluss an die Installation“, auf Seite 52 fort.

5.3.2 Installieren des Collector-Managers

Sie können den Collector-Manager als Appliance auf einem Xen-fähigen Linux-System installieren, das die Hardware-Mindestanforderungen für Collector-Manager erfüllt. Weitere Informationen finden Sie unter Abschnitt 1.1.2, „Hardwareanforderungen“, auf Seite 12.

1 Führen Sie Schritt 1 bis Schritt 14 in Abschnitt 5.3.1, „Installieren von Sentinel“, auf Seite 45 aus.

Der korrekte Dateiname für die Installationsdatei der virtuellen Xen-Collector-Manager-Appliance ist `sentinel_collector_manager_7.0.0.0.x86_64.xen.tar.gz`.

2 Wählen Sie auf dem Bildschirm „Netzwerkkonfiguration II“ *Ändern* aus und geben Sie die IP-Adresse der virtuellen Maschine an, auf der die zusätzliche Collector-Manager-Appliance installiert werden soll.

3 Geben Sie die Teilnetzmaske der angegebenen IP-Adresse an.

4 Wählen Sie *Weiter*. Die Netzwerkeinstellungen werden gespeichert.

5 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
```

6 Legen Sie das `root`-Passwort für SUSE Enterprise Server fest und klicken Sie auf *Weiter*.

7 Geben Sie den Hostnamen/die IP-Adresse des Sentinel-Servers an, mit dem die Correlation Engine eine Verbindung herstellen soll.

8 Geben Sie die Portnummer des Communication Server an. Der Standardport für den Nachrichtenbus ist `61616`.

9 Geben Sie den JMS-Benutzernamen an, der den Collector-Manager-Benutzernamen darstellt. Der Standardbenutzername ist `collectormanager`.

10 Geben Sie das Passwort für den JMS-Benutzer an.

Der Benutzername und das Passwort werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

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

```
collectormanager=<password>
```

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

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

Nach dem Abschluss der Installation wird eine Meldung angezeigt, die darauf hinweist, dass diese Appliance der Sentinel-Collector-Manager ist. Die Meldung enthält außerdem die IP-Adresse.

5.3.3 Installieren der Correlation Engine

Sie können die Correlation Engine als Appliance auf einem Xen-fähigen Linux-System installieren, das die Hardware-Mindestanforderungen für Collector-Manager erfüllt. Weitere Informationen finden Sie unter Abschnitt 1.1.2, „Hardwareanforderungen“, auf Seite 12.

1 Führen Sie Schritt 1 bis Schritt 14 in Abschnitt 5.3.1, „Installieren von Sentinel“, auf Seite 45 aus.

Der korrekte Dateiname für die Installationsdatei der virtuellen Xen-Correlation Engine-Appliance ist `sentinel_correlation_engine_7.0.0.0.x86_64.xen.tar.gz`.

2 Wählen Sie auf dem Bildschirm „Netzwerkkonfiguration II“ *Ändern* aus und geben Sie die IP-Adresse der virtuellen Maschine an, auf der die Correlation Engine-Appliance installiert werden soll.

3 Geben Sie die Teilnetzmaske der angegebenen IP-Adresse an.

4 Wählen Sie *Weiter*. Die Netzwerkeinstellungen werden gespeichert.

5 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
```

6 Legen Sie das `root`-Passwort für SUSE Enterprise Server fest und klicken Sie auf *Weiter*.

7 Geben Sie den Hostnamen/die IP-Adresse des Sentinel-Servers an, mit dem die Correlation Engine eine Verbindung herstellen soll.

8 Geben Sie die Portnummer des Communication Server an. Der Standardport für den Nachrichtenbus ist `61616`.

9 Geben Sie den JMS-Benutzernamen an, der den Correlation Engine-Benutzernamen darstellt. Der Standardbenutzername ist `correlationengine`.

10 Geben Sie das Passwort für den JMS-Benutzer an.

11 Klicken Sie auf *Weiter*.

Der Benutzername und das Passwort werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

12 Über folgende Zeile in der Datei `activemqusers.properties` können Sie das Passwort überprüfen:

```
correlationengine=<password>
```

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

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

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

Nach dem Abschluss der Installation wird eine Meldung angezeigt, die darauf hinweist, dass diese Appliance die Sentinel-Correlation Engine ist. Die Meldung enthält außerdem die IP-Adresse. Sie zeigt auch die IP-Adresse der Sentinel-Server-Benutzeroberfläche an.

5.4 Installieren der Appliance auf der Hardware

Stellen Sie vor dem Installieren der Appliance auf der Hardware sicher, dass das Appliance-ISO-Datenträger-Image von der Support-Website heruntergeladen wurde und auf DVD zur Verfügung steht.

IMPORTANT: Für die Installation auf einer Hardware mit dem ISO-Disk-Image (Bare-metal und Hyper-V) sind mindestens 4,5 GB Arbeitsspeicher erforderlich, um die Installation abzuschließen. Weitere Informationen zu den Hardwareanforderungen finden Sie unter Abschnitt 1.1.2, „Hardwareanforderungen“, auf Seite 12.

5.4.1 Installieren von Sentinel

1 Booten Sie den physischen Computer über die DVD im DVD-Laufwerk.

2 Folgen Sie den Bildschirmanweisungen des Installationsassistenten.

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

6 Lesen und akzeptieren Sie die SUSE Enterprise Server Software-Lizenzvereinbarung.

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

8 Wählen Sie *Weiter*.

9 Geben Sie auf der Seite mit dem Hostnamen bzw. Domänennamen die entsprechenden Namen ein und stellen Sie sicher, dass die Option *Hostname zur Loopback-ID zuweisen* ausgewählt ist.

