Sentinel Log Manager 1.2.2

Installationsanleitung

Juli 2014

NetIQ

Rechtliche Hinweise

NetIQ Sentinel ist durch folgendes US-Patent geschützt: Nr. 05829001.

DIESES DOKUMENT UND DIE HIER BESCHRIEBENE SOFTWARE WERDEN GEMÄSS EINER LIZENZVEREINBARUNG ODER EINER VERSCHWIEGENHEITSVERPFLICHTUNG BEREITGESTELLT UND UNTERLIEGEN DEN JEWEILIGEN BESTIMMUNGEN DIESER VEREINBARUNGEN. SOFERN NICHT AUSDRÜCKLICH IN DER LIZENZVEREINBARUNG ODER VERSCHWIEGENHEITSVERPFLICHTUNG ERKLÄRT; STELLT DIE NETIQ CORPORATION DIESES DOKUMENT UND DIE IN DIESEM DOKUMENT BESCHRIEBENE SOFTWARE OHNE MÄNGELGEWÄHR UND OHNE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN JEGLICHER ART BEREIT, BEISPIELSWEISE UNTER ANDEREM STILLSCHWEIGENDE GEWÄHRLEISTUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. IN EINIGEN LÄNDERN SIND HAFTUNGSAUSSCHLÜSSE FÜR AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN IN BESTIMMTEN TRANSAKTIONEN NICHT ZULÄSSIG. AUS DIESEM GRUND HAT DIESE BESTIMMUNG FÜR SIE UNTER UMSTÄNDEN KEINE GÜLTIGKEIT.

Der Klarheit halber werden alle Module, Adapter und anderes Material („Modul“) gemäß den Bestimmungen der Endbenutzer-Lizenzvereinbarung (EULA) für die jeweilige Version des NetIQ-Produkts oder der NetIQ-Software lizenziert, zu dem/der diese Module gehören oder mit dem/der sie zusammenarbeiten. Durch den Zugriff auf ein Modul bzw. durch das Kopieren oder Verwenden eines Moduls erklären Sie sich an diese Bestimmungen gebunden. Falls Sie den Bestimmungen der Endbenutzer-Lizenzvereinbarung nicht zustimmen, sind Sie nicht berechtigt, ein Modul zu verwenden oder zu kopieren bzw. auf ein Modul zuzugreifen, und Sie sind verpflichtet, jegliche Kopien des Moduls zu vernichten und weitere Anweisungen bei NetIQ zu erfragen.

Ohne vorherige schriftliche Genehmigung der NetIQ Corporation dürfen dieses Dokument und die in diesem Dokument beschriebene Software nicht vermietet, verkauft oder verschenkt werden, soweit dies nicht anderweitig gesetzlich gestattet ist. Ohne vorherige schriftliche Genehmigung der NetIQ Corporation darf dieses Dokument oder die in diesem Dokument beschriebene Software weder ganz noch teilweise reproduziert, in einem Abrufsystem gespeichert oder auf jegliche Art oder auf jeglichem Medium (elektronisch, mechanisch oder anderweitig) gespeichert werden, soweit dies nicht ausdrücklich in der Lizenzvereinbarung oder Verschwiegenheitsverpflichtung dargelegt ist. Ein Teil der Unternehmen, Namen und Daten in diesem Dokument dienen lediglich zur Veranschaulichung und stellen keine realen Unternehmen, Personen oder Daten dar.

Dieses Dokument enthält unter Umständen technische Ungenauigkeiten oder Rechtschreibfehler. Die hierin enthaltenen Informationen sind regelmäßigen Änderungen unterworfen. Diese Änderungen werden ggf. in neuen Ausgaben dieses Dokuments eingebunden. Die NetIQ Corporation ist berechtigt, jederzeit Verbesserungen oder Änderungen an der in diesem Dokument beschriebenen Software vorzunehmen.

Einschränkungen für US-amerikanische Regierungsstellen: Wenn die Software und Dokumentation von einer US-amerikanischen Regierungsstelle, im Namen einer solchen oder von einem Auftragnehmer einer US-amerikanischen Regierungsstelle erworben wird, unterliegen die Rechte der Regierung gemäß 48 C.F.R. 227.7202-4 (für Käufe durch das Verteidigungsministerium, Department of Defense (DOD)) bzw. 48 C.F.R. 2.101 und 12.212 (für Käufe einer anderen Regierungsstelle als das DOD) an der Software und Dokumentation in allen Punkten den kommerziellen Lizenzrechten und Einschränkungen der Lizenzvereinbarung. Dies umfasst auch die Rechte der Nutzung, Änderung, Vervielfältigung, Ausführung, Anzeige und Weitergabe der Software oder Dokumentation.

Inhalt

Allgemeines zu diesem Handbuch

Dieses Handbuch bietet einen Überblick über Novell Sentinel Log Manager und dessen Installation.

Zielgruppe

Dieses Handbuch richtet sich an Administratoren und Endbenutzer von Novell Sentinel Log Manager.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Sie können uns über die Option "Kommentare von Benutzern" im unteren Bereich jeder Seite der Online-Dokumentation oder auf der Website für Feedback zur Novell-Dokumentation (http://www.novell.com/documentation/feedback.html) Ihre Meinung mitteilen.

Weitere Dokumentation

Weitere Informationen über die Entwicklung eigener Plugins (z. B. JasperReports) finden Sie auf der Sentinel SDK-Webseite (http://developer.novell.com/wiki/index.php/Develop_to_Sentinel). Die Entwicklungsumgebung für Sentinel Log Manager-Berichts-Plugins ist mit der Umgebung identisch, die für Novell Sentinel dokumentiert ist.

Weitere Informationen zur Sentinel-Dokumentation finden Sie auf der Sentinel-Dokumentations-Website (http://www.novell.com/documentation/sentinel61/index.html).

Weitere Informationen zum Konfigurieren von Sentinel Log Manager finden Sie im *Sentinel Log Manager 1.2.2 Administration Guide (Sentinel Log Manager 1.2.2-Administrationshandbuch)*.

Anfragen an Novell

- Novell-Website (http://www.novell.com)

- Technischer Support von Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- Novell-Self-Support (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Patch Download Site (http://download.novell.com/index.jsp)
- Novell 24x7-Support (http://www.novell.com/company/contact.html)
- Sentinel TIDS (http://support.novell.com/products/sentinel)
- Sentinel Community Support Forum (http://forums.novell.com/novell-product-support-forums/sentinel/)

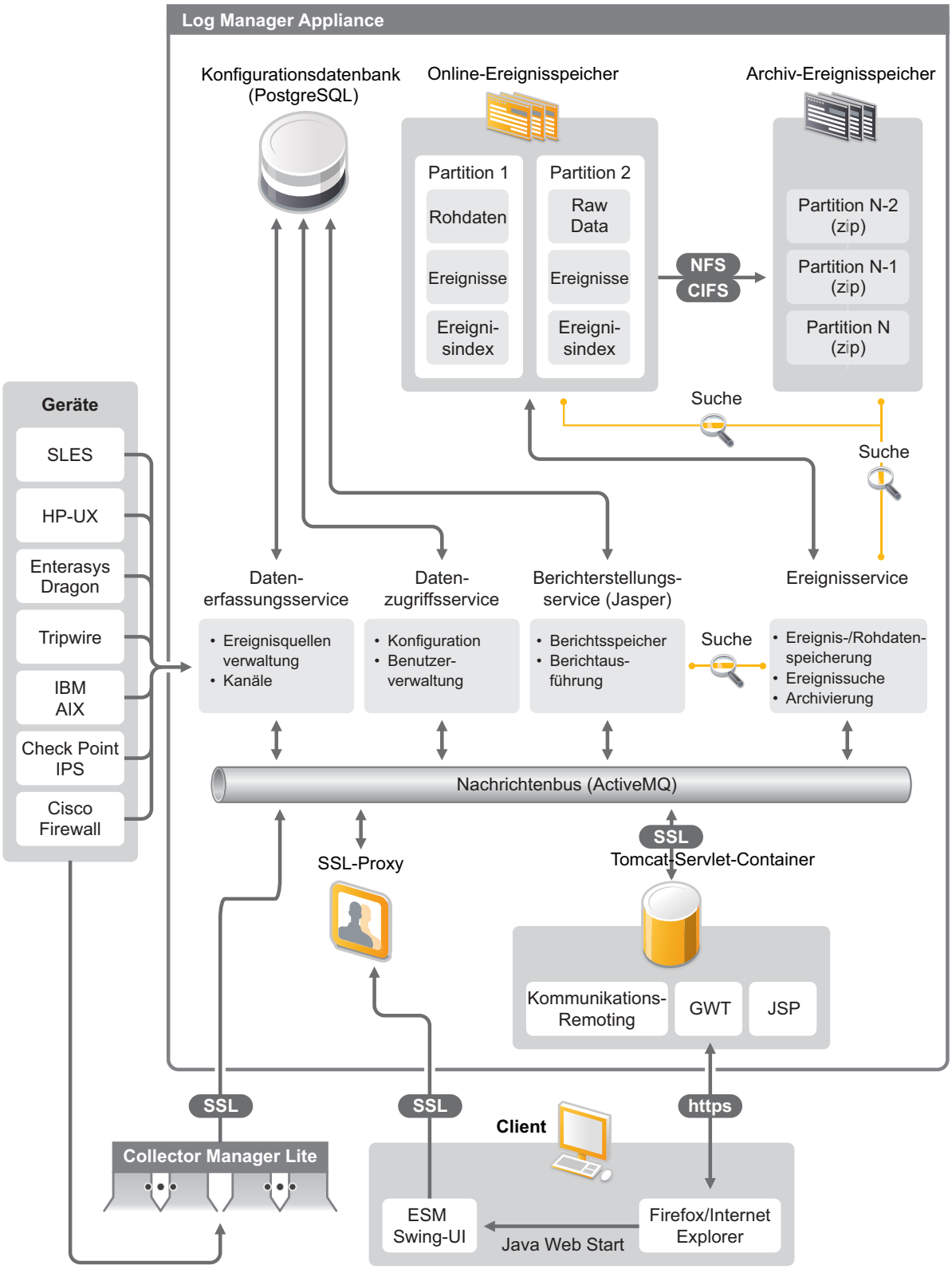
1 Einführung

Novell Sentinel Log Manager erfasst und verwaltet Daten von verschiedenen Geräten und Anwendungen, einschließlich Intrusion Detection-Systemen, Firewalls, Betriebssystemen, Routern, Webservern, Datenbanken, Switches, Mainframes und Virenschutz-Ereignisquellen. Novell Sentinel Log Manager ermöglicht die Verarbeitung mit hohen Ereignisraten, eine langfristige Datenaufbewahrung, eine richtlinienbasierte Datenaufbewahrung, die Aggregation regionaler Daten sowie eine einfache Such- und Berichterstellungsfunktionalität für eine breite Palette von Anwendungen und Geräten.

1.1 Produktübersicht

Novell Sentinel Log Manager 1.2 bietet Unternehmen eine flexible und skalierbare Protokollmanagementlösung. Als Protokollmanagementlösung bewältigt Novell Sentinel Log Manager grundlegende Protokollerfassungs- und -verwaltungsherausforderungen. Das Produkt stellt außerdem eine vollständige Lösung mit Hauptaugenmerk auf Reduzierung der Kosten und der Komplexität des Risikomanagements sowie Vereinfachung von Konformitätsanforderungen bereit.

Abbildung 1-1 *Architektur von Novell Sentinel Log Manager*



Novell Sentinel Log Manager umfasst folgende Funktionen:

- Mit den verteilten Suchfunktionen können Kunden erfasste Ereignisse nicht nur auf dem lokalen Sentinel Log Manager-Server, sondern auch auf einem oder mehreren Sentinel Log Manager-Servern von einer zentralen Konsole aus suchen.
- Integrierte Konformitätsberichte vereinfachen die Erstellung von entsprechenden Berichten für Revisions- oder forensische Analysen.
- Durch den Einsatz nicht herstellerspezifischer Speichertechnologie können Kunden ihre vorhandene Infrastruktur nutzen und die Kosten noch besser kontrollieren.
- Eine verbesserte browserbasierte Benutzeroberfläche trägt dank Unterstützung der Erfassung, Speicherung, Berichterstellung und Suche nach Protokolldaten erheblich zur Vereinfachung von Überwachungs- und Managementaufgaben bei.
- Granulare und effiziente Kontrollen und Anpassungen für IT-Administratoren durch neue Gruppen- und Benutzerberechtigungsfunktionen bieten mehr Transparenz in Bezug auf IT-Infrastrukturaktivitäten.

Dieser Abschnitt enthält folgende Informationen:

1.1.1 Ereignisquellen

Novell Sentinel Log Manager erfasst Daten aus Ereignisquellen, die Protokolle für Syslog, Windows-Ereignisprotokoll, Dateien, Datenbanken, SNMP, Novell Audit, Security Device Event Exchange (SDEE), Check Point Open Platforms for Security (OPSEC) und andere Speichermechnismen und Protokolle generieren.

Sentinel Log Manager unterstützt alle Ereignisquellen, sofern geeignete Connectors zur Analyse der Daten aus diesen Ereignisquellen zur Verfügung stehen. Novell Sentinel Log Manager stellt Collectors für viele Ereignisquellen bereit. Der generische Ereignis-Collector erfasst und verarbeitet Daten aus nicht erkannten Ereignisquellen, die über geeignete Connectors verfügen.

Über die Ereignisquellenverwaltungs-Schnittstelle können Sie die Ereignisquellen für die Datenerfassung konfigurieren.

Eine vollständige Liste der unterstützten Ereignisquellen finden Sie unter Abschnitt 2.6, „Unterstützte Ereignisquellen“, auf Seite 24.

1.1.2 Ereignisquellenverwaltung

Über die Ereignisquellenverwaltungs-Schnittstelle können Sie die Sentinel 6.0 und 6.1 Connectors und Collectors importieren und konfigurieren.

In der Live-Ansicht des Ereignisquellenverwaltungs-Fensters können Sie die folgenden Aufgaben ausführen:

- Hinzufügen oder Bearbeiten von Verbindungen zu Ereignisquellen unter Verwendung von Konfigurationsassistenten
- Anzeigen des Echtzeitstatus der Verbindungen zu den Ereignisquellen
- Importieren oder Exportieren der Konfiguration von Ereignisquellen in die bzw. aus der Live-Ansicht
- Anzeigen und Konfigurieren von Connectors und Collectors, die mit Sentinel installiert werden
- Importieren oder Exportieren von Connectors und Collectors aus einem bzw. in ein zentrales Repository
- Überwachen des über die konfigurierten Collectors und Connectors erfolgenden Datenflusses
- Anzeigen der Rohdateninformationen
- Entwickeln, Konfigurieren und Erstellen der Komponenten der Ereignisquellenhierarchie und Ausführen der erforderlichen Aktionen zur Verwendung dieser Komponenten

Weitere Informationen finden Sie im Abschnitt "Ereignisquellenverwaltung" des *Sentinel-Benutzerhandbuchs* (http://www.novell.com/documentation/sentinel61/#admin).

1.1.3 Datenerfassung

Novell Sentinel Log Manager erfasst Daten aus konfigurierten Ereignisquellen mit Hilfe von Connectors und Collectors.

Collectors sind Skripts, die Daten aus verschiedenen Ereignisquellen analysieren und in die normalisierte Sentinel-Ereignisstruktur integrieren. In einigen Fällen erfasst sie auch andere Arten von Daten aus externen Datenquellen. Jeder Collector sollte mit einem kompatiblen Connector bereitgestellt werden. Connectors erleichtern die Konnektivität zwischen Sentinel Log Manager Collectors und Ereignis- oder Datenquellen.

Novell Sentinel Log Manager stellt einen verbesserten webbasierten Benutzeroberflächen-Support für Syslog und Novell Audit zur Verfügung, um problemlos Daten aus verschiedenen Ereignisquellen zu erfassen.