10 Wählen Sie *Weiter* aus. Die Konfigurationen für den Hostnamen werden gespeichert.

11 Führen Sie einen der folgenden Vorgänge 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, wählen Sie *Ändern* aus und nehmen Sie die gewünschten Änderungen vor.

12 Wählen Sie *Weiter*. Die Netzwerkeinstellungen werden gespeichert.

13 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
```

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

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

16 Geben Sie den 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 14 festgelegte Passwort.

17 Stoppen Sie den Sentinel-Server:

```
service sentinel stop
```

18 Geben Sie folgenden Befehl ein, um die Benutzeroberfläche für eine klare Anzeige in YaST zurückzusetzen:

```
reset
```

19 Führen Sie den folgenden Befehl aus, um die Appliance auf dem physischen Server zu installieren:

```
/sbin/yast2 live-installer
```

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.

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

21 Fahren Sie mit Abschnitt 5.5, „Konfiguration der Appliance im Anschluss an die Installation“, auf Seite 52 fort.

5.4.2 Installieren des Collector-Managers

Sie können den Collector-Manager als Appliance auf einem System installieren, das die Hardware-Mindestanforderungen für Collector-Manager erfüllt. Weitere Informationen finden Sie unter Abschnitt 1.1.2, „Hardwareanforderungen“, auf Seite 12.

1 Führen Sie Schritt 1 bis Schritt 14 in Abschnitt 5.4.1, „Installieren von Sentinel“, auf Seite 49 aus.

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 für den Nachrichtenbus ist `61616`.

   Das Installationsskript versucht, mit dem angegebenen Berechtigungsnachweis eine Verbindung zum Server herzustellen. Wenn einer der Werte falsch eingegeben wurde, zeigt die Installation einen Fehler an.

4 Geben Sie den JMS-Benutzernamen an, der den Collector-Manager-Benutzernamen darstellt. Der Standardbenutzername ist `collectormanager`.

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

6 Klicken Sie auf *Weiter*.

   Der Benutzername und das Passwort werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

7 Über folgende Zeile in der Datei `activemqusers.properties` können Sie das Passwort überprüfen:

   ```
   collectormanager=<password>
   ```

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

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

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

   Nach dem Abschluss der Installation wird eine Meldung angezeigt, die darauf hinweist, dass diese Appliance der Sentinel-Collector-Manager ist. Die Meldung enthält außerdem die IP-Adresse. Sie zeigt auch die IP-Adresse der Sentinel-Server-Benutzeroberfläche an.

5.4.3 Installieren der Correlation Engine

Sie können die Correlation Engine als Appliance auf einem System installieren, das die Hardware-Mindestanforderungen für die Correlation Engine erfüllt. Weitere Informationen finden Sie unter Abschnitt 1.1.2, „Hardwareanforderungen“, auf Seite 12.

1 Führen Sie Schritt 1 bis Schritt 14 in Abschnitt 5.4.1, „Installieren von Sentinel“, auf Seite 49 aus.

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

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

4 Geben Sie den JMS-Benutzernamen an, der den Correlation Engine-Benutzernamen darstellt. Der Standardbenutzername ist `correlationengine`.

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

6 Klicken Sie auf *Weiter*.

   Der Benutzername und das Passwort werden in der Datei `/<installationsverzeichnis>/etc/opt/novell/sentinel/config/activemqusers.properties` auf dem Sentinel-Server gespeichert.

7 Über folgende Zeile in der Datei `activemqusers.properties` können Sie das Passwort überprüfen:

   ```
   correlationengine=<password>
   ```

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

8. Akzeptieren Sie das Zertifikat, wenn Sie dazu aufgefordert werden.
9. Klicken Sie auf *Weiter*, um die Installation abzuschließen.

   Nach dem Abschluss der Installation wird eine Meldung angezeigt, die darauf hinweist, dass diese Appliance die Sentinel-Correlation Engine ist. Die Meldung enthält außerdem die IP-Adresse. Sie zeigt auch die IP-Adresse der Sentinel-Server-Benutzeroberfläche an.
10. Fahren Sie mit Abschnitt 5.5, „Konfiguration der Appliance im Anschluss an die Installation“, auf Seite 52 fort.

5.5 Konfiguration der Appliance im Anschluss an die Installation

5.5.1 Installieren der VMware-Tools

Damit Sentinel ordnungsgemäß auf dem VMware-Server funktioniert, müssen Sie die VMware-Tools installieren. VMware-Tools ist eine Dienstprogramm-Suite, die die Betriebssystemleistung der virtuellen Maschine steigert. Auch die Verwaltung der virtuellen Maschine wird verbessert. Weitere Informationen zur Installation von VMware-Tools finden Sie unter VMware Tools for Linux Guests (VMware-Tools für Linux-Gäste) (https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177).