Novell Sentinel Log Manager erfasst Daten mit verschiedenen Verbindungsmethoden:

- Der Syslog-Connector akzeptiert und konfiguriert automatisch Syslog-Datenquellen, die Daten über UDP (User Datagram Protocol), TCP (Transmission Control Protocol) oder das sichere TLS (Transport Layer System) senden.
- Der Audit-Connector akzeptiert und konfiguriert automatisch für Revisionen geeignete Novell-Datenquellen.
- Der Datei-Connector liest Protokolldateien.
- Der SNMP-Connector empfängt SNMP-Traps.
- Der JDBC-Connector liest Daten aus Datenbanktabellen aus.
- Der WMS-Connector greift auf Windows-Ereignisprotokolle auf Desktops und Servern zu.
- Der SDEE-Connector stellt eine Verbindung mit Geräten her, die das SDEE-Protokoll unterstützen. Hierzu gehören z. B. Cisco-Geräte.

- Der Check Point LEA (Log Export API)-Connector erleichtert die Integration zwischen Sentinel Collectors und Check Point Firewall-Servern.
- Der Sentinel-Link-Connector nimmt Daten von anderen Novell Sentinel Log Manager-Servern entgegen.
- Der Prozess-Connector nimmt Daten von benutzerdefinierten Prozessen entgegen, die Ereignisprotokolle ausgeben.

Sie können auch eine zusätzliche Lizenz zum Herunterladen von Connectors auf SAP- und Mainframe-Betriebssysteme erwerben.

Um eine Lizenz zu erwerben, rufen Sie uns unter 1-800-529-3400 an oder wenden Sie sich an den Novell Technical Support (http://support.novell.com).

Weitere Informationen zum Konfigurieren von Connectors finden Sie in den Connector-Dokumenten auf der Sentinel -Plugins-Website (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Weitere Informationen zum Konfigurieren der Datensammlung finden Sie unter „Configuring Data Collection (Konfigurieren der Datensammlung)“ im *Sentinel Log Manager 1.2.2 Administration Guide (Sentinel Log Manager 1.2-Administrationshandbuch)*.

HINWEIS: Sie müssen stets die aktuelle Version der Collectors und Connectors herunterladen und importieren. Aktualisierte Collectors und Connectors werden regelmäßig auf der Sentinel 6.1-Plugins-Website (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) veröffentlicht. Aktualisierungen der Connectors und Collectors umfassen Problembehebungen, Unterstützung für zusätzliche Ereignisse und Leistungsverbesserungen.

1.1.4 Collector-Manager

Der Collector-Manager stellt eine flexible Datenerfassungsstelle für Sentinel Log Manager bereit. Bei der Installation von Novell Sentinel Log Manager wird ein Collector-Manager standardmäßig mit installiert. Sie können Collector-Manager-Instanzen auch remote an geeigneten Orten Ihres Netzwerks installieren. Diese Remote-Collector-Manager-Instanzen führen Connectors und Collectors aus und leiten die erfassten Daten zum Speichern und Verarbeiten an Novell Sentinel Log Manager weiter.

Informationen zum Installieren von zusätzlichen Collector-Manager-Instanzen finden Sie unter „Installieren zusätzlicher Collector-Manager-Instanzen“, auf Seite 64.

1.1.5 Datenspeicherung

Der Datenfluss verläuft von Datenerfassungskomponenten zu Datenspeicherkomponenten. Diese Komponenten verwenden einen dateibasierten Datenspeicher und ein Indizierungssystem, um die erfassten Geräteprotokolldaten aufzubewahren, sowie eine PostgreSQL-Datenbank zur Aufbewahrung von Novell Sentinel Log Manager-Konfigurationsdaten.

Die Daten werden in einem komprimierten Format auf dem Serverdateisystem gespeichert und anschließend zur langfristigen Aufbewahrung an einem konfigurierten Speicherort abgelegt. Die Daten können entweder lokal oder in einer remote bereitgestellten SMB (CIFS)- oder NFS-Freigabe gespeichert werden. Die Datendateien werden basierend auf dem in der Datenaufbewahrungsrichtlinie festgelegten Zeitplan am lokalen Speicherort und an den vernetzten Speicherorten gelöscht.

Sie können die Datenaufbewahrungsrichtlinien so konfigurieren, dass Daten am Speicherort gelöscht werden, wenn die Zeitbegrenzung für die Datenaufbewahrung für die entsprechenden Daten überschritten wird oder wenn der verfügbare Speicherplatz unter die angegebene Datenträgerkapazität sinkt.

Weitere Informationen zum Konfigurieren der Datenspeicherung finden Sie unter „Configuring Data Storage (Konfigurieren der Datenspeicherung)“ im *Sentinel Log Manager 1.2.2 Administration Guide (Sentinel Log Manager 1.2-Administrationshandbuch)*.

1.1.6 Suche und Berichterstellung

Die Komponenten für die Suche und Berichterstellung unterstützen Sie dabei, die Ereignisprotokolldaten sowohl in lokalen als auch in vernetzten Datenspeicherungs- und Indizierungssystemen zu suchen und in Berichten zusammenzustellen. Die gespeicherten Ereignisdaten können entweder generisch oder über spezifische Ereignisfelder wie Quellbenutzername gesucht werden. Die entsprechenden Suchergebnisse können weiter eingegrenzt oder gefiltert werden und als Berichtvorlage zur künftigen Verwendung gespeichert werden.

Im Lieferumfang von Sentinel Log Manager sind vorinstallierte Berichte enthalten. Außerdem können Sie zusätzliche Berichte hochladen. Berichte können planmäßig oder bei Bedarf ausgeführt werden.

Eine Liste der Standardberichte finden Sie unter „Reporting (Berichterstellung)“ im *Sentinel Log Manager 1.2.2 Administration Guide (Sentinel Log Manager 1.2-Administrationshandbuch)*.

Weitere Informationen zum Suchen von Ereignissen und Erstellen von Berichten finden Sie unter „Searching Events (Suchen von Ereignissen)“ und „Reporting (Berichterstellung)“ im *Sentinel Log Manager 1.2.2 Administration Guide (Sentinel Log Manager 1.2.2-Administrationshandbuch)*.

1.1.7 Sentinel Link

Sentinel Link kann verwendet werden, um Ereignisdaten von einem Sentinel Log Manager an einen anderen weiterzuleiten. Bei einem hierarchischen Aufbau von Sentinel Log Managern können vollständige Protokolle an mehreren regionalen Standorten beibehalten werden, während wichtigere Ereignisse an einen einzelnen Sentinel Log Manager zur zentralisierten Suche und Berichterstellung weitergeleitet werden.

Außerdem kann Sentinel Link wichtige Ereignisse an Novell Sentinel, ein vollständiges System zur Verwaltung von Sicherheitsinformationsereignissen (Security Information Event Management, SIEM), weiterleiten. Dort wird die Korrelation erweitert, es werden Störungen beseitigt und hochwertige kontextabhängige Informationen wie kritische Serverzustände oder Identitätsinformationen von einem Identitätsverwaltungssystem eingespeist.

1.1.8 Webbasierte Benutzeroberfläche

Im Lieferumfang von Novell Sentinel Log Manager ist eine webbasierte Benutzeroberfläche zum Konfigurieren und Verwenden von Log Manager enthalten. Die Funktionalität der Benutzeroberfläche wird durch einen Webserver und eine grafische Benutzeroberfläche bereitgestellt, die auf Java Web Start basieren. Alle Benutzeroberflächen kommunizieren über eine verschlüsselte Verbindung mit dem Server.

Mithilfe der Benutzeroberfläche von Novell Sentinel Log Manager können Sie folgende Aufgaben erledigen:

- Ereignisse suchen

- Die Suchkriterien als Berichtsschablone speichern
- Berichte anzeigen und verwalten
- Die Ereignisquellenverwaltungs-Schnittstelle zum Konfigurieren der Datensammlung für andere Datenquellen als Syslog und Novell-Anwendungen starten (nur Administratoren)
- Die Datenweiterleitung konfigurieren (nur Administratoren)
- Das Sentinel Collector-Manager-Installationsprogramm für die Remote-Installation herunterladen (nur Administratoren)
- Den Status der Ereignisquellen anzeigen (nur Administratoren)
- Die Datensammlung für Syslog- und Novell-Datenquellen konfigurieren (nur Administratoren)
- Den Datenspeicher konfigurieren und den Zustand der Datenbank anzeigen (nur Administratoren)
- Die Datenarchivierung konfigurieren (nur Administratoren)
- Zugehörige Aktionen zum Senden übereinstimmender Ereignisdaten an Ausgabekanäle konfigurieren (nur Administratoren)
- Benutzerkonten und Berechtigungen verwalten (nur Administratoren)

1.2 Installationsüberblick

Novell Sentinel Log Manager kann entweder als Appliance oder auf einem vorhandenen SUSE Linux Enterprise Server (SLES) 11 SP1-Betriebssystem installiert werden. Wird Sentinel Log Manager als Appliance installiert, erfolgt die Installation des Log Manager-Servers auf einem SLES 11 SP1-Betriebssystem.

Novell Sentinel Log Manager installiert standardmäßig die folgenden Komponenten:

- Sentinel Log Manager-Server
- Kommunikationsserver
- Webserver und webbasierte Benutzeroberfläche
- Reporting-Server
- Collector Manager

Für einige dieser Komponenten ist eine zusätzliche Konfiguration erforderlich.

Bei der Installation von Novell Sentinel Log Manager wird ein Collector-Manager standardmäßig mit installiert. Wenn Sie weitere Collector-Manager-Instanzen benötigen, können Sie diese separat auf Remote-Computern installieren. Weitere Informationen finden Sie unter Kapitel 7, „Installieren zusätzlicher Collector-Manager-Instanzen“, auf Seite 63.

2 Systemvoraussetzungen

Im folgenden Abschnitt werden die Anforderungen in Bezug auf Hardware, Betriebssystem, Browser, unterstützte Connectors und Ereignisquellenkompatibilität für Novell Sentinel Log Manager beschrieben.

2.1 Hardwareanforderungen

2.1.1 Sentinel Log Manager-Server

Novell Sentinel Log Manager wird auf 64-Bit-Intel Xeon und AMD Opteron-Prozessoren unterstützt. Auf Itanium-Prozessoren besteht hingegen keine Unterstützung.

Die folgende Tabelle enthält die empfohlenen Hardwareanforderungen für ein Produktionssystem, das 90 Tage Online-Daten speichert. Die empfohlenen Anforderungen beziehen sich auf eine durchschnittliche Ereignisgröße von 300 Byte.

Tabelle 2-1 *Hardwareanforderungen für Sentinel Log Manager*

Anforderungen	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
Komprimierung	Bis zu 10:1	Bis zu 10:1	Bis zu 10:1

Anforderungen	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
Maximale Ereignisquellen	Bis 1000	Bis 1000	Bis 2000
Maximale Ereignisrate	500	2500	7500
Prozessor	1 Intel Xeon E5450 3 GHz (4 Core)-CPU oder 2 Intel Xeon L5240 3 (2 Core)-CPUs (insgesamt 4 Cores)	1 Intel Xeon E5450 3 GHz (4 Core)-CPU oder 2 Intel Xeon L5240 3 (2 Core)-CPUs (insgesamt 4 Cores)	2 Intel Xeon X5470 3,33 GHz (4 Core)-CPUs (insgesamt 8 Cores)
RAM	4 GB	4 GB	8 GB
Lokaler Speicher (30 Tage)	2 x 500 GB, 7200-RPM-Laufwerke (Hardware-RAID mit 256 MB Cache, RAID 1)	4 x 10 TB, 7200-RPM-Laufwerke (Hardware-RAID mit 256 MB Cache, RAID 1)	16 x 600 GB, 15000-RPM-Laufwerke (Hardware-RAID mit 512 MB Cache, RAID 10) oder ein gleichwertiges Storage Area Network (SAN)
Netzwerkspeicher (90 Tage)	600 GB	2 TB	5,8 TB

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 2.1.3, „Schätzung der Datenspeicheranforderung“, auf Seite 19.
- Der Netzwerkspeicher enthält die Daten der gesamten 90 Tage, einschließlich einer komprimierten Kopie der Ereignisdaten aus dem lokalen Speicher. Aus Gründen der Such- und Berichterstellungsleistung enthält der lokale Speicher eine Kopie der Ereignisdaten. Bei Bedarf 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.
- Ein Computer kann mehr als eine Ereignisquelle enthalten. Ein Windows-Server kann z. B. zwei Sentinel-Ereignisquellen enthalten, wenn Sie Daten aus dem Windows-Betriebssystem und Daten aus der auf dem Computer gehosteten SQL Server-Datenbank erfassen möchten..
- Das empfohlene stationäre Speichervolumen beträgt 80 Prozent der maximal lizenzierten EPS. Novell empfiehlt, zusätzliche Sentinel Log Manager-Instanzen zu erwerben, wenn diese Grenze erreicht wird.
- Die maximalen Ereignisquellengrenzen stellen keine festen Grenzen dar. Es sind lediglich Empfehlungen, die auf den von Novell durchgeführten Leistungstests beruhen und von einer niedrigen durchschnittlichen Ereignisrate pro Sekunde und Ereignisquelle (weniger als 3 EPS) ausgehen. Höhere EPS-Raten führen zu einem niedrigeren dauerhaften Maximum an Ereignisquellen. Mit der folgenden Gleichung können Sie die ungefähren Grenzen für Ihre spezifische durchschnittliche EPS-Rate oder die Anzahl der Ereignisquellen ermitteln, sofern die

maximale Anzahl der Ereignisquellen die oben angegebene Grenze nicht überschreitet: (maximale Ereignisquellen) x (durchschnittliche EPS pro Ereignisquelle) = maximale Ereignisrate.

2.1.2 Collector-Manager-System

- ❒ Ein Intel Xeon X5570 2,93 GHz (4 CPU-Kerne)
- ❒ 4 GB RAM
- ❒ 10 GB freier Festplattenspeicher

2.1.3 Schätzung der Datenspeicheranforderung

Mit Sentinel Log Manager werden Rohdaten über einen längeren Zeitraum aufbewahrt, um rechtliche sowie andere Vorschriften zu erfüllen. Sentinel Log Manager 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 *Sentinel Log Manager 1.2.2 Administration Guide* (Sentinel Log Manager 1.2-Administrationshandbuch).

Um den für Sentinel Log Manager 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 Log Manager-Computer oder remote im SMB (Server Message Block)-Protokoll oder CIFS-Protokoll, im NFS (Network File System) oder einem SAN über ausreichend Festplattenspeicher verfügen, der von Sentinel Log Manager 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 Log Manager 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 0,00007 = 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 0,00002 = 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 0,000012 = 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

  Bei aktiviertem Netzwerkspeicher werden Ereignisdaten zum Netzwerkspeicher verschoben, wenn der lokale Speicher voll ist. Rohdaten sind jedoch nur vorübergehend im lokalen Speicher enthalten, bevor sie zum Netzwerkspeicher verschoben werden. Rohdaten werden üblicherweise in weniger als einem Tag vom lokalen Speicher zum Netzwerkspeicher verschoben.
- **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

HINWEIS:

- 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.

2.1.4 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 0,004 Kompressionsverhältnis = pro Sekunde auf den Datenträger geschriebene Daten

  Bei beispielsweise 500 EPS, einer durchschnittlichen Ereignisgröße von 464 Byte und einer durchschnittlichen Rohdatengröße von 300 Byte in der Protokolldatei kann die Größe der auf den Datenträger geschriebenen Daten folgendermaßen ermittelt werden:

  (464 Byte + 300 Byte) x 500 EPS x 0,004 = 1558 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 0,00007 Kompressionsverhältnis = E/A-Anforderungen an Datenträger pro Sekunde

  Bei beispielsweise 500 EPS, einer durchschnittlichen Ereignisgröße von 464 Byte und einer durchschnittlichen Rohdatengröße von 300 Byte in der Protokolldatei kann die Anzahl der E/A-Anforderungen an den Datenträger pro Sekunde folgendermaßen ermittelt werden:

  (464 Byte + 300 Byte) x 500 EPS x 0,00007 = 26 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 0,008 Kompressionsverhältnis = pro Sekunde auf den Datenträger geschriebene Blöcke

  Bei beispielsweise 500 EPS, einer durchschnittlichen Ereignisgröße von 464 Byte und einer durchschnittlichen Rohdatengröße von 300 Byte in der Protokolldatei kann die Anzahl der pro Sekunde auf den Datenträger geschriebenen Blöcke folgendermaßen ermittelt werden:

  (464 Byte + 300 Byte) x 500 EPS x 0,008 = 3056

- **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 0,013 Kompressionsverhältnis = pro Sekunde vom Datenträger gelesene Kilobyte

  Bei beispielsweise 3 Millionen Ereignissen, die mit der Suchabfrage übereinstimmen, einer durchschnittlichen Ereignisgröße von 464 Byte und einer durchschnittlichen Rohdatengröße von 300 Byte in der Protokolldatei kann die Größe der pro Sekunde vom Datenträger gelesenen Daten folgendermaßen ermittelt werden:

  (464 Byte + 300 Byte) x 3 x 0,013 = 300 KB

2.1.5 Schätzung der Netzwerkbandbreitennutzung

Verwenden Sie die folgenden Formeln zur Schätzung der Netzwerkbandbreitennutzung auf dem Server bei unterschiedlichen 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 464 Byte und einer durchschnittlichen Rohdatengröße von 300 Byte in der Protokolldatei kann die Netzwerkbandbreitennutzung folgendermaßen ermittelt werden:

(464 Byte + 300 Byte} x 500 EPS x 0,0003 = 115 KBit/s

2.1.6 Virtuelle Umgebung

Sentinel Log Manager ist eingehend getestet und wird auf einem VMware ESX-Server vollständig unterstützt. 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 2.1, „Hardwareanforderungen“, auf Seite 17.

2.2 Unterstützte Betriebssysteme

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

- Abschnitt 2.2.1, „Sentinel Log Manager“, auf Seite 22
- Abschnitt 2.2.2, „Collector Manager“, auf Seite 22

2.2.1 Sentinel Log Manager

- ❒ SUSE Linux Enterprise Server 11 SP3 (64-Bit)
- ❒ Ein Dateisystem mit hoher Leistungsfähigkeit

HINWEIS: Alle Novell-Tests werden mit dem ext3-Dateisystem ausgeführt.

2.2.2 Collector Manager

Auf folgenden Betriebssystemen können Sie zusätzliche Collector-Manager-Instanzen installieren:

- „Linux“, auf Seite 22
- „Windows“, auf Seite 22

Linux

- ❒ SUSE Linux Enterprise Server 11 SP3 (64 Bit)

Windows

- ❒ Windows Server 2003 (32- und 64-Bit)
- ❒ Windows Server 2003 SP2 (32-Bit und 64-Bit)
- ❒ Windows Server 2003 R2 (32- und 64-Bit)
- ❒ Windows Server 2008 (64-Bit)
- ❒ Windows Server 2008 R2 (64 Bit)

2.3 Unterstützte Browser

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

- Abschnitt 2.3.1, „Linux“, auf Seite 23
- Abschnitt 2.3.2, „Windows“, auf Seite 23

2.3.1 Linux

- ❒ Mozilla Firefox 5 und höher

2.3.2 Windows

- ❒ Mozilla Firefox 5 und höher
- ❒ Microsoft Internet Explorer 8 und 11*

* Weitere Informationen hierzu finden Sie unter „Voraussetzungen für Internet Explorer“, auf Seite 23.

Voraussetzungen für Internet Explorer

- Wenn die Sicherheitsstufe auf "Hoch" eingestellt ist, wird nach dem Anmelden in Sentinel Log Manager nur eine leere Seite angezeigt. Zur Umgehung dieses Problems navigieren Sie zu *Extras* > *Internetoptionen* > *Sicherheit (Registerkarte)* > *Vertrauenswürdige Sites*. Klicken Sie auf die Schaltfläche *Sites* und fügen Sie die Sentinel Log Manager-Website der Liste der vertrauenswürdigen Sites hinzu.
- Stellen Sie sicher, dass die Option *Extras* > *Kompatibilitätsansicht* nicht aktiviert ist.
- Wenn die Option *Automatische Eingabeaufforderung für Dateidownloads* nicht aktiviert ist, wird das Popup-Fenster für den Dateidownload möglicherweise vom Browser blockiert. Zur Umgehung dieses Problems navigieren Sie zu *Extras* > *Internetoptionen* > *Sicherheit (Registerkarte)* > *Stufe anpassen*, führen Sie einen Bildlauf nach unten bis zum Bereich "Download" durch und wählen Sie *Aktivieren*, um die Option *Automatische Eingabeaufforderung für Dateidownloads* auszuwählen.

2.4 Unterstützte virtuelle Umgebung

- ❒ VMware ESX/ESXi 3.5/4.0 oder höher
- ❒ VMPlayer 3 (nur zur Demo)
- ❒ Xen 3.1.1

2.5 Unterstützte Connectors

Sentinel Log Manager unterstützt alle Connectors, die von Sentinel und Sentinel RD unterstützt werden.

- ❒ Audit-Connector
- ❒ Check Point LEA-Prozess-Connector
- ❒ Datenbank-Connector
- ❒ Datengenerator-Connector
- ❒ Datei-Connector
- ❒ Prozess-Connector
- ❒ Syslog-Connector
- ❒ SNMP-Connector

- ❒ SDEE-Connector
- ❒ Sentinel-Link-Connector
- ❒ WMS-Connector
- ❒ Mainframe-Connector
- ❒ SAP-Connector

HINWEIS: Für den Mainframe- und den SAP-Connector ist eine separate Lizenz erforderlich.

2.6 Unterstützte Ereignisquellen

Sentinel Log Manager erfasst Daten von verschiedenen Geräten und Anwendungen, einschließlich Intrusion Detection-Systemen, Firewalls, Betriebssystemen, Routern, Webservern, Datenbanken, Switches, Mainframes und Virenschutz-Ereignisquellen. Die Daten aus diesen Ereignisquellen werden in unterschiedlichem Ausmaß analysiert und normalisiert. Dies hängt davon ab, ob die Daten mit dem generischen Ereignis-Collector, der die gesamte Nutzlast des Ereignisses in ein gemeinsames Feld überträgt, oder mit dem gerätespezifischen Collector verarbeitet werden, der die Daten in einzelnen Feldern analysiert.

Sentinel Log Manager unterstützt folgende Ereignisquellen:

- ❒ Cisco Firewall (6 und 7)
- ❒ Cisco Switch Catalyst 6500 Series (CatOS 8.7)
- ❒ Cisco Switch Catalyst 6500 Series (IOS 12.2SX)
- ❒ Cisco Switch Catalyst 5000 Series (CatOS 4.x)
- ❒ Cisco Switch Catalyst 4900 Series (IOS 12.2SG)
- ❒ Cisco Switch Catalyst 4500 Series (IOS 12.2SG)
- ❒ Cisco Switch Catalyst 4000 Series (CatOS 4.x)
- ❒ Cisco Switch Catalyst 3750 Series (IOS 12.2SE)
- ❒ Cisco Switch Catalyst 3650 Series (IOS 12.2SE)
- ❒ Cisco Switch Catalyst 3550 Series (IOS 12.2SE)
- ❒ Cisco Switch Catalyst 2970 Series (IOS 12.2SE)
- ❒ Cisco Switch Catalyst 2960 Series (IOS 12.2SE)
- ❒ Cisco VPN 3000 (4.1.5, 4.1.7 und 4.7.2)
- ❒ Extreme Networks Summit X650 (mit ExtremeXOS 12.2.2 und früher)
- ❒ Extreme Networks Summit X450a (mit ExtremeXOS 12.2.2 und früher)
- ❒ Extreme Networks Summit X450e (mit ExtremeXOS 12.2.2 und früher)
- ❒ Extreme Networks Summit X350 (mit ExtremeXOS 12.2.2 und früher)
- ❒ Extreme Networks Summit X250e (mit ExtremeXOS 12.2.2 und früher)
- ❒ Extreme Networks Summit X150 (mit ExtremeXOS 12.2.2 und früher)
- ❒ Enterasys Dragon (7.1 und 7.2)
- ❒ Generischer Ereignis-Collector