Weitere Informationen zur VMware-Dokumentation finden Sie unter Workstation Users's Manual (Arbeitsstation-Benutzerhandbuch) (http://www.vmware.com/pdf/ws71_manual.pdf).

5.5.2 Anmelden an der Appliance-Weboberfläche

So melden Sie sich an der Appliance-Webkonsole an und initialisieren die Software:

1. Öffnen Sie einen Webbrowser und melden Sie sich bei https://<*IP-Adresse*>:8443 an. 8443 ist der Standardport für den Sentinel-Server. Die Sentinel-Webseite wird angezeigt.

   Die IP-Adresse der Appliance wird in der Appliance-Konsole angezeigt, nachdem die Installation abgeschlossen und der Server neu gestartet wurde.
2. Konfigurieren Sie die Sentinel Appliance für die Datenspeicherung und die Datensammlung.

   Weitere Informationen zum Konfigurieren der Appliance finden Sie im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.
3. Registrieren Sie sich zum Erhalt der Aktualisierungen.

   Weitere Informationen finden Sie unter Abschnitt 5.9, „Registrieren für Aktualisierungen“, auf Seite 54.

5.6 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 5.9, „Registrieren für Aktualisierungen“, auf Seite 54 beschrieben zum Empfang von Aktualisierungen.
4. Klicken Sie auf *Weiter*, um die Ersteinrichtung fertig zu stellen.

5.7 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 Novell Customer Center integriert ist und Kernfunktionen des Novell Customer Centers zur Verfügung stellt.

5.7.1 Voraussetzungen

- Besorgen Sie die Anmeldedaten für das Novell Customer Center, damit Sentinel Aktualisierungen von Novell abrufen kann. Weitere Informationen zum Erhalt der Anmeldedaten erhalten Sie vom Novell Support (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup).
- Stellen Sie sicher, dass SLES 11 SP1 mit folgenden Paketen auf dem Computer installiert ist, auf dem SMT installiert werden soll:
  - htmldoc
  - smt
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - pertl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - smt-support
  - yast2-smt
  - yum-metadata-parser
  - createrepo
  - sle-smt-release-cd
  - sle-smt_en
  - 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 (http://www.novell.com/documentation/smt11/).
  - 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.

5.7.2 Konfigurieren der Appliance

Informationen zur Konfiguration der Appliance mit SMT finden Sie im Abschnitt „Configuring Clients to Use SMT“ (Konfigurieren von Clients zur Verwendung von SMT) (http://www.novell.com/documentation/smt11/smt_sle_11_guide/?page=/documentation/smt11/smt_sle_11_guide/data/smt_client.html) in der Subscription Management Tool-Dokumentation.

5.8 Stoppen und Starten des Servers über die Weboberfläche

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“).

5.9 Registrieren für Aktualisierungen

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*.

6 Fehlersuche zur Installation

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

6.1 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.

6.2 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.

7 Weitere Schritte

Um Sie nach der Installation bei der Konfiguration von Sentinel zu unterstützen, stehen Ihnen zwei Handbücher zur Verfügung: *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)* und *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

Das Administrationshandbuch enthält Informationen zu Konfigurationsaufgaben, die nur von einem Benutzer mit Administratorrechten ausgeführt werden können. Beispiel:

- "Konfigurieren von Benutzern und Rollen"
- "Konfigurieren der Datenspeicherung"
- "Konfigurieren der Datenerfassung"
- "Ereignissuche und -berichterstellung in einer verteilten Umgebung"

Weitere Informationen zu diesen und anderen Administrationsaufgaben finden Sie im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.

Das Benutzerhandbuch enthält Anleitungen zu Aufgaben, die von Benutzern in Sentinel ausgeführt werden können. Beispiel:

- "Suchen von Ereignissen"
- "Analysieren von Datentrends"
- "Berichterstellung"
- "Konfigurieren von Vorfällen"

Weitere Informationen zu diesen und anderen Benutzeraufgaben finden Sie im *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

Die Konfigurationsmöglichkeiten in Sentinel umfassen unter anderem die Ereignisanalyse, das Hinzufügen von Daten anhand von Korrelationsregeln, das Erstellen von Grundwerten und die Konfiguration von Workflows. Die Informationen im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)* unterstützen Sie bei der Konfiguration dieser Sentinel-Funktionen.

II Konfigurieren

Nach der Installation können Sie Sentinel für die Ausführung in Ihrer Umgebung konfigurieren.

8 Zugriff auf die Sentinel-Weboberfläche

Nach der Installation von Sentinel können Sie sich an der Sentinel-Weboberfläche anmelden, um Verwaltungsaufgaben auszuführen und Sentinel zum Erfassen von Daten zu konfigurieren.

1. Öffnen Sie einen Webbrowser und melden Sie sich bei https://<*IP-Adresse*>:8443 an. 8443 ist der Standardport für den Sentinel-Server.
2. (Bedingt) Akzeptieren Sie beim ersten Anmelden in Sentinel das Zertifikat, wenn Sie dazu aufgefordert werden.

   Sobald Sie das Zertifikat akzeptieren, wird die Sentinel-Anmeldeseite angezeigt.
3. Geben Sie den Benutzernamen und das Passwort für den Sentinel-Administrator ein.
4. Klicken Sie auf *Anmelden*.

   Die NetIQ Sentinel-Weboberfläche wird angezeigt.

9 Hinzufügen zusätzlicher Sentinel-Komponenten

Standardmäßig sind in Sentinel ein Syslog-Connector und -Collector installiert und konfiguriert, sowie verschiedene Audit- und Novell-Produkt-Connectors. In den folgenden Abschnitten erhalten Sie Anweisungen zur Installation und Konfiguration zusätzlicher Connectors und Collectors.

9.1 Installieren von Collectors und Connectors

Standardmäßig werden alle herausgegebenen Collectors und Connectors bei der Installation von Sentinel 7 installiert. Wenn nach Sentinel 7 ein neuer Collector oder Collector herausgegeben wird, müssen Sie zunächst die Collector- bzw. Connector-Dateien installieren, bevor Sie den Collector oder Connector konfigurieren können.

9.1.1 Installieren eines Collectors

1. Laden Sie den richtigen Collector von der Sentinel-Plugins-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) 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 Sentinel-Plugins-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.1.2 Installieren eines Connectors

1. Laden Sie den richtigen Connector von der Sentinel-Plugins-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) 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 Sentinel-Plugins-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2 Hinzufügen zusätzlicher Collectors und Connectors

9.2.1 Hinzufügen zusätzlicher Collectors

Sie können zusätzliche Collectors hinzufügen, um Daten aus anderen Quellen zu normalisieren.

1. Melden Sie sich unter https://<*IP-Adresse*>:8443 bei der Sentinel-Weboberfläche an. 8443 ist der Standardport für den Sentinel-Server.
2. Klicken Sie in der Symbolleiste auf *Anwendung* und klicken Sie dann auf *Anwendungen*.
3. Klicken Sie auf *Control Center starten*, um das Sentinel Control Center zu starten.
4. Klicken Sie in der Symbolleiste auf *Ereignisquellenverwaltung* > *Live-Ansicht*.
5. Klicken Sie mit der rechten Maustaste auf den Collector-Manager und klicken Sie dann auf *Collector hinzufügen*.
6. Wählen Sie den Collector aus der Spalte *Hersteller* aus und klicken Sie auf *Weiter*.
7. Die Felder sind je nach Collector unterschiedlich. Befolgen Sie ab diesem Punkt die Collector-spezifische Dokumentation zur Konfiguration des Collectors.

   Die Collector-Dokumentation finden Sie auf der Sentinel-Plugin-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2.2 Hinzufügen zusätzlicher Connectors

Sie können zusätzliche Connectors hinzufügen, um Informationen von anderen Quellen zu erfassen.

1. Melden Sie sich unter https://<*IP-Adresse*>:8443 bei der Sentinel-Weboberfläche an. 8443 ist der Standardport für den Sentinel-Server.
2. Klicken Sie in der Symbolleiste auf *Anwendung* und klicken Sie dann auf *Anwendungen*.
3. Klicken Sie auf *Control Center starten*, um das Sentinel Control Center zu starten.
4. Wählen Sie in der Symbolleiste *Ereignisquellenverwaltung* > *Live-Ansicht* aus.
5. Klicken Sie mit der rechten Maustaste auf den Collector, zu dem der zusätzliche Connector hinzugefügt werden soll. Klicken Sie dann auf *Connector hinzufügen*.
6. Wählen Sie den gewünschten Connector aus der Spalte *Name* aus und klicken Sie auf *Weiter*.
7. Die Felder sind je nach Connector unterschiedlich. Befolgen Sie ab diesem Punkt die Connector-spezifische Dokumentation zur Konfiguration des Connectors.

   Die Connector-Dokumentation finden Sie auf der Sentinel-Plugin-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

10 Verwalten von Daten

10.1 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`.
- Ausführbaren Programme und Bibliotheken befinden sich in folgenden Verzeichnissen:
  - `/opt/novell/sentinel/bin`
  - `/opt/novell/sentinel/setup`
  - `/opt/novell/sentinel/3rdparty`
- 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.

10.2 Hinweise zur Speicherung

Achten Sie für die Speicherung der Sentinel-Datendateien darauf, dass diese auf einer anderen Partition als die ausführbaren Dateien, Konfigurationsdateien und Betriebssystemdateien gespeichert werden. Das getrennte Speichern der Daten erleichtert das Imaging eines Dateisatzes und die Wiederherstellung, falls Dateien beschädigt werden. Außerdem verbessert es die allgemeine Leistung in Systemen, in denen kleinere Dateisysteme effizienter sind. Weitere Informationen finden Sie unter “Disk partitioning (Festplattenpartitionierung)” (http://en.wikipedia.org/wiki/Disk_partitioning#Benefits_of_multiple_partitions).