- HP HP-UX (11iv1 und 11iv2)
- IBM AIX (5.2, 5.3 und 6.1)
- Juniper Netscreen Series 5
- McAfee Firewall Enterprise
- McAfee Network Security Platform (2.1, 3.x und 4.1)
- McAfee VirusScan Enterprise (8.0i, 8.5i und 8.7i)
- McAfee ePolicy Orchestrator (3.6 und 4.0)
- McAfee AV Via ePolicy Orchestrator 8.5
- Microsoft Active Directory (2000, 2003 und 2008)
- Microsoft SQL Server (2005 und 2008)
- Nortel VPN (1750, 2700, 2750 und 5000)
- Novell Access Manager 3.1
- Novell Identity Manager 3.6.1
- Novell NetWare 6.5
- Novell Modular Authentication Services 3.3
- Novell Open Enterprise Server 2.0.2
- Novell Privileged User Manager 2.2.1
- Novell Sentinel Link 1
- Novell SUSE Linux Enterprise Server
- Novell eDirectory 8.8.3 mit dem eDirectory-Ausrüstungs-Patch finden Sie auf der Website des Novell-Kundendiensts (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~)
- Novell iManager 2.7
- Red Hat Enterprise Linux
- Sourcefire Snort (2.4.5, 2.6.1, 2.8.3.2 und 2.8.4)
- Snare for Windows Intersect Alliance (3.1.4 und 1.1.1)
- Sun Microsystems Solaris 10
- Symantec AntiVirus Corporate Edition (9 und 10)
- TippingPoint Security Management System (2.1 und 3.0)
- Websense Web Security 7.0
- Websense Web Filter 7.0

HINWEIS: Um die Datenerfassung von den Novell iManager- und Novell Netware 6.5-Ereignisquellen zu aktivieren, fügen Sie für jede Ereignisquelle in der Ereignisquellenverwaltungs-Schnittstelle eine Instanz eines Collectors und einen untergeordneten Connector (Audit-Connector) hinzu. Danach werden diese Ereignisquellen in der Sentinel Log Manager-Weboberfläche unter *Sammlung* > *Ereignisquellen* angezeigt.

Collectors, die zusätzliche Ereignisquellen unterstützen, können entweder über die Sentinel - Plugins-Website (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) bezogen oder mit den SDK Plugins erstellt werden, die auf der Sentinel-Plugin-SDK-Website (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) verfügbar sind.

2.7 Empfohlene Begrenzungen

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

- Abschnitt 2.7.1, „Begrenzungen für den Collector-Manager“, auf Seite 26
- Abschnitt 2.7.2, „Begrenzungen für Berichte“, auf Seite 27
- Abschnitt 2.7.3, „Begrenzungen für Aktions-EPS“, auf Seite 27
- Abschnitt 2.7.4, „Begrenzungen für geöffnete Dateien in SLES“, auf Seite 27

2.7.1 Begrenzungen für den Collector-Manager

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

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

Attribut	Begrenzungen	Kommentar
Maximale Anzahl der Collector-Manager-Instanzen	20	Für diesen Wert wird vorausgesetzt, dass jeder Collector-Manager mit wenigen EPS (z. B. weniger als 100 EPS) läuft. Der Wert verringert sich mit zunehmender Anzahl von Ereignissen pro Sekunde.
Maximale Anzahl von Connectors (voll ausgelastet) auf einem einzelnen Collector-Manager	1 pro CPU-Kern, wobei mindestens 1 CPU-Kern für das Betriebssystem und andere Prozesse reserviert ist	Ein voll ausgelasteter Connector läuft mit der für diesen Connector-Typ höchsten EPS.
Maximale Anzahl von Collectors (voll ausgelastet) auf einem einzelnen Collector-Manager	1 pro CPU-Kern, wobei mindestens 1 CPU-Kern für das Betriebssystem und andere Prozesse reserviert ist	Ein voll ausgelasteter Collector läuft mit der für diesen Collector-Typ höchsten EPS.
Maximale Anzahl von Ereignisquellen auf einem einzelnen Collector-Manager	2000	Die Begrenzung für den Sentinel Log Manager-Server ist entweder 1000 oder 2000, je nach Hardware. Wenn die Serverbegrenzung auf einem einzelnen Collector-Manager erreicht ist, ist die Ereignisquellenbegrenzung für das gesamte Sentinel-System mit diesem einzelnen Collector-Manager erreicht.

Attribut	Begrenzungen	Kommentar
Höchstanzahl der Ereignisquellen pro Sentinel Log Manager-Serverinstanz	2000	

2.7.2 Begrenzungen für Berichte

Tabelle 2-3 *Leistungserhaltende Begrenzungen für Berichte*

Attribut	Begrenzungen	Kommentar
Höchstanzahl gespeicherter Berichte	200	
Höchstanzahl gleichzeitig ausgeführter Berichte	3	Die Begrenzung beruht auf der Annahme, dass der Server nicht bereits für die Datenerfassung oder andere Aufgaben stark genutzt wird.

2.7.3 Begrenzungen für Aktions-EPS

Sofern nicht anders angegeben, beruhen die Begrenzungen für die Aktions-EPS auf der Annahme, dass pro Regel eine Aktion konfiguriert ist.

Tabelle 2-4 *Leistungsdaten für Aktionen*

Aktion	EPS pro Aktion
Sentinel Link	300
In Datei protokollieren	30–50
Email senden	40
In Syslog protokollieren	5–10
Skript ausführen	5–10

2.7.4 Begrenzungen für geöffnete Dateien in SLES

In Systemen mit einer großen Anzahl an Ereignisquellen (beispielsweise mehr als 75), die zur Mehrheit den Datei-Connector verwenden und den Offset auf den Dateianfang festgelegt haben, entspricht die Begrenzung für geöffnete Dateien in SLES möglicherweise nicht der Anzahl der aktuell geöffneten Dateien im System. Dies führt möglicherweise zu Leistungsproblemen in Sentinel Log Manager.

Um dieses Problem zu umgehen, können Sie die weichen und harten Begrenzungen für die Höchstanzahl geöffneter Dateien auf die Zahl der tatsächlich geöffneten Dateien festlegen.

Führen Sie folgende Schritte aus, um die Begrenzungen für die Anzahl geöffneter Dateien festzulegen:

1. Melden Sie sich am System mit dem Benutzer „novell“ an.
2. Zeigen Sie die Anzahl der Dateien an, die für den Sentinel-Benutzer („novell“) geöffnet sind.

   ```
   lsof | wc -l
   ```

3. Zeigen Sie die harten und weichen Begrenzungen an:

   ```
   ulimit -Hn
   ```

   ```
   ulimit -Sn
   ```

   Ausgehend von der Anzahl der geöffneten Dateien können die Begrenzungen der Dateideskriptoren in der Datei `/etc/security/limits.conf` festgelegt werden. Beispielsweise können bei einer Anzahl von 1000 geöffneten Dateien die Begrenzungen auf 2000 festgelegt werden.

   HINWEIS: Nur der root-Benutzer kann die Datei `/etc/security/limits.conf` bearbeiten.

4. Stellen Sie sicher, dass der root-Benutzer die Begrenzungen der Dateideskriptoren folgendermaßen festlegt:

   ```
   novell soft nofile 2000
   ```

   ```
   novell hard nofile 2000
   ```

   HINWEIS: Das Festlegen der weichen Begrenzungen ist optional. Das Festlegen der harten Begrenzungen ist jedoch obligatorisch.

5. Speichern Sie die Änderungen.

2.8 Suchleistung und Berichterstellungsleistung

Die Leistung von Sentinel Log Manager kann je nach Umgebung, Konfiguration und Hardware variieren. Die Qualitätsattribute des Sentinel Log Manager-Systems, wie Skalierbarkeit, Zuverlässigkeit und Ressourcennutzung, wurden von Novell durch gründliche Leistungstests überprüft und bestätigt.

- Abschnitt 2.8.1, „Antwort- und Ausführungsgeschwindigkeit für Suchvorgänge“, auf Seite 28
- Abschnitt 2.8.2, „Berichterstellungsgeschwindigkeit“, auf Seite 29

2.8.1 Antwort- und Ausführungsgeschwindigkeit für Suchvorgänge

Die erforderliche Zeit zur Rückgabe der ersten Suchergebnisse wurde mittels mehrerer Tests mit folgender Konfiguration ermittelt:

- **Hardware:** 4 CPU-Kerne mit je 2,93 GHz, 4 GB RAM, SLES 11
- **EPS-Rate:** Die Eingangs-EPS-Rate während des Suchvorgangs beträgt 2000.
- **Datenspeicherung:** Alle Ereignisdaten des Zeitbereichs sind im lokalen Speicher enthalten.