Wie Sie Sentinel auf mehreren bzw. einer einzelnen Partition installieren können, hängt davon ab, welche der folgenden Installationsarten Sie anwenden:

- Eigenständige Installation
- Appliance-Installation

10.2.1 Partitionen in einer eigenständigen Installation

Wenn Sie Sentinel als eigenständige Installation installieren, können Sie das Partitionslayout des Betriebssystems vor der Sentinel-Installation ändern. Der Administrator muss hierzu die gewünschten Partitionen erstellen und in den entsprechenden Verzeichnissen einhängen. Beachten Sie hierzu die in Abschnitt 10.1, „Verzeichnisstruktur“, auf Seite 69 detailliert dargestellte Verzeichnisstruktur. Beim Ausführen des Installationsprogramms wird Sentinel in die vorerstellten Verzeichnisse installiert. Die sich daraus ergebende Installation erstreckt sich über mehrere Partitionen.

NOTE:

- Beim Ausführen des Installationsprogramms können Sie mit der Option `--location` einen anderen Standort 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`.

10.2.2 Partitionen in einer Appliance-Installation

Wenn Sie Sentinel mit einer Appliance-Installation installieren, können Sie das Betriebssystem nicht vor der Sentinel-Installation neu konfigurieren, da es zusammen mit Sentinel installiert wird. Sie können jedoch mit dem YaST-Tool eine Partition in der Appliance hinzufügen und ein Verzeichnis in die neue Partition verschieben.

Mit der folgenden Prozedur können Sie eine neue Partition erstellen und die Datendateien aus ihrem Verzeichnis zur neu erstellten Partition 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.
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 Wechseln Sie zum `root`-Benutzer.

13 Führen Sie den folgenden Befehl aus, um die Sentinel-Appliance neu zu starten:

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

11 Konfigurieren einsatzbereiter Inhalte

Sentinel enthält eine Vielzahl nützlicher, einsatzbereiter Inhalte, die Sie sofort anwenden können, um verschiedenste Analyseanforderungen zu erfüllen. Ein Großteil der Inhalte ist in einem vorinstallierten Sentinel Core-Lösungspaket enthalten. Weitere Informationen finden Sie im Abschnitt "Using Solution Packs" (Verwenden von Lösungspaketen) im *NetIQ Sentinel 7.0.1 Administration Guide* (NetIQ Sentinel 7.0.1-Administrationshandbuch).

Das Lösungspaket ermöglicht das Einteilen und Gruppieren von Inhalten in Steuerelemente oder Richtliniensätze, die als Einheit behandelt werden. Die Steuerelemente des Sentinel Core-Lösungspakets sind vorinstalliert, um Ihnen einsatzbereiten Inhalte zur Verfügung zu stellen. Sie müssen diese Steuerelemente jedoch implementieren bzw. über die Sentinel-Weboberfläche testen.

Wenn Sie das ordnungsgemäße Funktionieren der Sentinel-Bereitstellung etwas strenger überprüfen möchten, können Sie hierzu den formellen Bescheinigungsvorgang nutzen, der in den Lösungspaketen enthalten ist. Der Bescheinigungsvorgang implementiert die Sentinel Core-Steuerelemente 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 Bescheinigungsvorgang über den Solution Manager ausführen. Weitere Informationen zur Implementierung und zum Testen der Steuerelemente finden Sie unter "Installing and Managing Solution Packs" (Installieren und Verwalten von Lösungspaketen) im *NetIQ Sentinel 7.0.1 Administration Guide* (NetIQ Sentinel 7.0.1-Administrationshandbuch).

12 Konfigurieren der Zeit

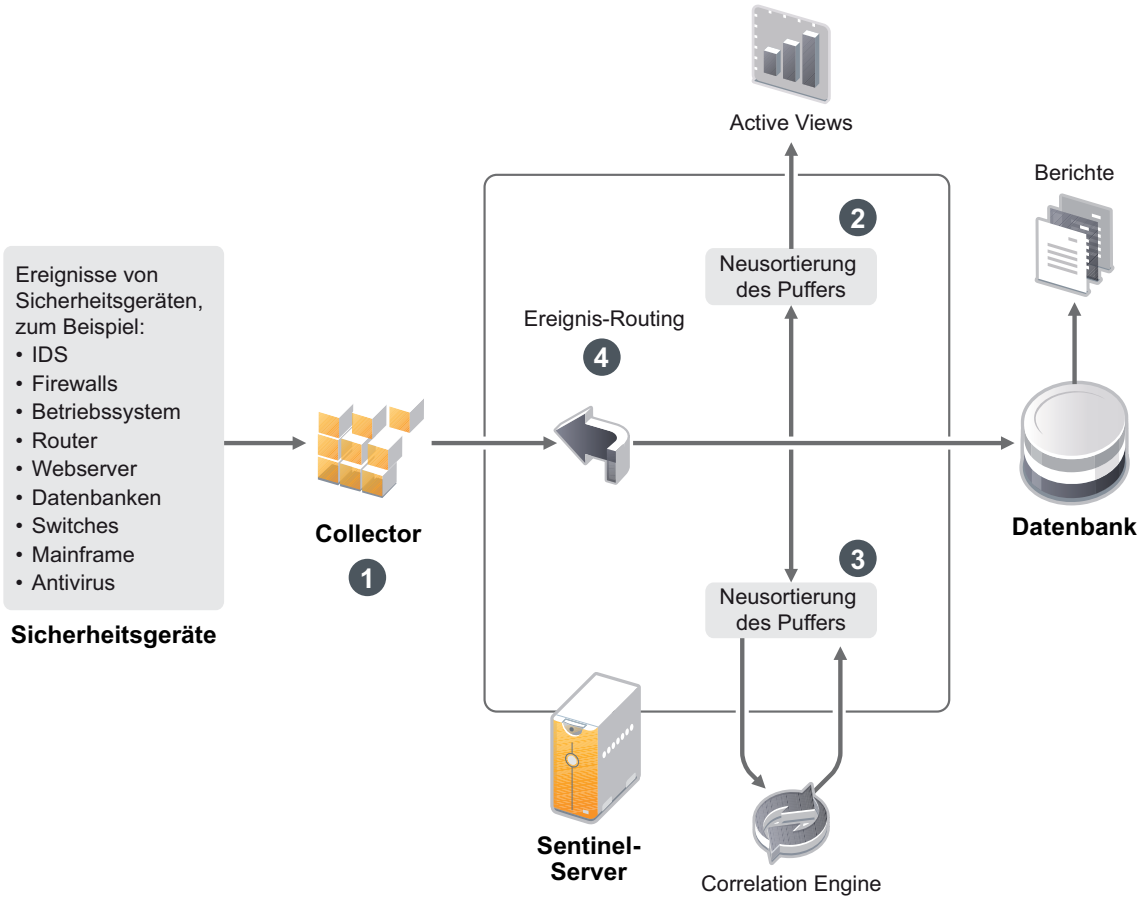
Die Uhrzeit eines Ereignisses ist für seine Verarbeitung in Sentinel von ausgesprochen großer Bedeutung. Sie spielt für Berichterstellung und Revision sowie für die Echtzeitverarbeitung eine wichtige Rolle.

12.1 Zeit in Sentinel

Sentinel ist ein verteiltes System und umfasst mehrere Vorgänge, die sich in unterschiedlichen Teilen des Netzwerks befinden können. Zudem kann es durch das Gerät zu einer gewissen Verzögerung kommen. Aus diesem Grund ordnen die Sentinel-Vorgänge die Ereignisse vor der Verarbeitung nach der Uhrzeit neu an.

Die folgende Abbildung erläutert, wie Sentinel hierzu vorgeht:

Abbildung 12-1 *Sentinel-Zeit*



1. Standardmäßig wird die Ereigniszeit auf die Collector-Manager-Zeit festgelegt. Die ideale Zeit ist die Gerätezeit. Folglich ist es am besten, die Ereigniszeit auf die Gerätezeit einzustellen, wenn die Gerätezeit verfügbar und präzise ist und vom Collector vorschriftsmäßig analysiert wird.
2. Ereignisse werden in 30-Sekunden-Intervallen für die Anzeige in Active Views sortiert. Standardmäßig werden Ereignisse, deren Zeitstempel innerhalb eines Zeitraums von 5 Minuten von der Serverzeit (in der Vergangenheit oder Zukunft) liegt, normal verarbeitet. Ereignisse, deren Zeitstempel mehr als 5 Minuten in der Zukunft liegen, werden in den Active Views nicht angezeigt, jedoch in den Ereignisspeicher eingefügt. Ereignisse, deren Zeitstempel zwischen 5 Minuten und 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. 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-Zeit (richtige Zeit), werden die Ereignisse direkt an den Ereignisspeicher weitergeleitet.

12.2 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 "Accessing Event Source Management (Zugriff auf die Ereignisquellenverwaltung)" im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-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*.

12.3 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.

Das zweite Szenario ist aus vielen Gesichtspunkten das einfachste. Wenn die Zeitzone im langen Format oder als Abweichung angegeben wird, kann die Zeit sehr einfach in UTC-Zeit umgerechnet werden (in „DeviceEventTime“ gespeichert). Auch die Ortszeit für die ObserverTZ-Felder kann auf einfache Weise errechnet werden. Bei der Verwendung von kurzen Zeitzonen-IDs können gegebenenfalls Konflikte auftreten.

Das dritte Szenario ist unter Umständen am kompliziertesten, da der Administrator die Ereignisquellenzeitzone manuell für alle betroffenen Quellen festlegen muss, 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.

13 Lizenzinformationen

Dieser Abschnitt enthält eine Beschreibung der verschiedenen Sentinel-Lizenzen sowie Informationen zur Verwaltung dieser Lizenzen.

13.1 Über Sentinel-Lizenzen

Für Sentinel stehen verschiedene Lizenzen zur Verfügung. Standardmäßig wird Sentinel mit der Probelizenz zur Verfügung gestellt.

13.1.1 Probelizenz

Mit der Sentinel-Standardlizenz können Sie alle Unternehmensfunktionen von Sentinel während des Evaluierungszeitraums von 90 Tagen nutzen. Bei einem System, das mit der Probelizenz ausgeführt wird, enthält die Weboberfläche einen Hinweis dazu, dass ein temporärer Lizenzschlüssel verwendet wird. Außerdem werden die Anzahl der verbleibenden Tage bis zum Ablauf der Funktionen und ein Hinweis zur Aufrüstung auf eine volle Lizenz angezeigt.

NOTE: Das Ablaufdatum des Systems bezieht sich auf die ältesten Daten im System. Wenn Sie alte Ereignisse im System wiederherstellen, wird das Ablaufdatum entsprechend angepasst.

Nach dem 90-Tage-Evaluierungszeitraum wird ein Großteil der Funktionen deaktiviert. Sie können sich jedoch weiterhin anmelden und das System für die Verwendung mit einem Unternehmenslizenzschlüssel aktualisieren.

Nach der Aufrüstung auf eine Unternehmenslizenz werden sämtliche Funktionen wiederhergestellt. Um eine Unterbrechung der Funktionen zu vermeiden, muss das System vor dem Ablaufdatum auf eine Unternehmenslizenz aufrüsten.

13.1.2 Unternehmenslizenzen

Beim Kauf von Sentinel erhalten Sie über das Kundenportal einen Lizenzschlüssel. Je nach dem Umfang der erworbenen Funktionen aktiviert der Lizenzschlüssel bestimmte Funktionen, Datenerfassungsraten 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. Informationen über das Hinzufügen des Lizenzschlüssels zum System finden Sie in Abschnitt 13.2.1, „Hinzufügen eines Lizenzschlüssels über die Weboberfläche“, auf Seite 80.

13.2 Hinzufügen eines Lizenzschlüssels

NOTE: Für das Hinzufügen, Anzeigen oder Löschen einer Lizenz sind Administratorberechtigungen erforderlich.

Sie können einen Lizenzschlüssel entweder über die Weboberfläche oder über die Befehlszeile hinzufügen.

- Abschnitt 13.2.1, „Hinzufügen eines Lizenzschlüssels über die Weboberfläche“, auf Seite 80
- Abschnitt 13.2.2, „Hinzufügen eines Lizenzschlüssels über die Befehlszeile“, auf Seite 80

13.2.1 Hinzufügen eines Lizenzschlüssels über die Weboberfläche

1. Melden Sie sich als Administrator bei der Sentinel-Weboberfläche an.
2. Klicken Sie in der linken oberen Ecke der Seite auf den Link *Info*.
3. Klicken Sie auf die Registerkarte *Lizenzen*.
4. Klicken Sie im Abschnitt „Lizenzen“ auf *Lizenz hinzufügen*.
5. Geben Sie den Lizenzschlüssel im Feld *Schlüssel* an. Nach der Angabe der Lizenz werden folgende Informationen im Vorschau-Abschnitt angezeigt:

   Funktionen: Die mit der Lizenz verfügbaren Funktionen.

   Hostname: Dieses Feld dient ausschließlich NetIQ-internen Zwecken.

   Seriennummer: Dieses Feld dient ausschließlich NetIQ-internen Zwecken.

   EPS: Im Lizenzschlüssel enthaltene Ereignisrate. Wenn die Rate überschritten wird, generiert Sentinel Warnmeldungen, erfasst jedoch weiterhin Daten.

   Läuft ab: Ablaufdatum der Lizenz. Um eine Unterbrechung der Funktionen zu vermeiden, müssen Sie vor dem Ablaufdatum einen gültigen Lizenzschlüssel eingeben.
6. Klicken Sie auf *Speichern*.

13.2.2 Hinzufügen eines Lizenzschlüssels über die Befehlszeile

Sie können die Lizenz über die Befehlszeile mit dem Skript `softwarekey.sh` hinzufügen.

1. Melden Sie sich beim Sentinel-Server als `root` an.
2. Wechseln Sie in das Verzeichnis `/opt/novell/sentinel/bin`.

3 Geben Sie folgenden Befehl ein, um zum Benutzer „novell“ zu wechseln:

```
su novell
```

4 Geben Sie folgenden Befehl an, um das Skript `softwarekey.sh` auszuführen.

```
./softwarekey.sh
```

5 Geben Sie „1“ ein, um den Lizenzschlüssel einzufügen.

6 Geben Sie den Lizenzschlüssel ein und drücken Sie die Eingabetaste.

14 Konfigurieren von Sentinel für Hochverfügbarkeitssysteme

Sentinel wurde für die Arbeit in Hochverfügbarkeitsumgebungen getestet und zertifiziert und unterstützt Disaster Recovery-Architekturen. NetIQ Consulting und NetIQ-Partner können Sie bei der Implementierung von Sentinel in Hochverfügbarkeitsumgebungen und von Disaster Recovery-Funktionen unterstützen.

Um Sentinel-Server für eine hohe Verfügbarkeit zu konfigurieren, ist Folgendes erforderlich:

- Redundante, als Cluster gruppierte Sentinel-Knoten.
- Zugriff auf einen gemeinsamen Datenspeicher.
- Virtuelle IP-Adressen für ein transparentes Umschalten von einem ausgefallenen auf einen anderen Knoten.
- Skripte zum Starten, Stoppen und Überwachen der Anwendung, die auf den für Ihre Cluster-Lösung festgelegten Richtlinien basieren. Sie können Cluster-Lösungen wie Cluster Resource Agents oder LSB-Initialisierungsskripts auf Linux-Hochverfügbarkeitssystemen verwenden.

Auf dem Markt sind viele Pakete verfügbar, die ein Hochverfügbarkeitssystem ermöglichen. Die Sentinel-Tests wurden mit der *SUSE Linux Enterprise High Availability (HA)-Erweiterung* (http://www.novell.com/products/highavailability/), RAID-Festplatten für gemeinsamen Speicher und benutzerdefinierten Skripten ausgeführt. Diese Architektur kann über Datenzentren repliziert werden, um die Verfügbarkeit aller Komponenten vom Sentinel-Server bis zu den Collector-Manager-Instanzen und Collectors zu gewährleisten.

Hochverfügbarkeitslösungen für Ereignisquellen sollten fallweise betrachtet werden, da eine breite Vielfalt an Geräten verwendet werden kann.

III Aufrüsten von Sentinel

15 Aufrüsten des Sentinel-Servers

1. Erstellen Sie eine Sicherung der Konfiguration und anschließend einen ESM-Export.

   Weitere Informationen zum Sichern von Daten finden Sie unter “Backup and Restoring Data” (Sichern und Wiederherstellen von Daten) im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.
2. Laden Sie das aktuellste Installationsprogramm von der Novell-Download-Website (http://download.novell.com) herunter.
3. Melden Sie sich am Server, auf dem Sentinel aufgerüstet werden soll, als `root` an.
4. Geben Sie den folgenden Befehl an, um die Installationsdateien aus der TAR-Datei zu extrahieren:

   ```
   tar xfz <install_filename>
   ```

   Ersetzen Sie *<install_filename>* durch den tatsächlichen Namen der Installationsdatei.
5. Wechseln Sie in das Verzeichnis, in das die Installationsdatei extrahiert wurde.
6. Geben Sie folgenden Befehl ein, um Sentinel aufzurüsten:

   ```
   ./install-sentinel
   ```
7. 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.
8. Lesen Sie die Endbenutzer-Lizenzvereinbarung, geben Sie `ja` oder `j` ein, um die Lizenzbedingungen zu akzeptieren, und setzen Sie die Installation fort.
9. Das Installationsskript erkennt, dass bereits eine ältere Produktversion vorhanden ist, und fordert Sie auf, anzugeben, ob Sie das Produkt aufrüsten möchten. Wenn Sie "n" drücken, wird die Installation beendet. Zum Fortsetzen der Aufrüstung drücken Sie "j".

   Die Installation wird gestartet. Zunächst werden alle RPM-Pakete installiert. Diese Installation kann einige Sekunden dauern.
10. (Bedingt) Zum Aufrüsten von Collector-Manager-Systemen siehe Kapitel 17, „Aktualisieren des Collector-Managers“, auf Seite 91.
11. (Bedingt) Zum Aufrüsten des Correlation Engine-Systems siehe Kapitel 18, „Aufrüsten der Correlation Engine“, auf Seite 93.

16 Aufrüsten der Sentinel-Appliance

Die Prozedur führt Sie durch die Aufrüstung der Sentinel-Appliance und der Collector-Manager- und Correlation Engine-Appliances.

1. Melden Sie sich an der Sentinel-Appliance als Benutzer mit Verwalterfunktion an.
2. ***Wenn Sie die Sentinel-Appliance aufrüsten möchten***, klicken Sie auf *Appliance*, um WebYaST zu starten.
3. ***Wenn Sie eine Collector-Manager- oder Correlation Engine-Appliance aufrüsten möchten***, geben Sie unter Verwendung von Port 54984 die URL des Computers an, auf dem der Collector-Manager bzw. die Correlation Engine ausgeführt wird, um WebYaST zu starten.
4. Erstellen Sie eine Sicherung der Konfiguration und anschließend einen ESM-Export.

   Weitere Informationen zum Sichern von Daten finden Sie unter "Backup and Restoring Data" (Sichern und Wiederherstellen von Daten). im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.
5. (Bedingt) Wenn Sie die Appliance noch nicht für automatische Aktualisierungen registriert haben, registrieren Sie sie jetzt.

   Weitere Informationen finden Sie unter Abschnitt 5.9, „Registrieren für Aktualisierungen“, auf Seite 54.

   Wenn die Appliance nicht registriert ist, wird eine gelbe Warnmeldung angezeigt, die auf diesen Zustand hinweist.
6. Klicken Sie auf *Aktualisieren*, um zu überprüfen, ob Aktualisierungen vorhanden sind.

   Die verfügbaren Aktualisierungen werden angezeigt.
7. 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.
8. Starten Sie den Sentinel-Service über die Weboberfläche neu.

   Weitere Informationen finden Sie unter Abschnitt 5.8, „Stoppen und Starten des Servers über die Weboberfläche“, auf Seite 54.

17 Aktualisieren des Collector-Managers

1. Erstellen Sie eine Sicherung der Konfiguration und einen ESM-Export.