Folgende Ergebnisse wurden beobachtet:

Tabelle 2-5 *Ergebnisse hinsichtlich der Suchleistung*

Gesamtanzahl der Ereignisse	Ereignisse, die mit der Suchabfrage übereinstimmen	Zeit bis zum Anzeigen der ersten Suchergebnisse
10.000.000	1.000–10.000.000	5–10 Sekunden
100.000.000	20.000.000–100.000.000	10–30 Sekunden
200.000.000	110.000.000–200.000.000	1–5 Minuten

2.8.2 Berichterstellungsgeschwindigkeit

Die erforderliche Zeit zur Erstellung eines Berichts wurde mittels mehrerer Tests mit folgender Konfiguration ermittelt:

- **Hardware:** 4 CPU-Kerne mit je 2,93 GHz, 4 GB RAM, SLES 11
- **EPS-Rate:** Die Eingangs-EPS-Rate während des Suchvorgangs beträgt 2000.
- **Speicherort der Daten:** Alle Ereignisdaten des Zeitbereichs sind im lokalen Speicher enthalten.

Folgende Ergebnisse wurden beobachtet:

Tabelle 2-6 *Ergebnisse hinsichtlich der Berichterstellungsleistung*

Gesamtanzahl der Ereignisse	Anzahl der Ereignisse, die mit der Suchabfrage übereinstimmen	Dauer der Berichterstellung
10.000.000	1.000–10.000.000	1–2 Minuten
100.000.000	20.000.000–100.000.000	10–50 Minuten
200.000.000	110.000.000–200.000.000	1–3 Stunden

HINWEIS: Bei Berichten mit sehr vielen Feldern und großen Ereignismengen, wie dem Bericht „Ereignisdetails“, kann die Berichtserstellung sehr lange dauern, eventuell auch der Arbeitsspeicher ausgehen. Zur Verbesserung der Berichtsperformance empfiehlt es sich eventuell, den RAM-Speicher des Systems zu erhöhen.

3 Installation auf einem vorhandenen SLES 11 SP1-System

In diesem Abschnitt wird die Installation von Sentinel Log Manager auf einem vorhandenen SUSE Linux Enterprise Server (SLES) 11 SP1-System mit dem Anwendungsinstallationsprogramm beschrieben. Für die Installation des Sentinel Log Manager-Servers stehen mehrere Möglichkeiten zur Verfügung: die Standardinstallationsprozedur, die benutzerdefinierte Installationsprozedur und die automatische Installationsprozedur, bei der die Installation ohne Benutzereingriff unter Verwendung der Standardwerte ausgeführt wird. Sie können Sentinel Log Manager auch als Nicht-Root-Benutzer installieren.

Bei der benutzerdefinierten Installation haben Sie die Möglichkeit, das Produkt mit einem Lizenzschlüssel zu installieren und eine Authentifizierungsoption auszuwählen. Zusätzlich zur Datenbankauthentifizierung können Sie für Sentinel Log Manager die LDAP-Authentifizierung einrichten. Wenn Sie Sentinel Log Manager für die LDAP-Authentifizierung konfigurieren, können sich Benutzer mit ihren Novell eDirectory- oder Microsoft Active Directory-Anmeldedaten beim Server anmelden.

Wenn Sie mehrere Sentinel Log Manager-Server in Ihrer Bereitstellung installieren möchten, können Sie die Installationsoptionen in einer Konfigurationsdatei aufzeichnen und anhand dieser Datei eine unbeaufsichtigte Installation ausführen. Weitere Informationen finden Sie unter Abschnitt 3.4, „Automatische Installation“, auf Seite 36.

3.1 Vor dem Beginn

- Stellen Sie sicher, dass die Hardware und die Software den in Kapitel 2, „Systemvoraussetzungen“, auf Seite 17 angegebenen Mindestanforderungen entsprechen.
- Stellen Sie sicher, dass das RPM „libstdc++33-32-bit“ installiert ist. Sie können dieses RPM entweder unter Verwendung von YaST oder mit folgendem zypper-Befehl installieren:

  ```
  zypper in libstdc++33-32bit
  ```

- Folgende RPMs oder höhere Versionen müssen installiert sein, damit Sentinel Log Manager 1.2 und höhere Versionen ordnungsgemäß auf SLES 11 SP1 arbeiten:
  - **Kernel-Patches:**
    - `kernel-default-2.6.32.29-0.3.1.x86_64.rpm`
    - `kernel-default-base-2.6.32.29-0.3.1.x86_64.rpm`

- **Linux-util-RPMs:**
  - `libblkid1-2.16-6.11.1.x86_64.rpm`
  - `libuuid1-2.16-6.11.1.x86_64.rpm`
  - `util-linux-2.16-6.11.1.x86_64.rpm`
  - `util-linux-lang-2.16-6.11.1.x86_64.rpm`
  - `uuid-runtime-2.16-6.11.1.x86_64.rpm`

  Sentinel Log Manager 1.1.0.x verwendet die squashfs-Version 3.4-35.1. SLES 11 SP1 unterstützt jedoch squashfs 4.0 und höhere Versionen, die nicht rückwärtskompatibel sind und ein mit früheren squash-Versionen komprimiertes Dateisystem nicht öffnen können. Die Installation der oben genannten RPMs behebt dieses Inkompatibilitätsproblem zwischen den squashfs-Versionen von Sentinel Log Manager 1.1.0.x und SLES 11 SP1.

  Die RPMs sind über den SLES 11-Online-Aktualisierungskanal verfügbar. Weitere Informationen zur Aktualisierung des SLES-Systems finden Sie unter „YaST Online Update“ (http://www.novell.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html) (YaST-Onlineaktualisierung) im *SLES 11 SP1 Administration Guide (http://www.novell.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html)* (SLES 11 SP1-Administrationshandbuch).

HINWEIS: Die Installation wird erst fortgesetzt, wenn die oben aufgeführten Kernel-Patches und Linux-util-RPMs installiert sind.

- Konfigurieren Sie das Betriebssystem so, dass der Befehl `hostname -f` einen gültigen Hostnamen zurückgibt.
- 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 und eine lizenzierte Version zu installieren.
- Synchronisieren Sie die Zeit mit NTP (Network Time Protocol).
- Richten Sie die folgenden Betriebssystembefehle ein:
  - `mount`
  - `umount`
  - `id`
  - `df`
  - `du`
  - `sudo`
- Die folgenden Ports müssen in der Firewall geöffnet sein:

  TCP 8080, TCP 8443, TCP 61616, TCP 10013, TCP 1289, TCP 1468, TCP 1443 und UDP 1514

  Weitere Informationen zur Verwendung dieser Ports finden Sie unter Abschnitt 4.2, „Verwendete Ports“, auf Seite 40.

3.2 Standardinstallation

Mit der Standardinstallationsprozedur wird Sentinel Log Manager mit einer 60-Tage-Probelizenz und mit allen Funktionen außer der Datenwiederherstellungsfunktion installiert.

1. Laden Sie die Installationsdateien von der Novell-Download-Website herunter und kopieren Sie sie.
2. Melden Sie sich als `root` an dem Server an, auf dem Sie Sentinel Log Manager installieren möchten.
3. 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.
4. Wechseln Sie in das Verzeichnis, in das die Installationsdatei extrahiert wird.
5. Geben Sie den folgenden Befehl ein, um das Skript `install-slm` zum Installieren von Sentinel Log Manager auszuführen:

   ```
   ./install-slm
   ```

   Wenn Sie Sentinel Log Manager auf mehr als einem Server installieren möchten, können Sie die Installationsoptionen in einer Datei aufzeichnen. Mit dieser Datei können Sie Sentinel Log Manager unbeaufsichtigt auf anderen Systemen installieren. Geben Sie zum Aufzeichnen Ihrer Installationsoptionen den folgenden Befehl an:

   ```
   ./install-slm -r responseFile
   ```
6. 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.
7. 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.

   Bei der Installation werden eine Gruppe mit dem Namen `novell` und ein Benutzer mit dem Namen `novell` erstellt, sofern noch nicht vorhanden.
8. Geben Sie die Option zum Fortfahren mit der Standardinstallation an, wenn Sie dazu aufgefordert werden.