   Weitere Informationen finden Sie im Abschnitt "Backing Up and Restoring Data (Sichern und Wiederherstellen von Daten)" im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.
2. Melden Sie sich an der Sentinel-Weboberfläche als Benutzer mit Verwalterfunktion 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:

   ./install-cm
9. Befolgen Sie die Anweisungen auf dem Bildschirm bis zum Abschluss der Installation.

18 Aufrüsten der Correlation Engine

1. Erstellen Sie eine Sicherung der Konfiguration und einen ESM-Export.

   Weitere Informationen finden Sie im Abschnitt "Backing Up and Restoring Data (Sichern und Wiederherstellen von Daten)" im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.
2. Melden Sie sich an der Sentinel-Weboberfläche als Benutzer mit Verwalterfunktion an.
3. Wählen Sie *Downloads* aus.
4. Klicken Sie im Abschnitt zum Correlation Engine-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:

   ./install-ce
9. Befolgen Sie die Anweisungen auf dem Bildschirm bis zum Abschluss der Installation.

19 Aufrüsten von Sentinel-Plugins

Neue und aktualisierte Sentinel-Plugins werden regelmäßig auf die Sentinel -Plugins-Website (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) hochgeladen. Laden Sie die aktuellste Version eines Plugins herunter, um die neuesten Fehlerpatches, Dokumentationsaktualisierungen und Verbesserungen für das entsprechende Plugin zu erhalten. Informationen zur Installation und zur Aufrüstung eines Plugins finden Sie in der separaten Plugin-Dokumentation.

IV Migrieren

20 Unterstützte Migrationsszenarien

Für diese Version von Sentinel werden keine Migrationsszenarien unterstützt. Sie müssen Sentinel neu installieren, statt eine Migration oder Aufrüstung durchzuführen. Ein Datenmigrationswerkzeug wird jedoch bald verfügbar sein.

Die Installationsanweisungen finden Sie unter Kapitel 2, „Installieren von Sentinel“, auf Seite 23.

21 Weitere Schritte

Um Sie nach der Installation bei der Konfiguration von Sentinel zu unterstützen, stehen Ihnen zwei Handbücher zur Verfügung: *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)* und *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

Das Administrationshandbuch enthält Informationen zu Konfigurationsaufgaben, die nur von einem Benutzer mit Administratorrechten ausgeführt werden können. Beispiel:

- "Konfigurieren von Benutzern und Rollen"
- "Konfigurieren der Datenspeicherung"
- "Konfigurieren der Datenerfassung"
- "Ereignissuche und -berichterstellung in einer verteilten Umgebung"

Weitere Informationen zu diesen und anderen Administrationsaufgaben finden Sie im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.

Das Benutzerhandbuch enthält Anleitungen zu Aufgaben, die von Benutzern in Sentinel ausgeführt werden können. Beispiel:

- "Suchen von Ereignissen"
- "Analysieren von Datentrends"
- "Berichterstellung"
- "Konfigurieren von Vorfällen"

Weitere Informationen zu diesen und anderen Benutzeraufgaben finden Sie im *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

Die Konfigurationsmöglichkeiten in Sentinel umfassen unter anderem die Ereignisanalyse, das Hinzufügen von Daten anhand von Korrelationsregeln, das Erstellen von Grundwerten und die Konfiguration von Workflows. Die Informationen im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)* unterstützen Sie bei der Konfiguration dieser Sentinel-Funktionen.

V Deinstallation

Führen Sie folgende Aufgaben aus, um Sentinel zu deinstallieren:

22 Deinstallieren von Sentinel

Zum Entfernen einer Sentinel-Installation steht Ihnen ein Deinstallationsskript zur Verfügung. Zahlreiche Dateien, einschließlich Protokolldateien, werden aufbewahrt und können, falls gewünscht, manuell entfernt werden. Vor dem Durchführen einer neuen Installation sollten Sie alle folgenden Schritte durchführen, um sicherzustellen, dass keine Dateien oder Systemeinstellungen einer vorherigen Installation übrig bleiben.

WARNING: 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.

22.1 Deinstallieren des Sentinel-Servers

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

NOTE: 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.

22.2 Deinstallation des Remote-Collector-Managers oder der Correlation Engine

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

NOTE: 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.

23 Nach der Deinstallation auszuführende Aufgaben

NOTE: Durch das Deinstallieren des Sentinel-Servers wird der Sentinel-Administratorbenutzer nicht aus dem Betriebssystem entfernt. Sie müssen diesen Benutzer bei Bedarf manuell entfernen.

23.1 Entfernen der Sentinel-Systemeinstellungen

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.

23.1.1 Abschließen der Correlation Engine-Deinstallation

Nach dem Ausführen des Deinstallationsskripts für die Correlation Engine wird das Correlation Engine-Symbol weiterhin mit dem inaktiven Status in der Weboberfläche angezeigt. Führen Sie folgende zusätzliche Schritte aus, um die Correlation Engine manuell aus der Weboberfläche zu entfernen:

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).

23.1.2 Abschließen der Collector-Manager-Deinstallation

Nach dem Ausführen des Deinstallationsskripts für den Collector-Manager wird das Collector-Manager-Symbol weiterhin mit dem inaktiven Status in der Weboberfläche angezeigt. Führen Sie folgende zusätzliche Schritte aus, um den Collector-Manager manuell aus der Weboberfläche zu entfernen:

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*.