   Der Installationsvorgang wird mit dem 60-Tage-Evaluierungsschlüssel, der im Installationsprogramm enthalten ist, fortgesetzt. Der Lizenzschlüssel aktiviert sämtliche Produktfunktionen für einen Probezeitraum von 60 Tagen, mit Ausnahme der Datenwiederherstellungsfunktion. 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 Administrator an.
10. Bestätigen Sie das Passwort für den Administrator.

    Das Installationsprogramm wählt die Methode *Authentifizierung nur gegenüber Datenbanken* aus und setzt die Installation fort.

Die Installation von Sentinel Log Manager wird abgeschlossen und der Server gestartet. Nach der Installation dauert es etwa fünf bis zehn Minuten, bis alle Services gestartet sind, da das System eine einmalige Initialisierung durchführt. Warten Sie diesen Zeitraum ab, bevor Sie sich am Server anmelden.

11 Verwenden Sie zum Anmelden am Sentinel Log Manager-Server die in der Installationsausgabe angegebene URL. Die URL lautet beispielsweise `https://10.0.0.1:8443/novelllogmanager`.

   Weitere Informationen zur Anmeldung am Server finden Sie unter Kapitel 6, „Anmelden an der Weboberfläche“, auf Seite 61.

12 Informationen zum Konfigurieren von Ereignisquellen für das Senden von Daten an Sentinel Log Manager finden Sie unter „Configuring Data Collection (Konfigurieren der Datensammlung)“ im *Sentinel Log Manager 1.2.2 Administration Guide (Sentinel Log Manager 1.2-Administrationshandbuch)*.

HINWEIS: Wenn Sie das System zum ersten Mal nach der Installation starten, kann es etwa 5 Minuten dauern, bis das System initialisiert ist und benutzt werden kann. Diese Verzögerung tritt nur beim ersten Systemstart nach der Installation oder nach einer Aktualisierung auf.

3.3 Benutzerdefinierte Installation

Bei der benutzerdefinierten Installation haben Sie die Möglichkeit, das Produkt mit einem Lizenzschlüssel zu installieren und eine Authentifizierungsoption auszuwählen. Zusätzlich zur Datenbankauthentifizierung können Sie für Sentinel Log Manager die LDAP-Authentifizierung einrichten. Wenn Sie Sentinel Log Manager für die LDAP-Authentifizierung konfigurieren, können sich Benutzer mit den Anmeldedaten für das LDAP-Verzeichnis am Server anmelden.

Wird Sentinel Log Manager nicht während der Installation für die LDAP-Authentifizierung konfiguriert, können Sie dies bei Bedarf später nachholen. Informationen zum Einrichten der LDAP-Authentifizierung nach der Installation finden Sie unter „LDAP Authentication (LDAP-Authentifizierung)“ im *Sentinel Log Manager 1.2.2 Administration Guide (Sentinel Log Manager 1.2 Administrations-Anleitung)*.

1 Laden Sie die Installationsdateien von der Novell-Download-Website herunter und kopieren Sie sie.

2 Melden Sie sich als `root` an dem Server an, auf dem Sie Sentinel Log Manager installieren möchten.

3 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.

4 Wechseln Sie in das Verzeichnis, in das die Installationsdatei extrahiert wird.

5 Geben Sie den folgenden Befehl ein, um das Skript `install-slm` zum Installieren von Sentinel Log Manager auszuführen:

   ```
   ./install-slm
   ```

6 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.

7 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.

Bei der Installation werden eine Gruppe mit dem Namen `novell` und ein Benutzer mit dem Namen `novell` erstellt, sofern noch nicht vorhanden.

8 Geben Sie die Option zum Fortfahren mit der benutzerdefinierten Installation an, wenn Sie dazu aufgefordert werden.

9 Geben Sie bei der Aufforderung zur Eingabe der Lizenzschlüsseloption `2` ein, um den Lizenzschlüssel für das erworbene Produkt anzugeben.

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

Weitere Informationen zu Lizenzschlüsseln finden Sie unter „ License Information“ (Lizenzinformationen) im *Sentinel Log Manager 1.2.2 Administration Guide* (Sentinel Log Manager 1.2-Administrationshandbuch).

11 Geben Sie das Passwort für den Administrator an.

12 Bestätigen Sie das Passwort für den Administrator.

13 Geben Sie das Passwort für den Datenbankadministrator (dbauser) an.

14 Bestätigen Sie das Passwort für den Datenbankadministrator (dbauser).

15 Für die folgenden Services können Sie jede beliebige Portnummer innerhalb des angegebenen Bereichs konfigurieren:

- Webserver
- Java Message Service
- Client-Proxy-Service
- Datenbank-Service
- Internes Gateway des Agenten

Wenn Sie mit den Standard-Ports fortfahren möchten, geben Sie die Option 6 ein, um die benutzerdefinierte Installation fortzusetzen.

16 Legen Sie die Option zum Authentifizieren der Benutzer über ein externes LDAP-Verzeichnis fest.

17 Geben Sie die IP-Adresse oder den Hostnamen des LDAP-Servers an.

Der Standardwert ist "localhost". Der LDAP Server sollte jedoch nicht auf demselben Computer wie der Sentinel Log Manager-Server installiert werden.

18 Wählen Sie eine der folgenden LDAP-Verbindungen aus:

- **SSL/TSL LDAP-Verbindung:** Stellt zur Authentifizierung eine sichere Verbindung zwischen dem Browser und dem Server her. Geben Sie "1" ein, um diese Option festzulegen.
- **Unverschlüsselte LDAP-Verbindung:** Stellt eine unverschlüsselte Verbindung her. Geben Sie "2" ein, um diese Option festzulegen.

19 Geben Sie die Portnummer des LDAP-Servers an. Der Standard-SSL-Port ist 636 und der Standard-Port ohne SSL ist 389.

20 (Bedingt) Geben Sie bei Auswahl der SSL/TSL LDAP-Verbindung an, ob das LDAP-Serverzertifikat von einer bekannten Zertifizierungsstelle signiert ist.

21 (Bedingt) Wenn Sie `n` angegeben haben, geben Sie den Dateinamen des LDAP-Serverzertifikats an.

22 Geben Sie an, ob Sie anonyme Suchvorgänge im LDAP-Verzeichnis ausführen möchten:

- **Ausführen von anonymen Suchvorgängen im LDAP-Verzeichnis:** Der Sentinel Log Manager-Server führt eine *anonyme Suche* im LDAP-Verzeichnis basierend auf dem angegebenen Benutzernamen durch, um den entsprechenden eindeutigen Namen (Distinguished Name, DN) des LDAP-Benutzers abzurufen. Geben Sie "1" ein, um diese Methode festzulegen.
- **Kein Ausführen von anonymen Suchvorgängen im LDAP-Verzeichnis:** Geben Sie "2" ein, um diese Option festzulegen.

23 (Bedingt) Wenn Sie die anonyme Suche ausgewählt haben, geben Sie das Suchattribut an und fahren Sie mit Schritt 26 fort.

24 (Bedingt) Wenn Sie die anonyme Suche in Schritt 22 nicht ausgewählt haben, geben Sie an, ob Sie Microsoft Active Directory verwenden.

Für Active Directory kann das Attribut `userPrincipalName` mit dem Wert in der Form `userName@domainName` wahlweise zur Authentifizierung des Benutzers verwendet werden, bevor die Suche nach dem LDAP-Benutzerobjekt ausgeführt wird, ohne dass der eindeutige Name des Benutzers eingegeben werden muss.

25 (Bedingt) Wenn Sie den oben angegebenen Ansatz für Active Directory verwenden möchten, geben Sie den Domänennamen an.

26 Geben Sie den Basis-DN an.

27 Drücken Sie "j", um die Richtigkeit der angegebenen Optionen zu bestätigen. Andernfalls drücken Sie "n" und ändern die Konfiguration.

28 Verwenden Sie zum Anmelden am Sentinel Log Manager-Server die in der Installationsausgabe angegebene URL. Die URL lautet beispielsweise `https://10.0.0.1:8443/novelllogmanager`.

Weitere Informationen zur Anmeldung am Server finden Sie unter Kapitel 6, „Anmelden an der Weboberfläche“, auf Seite 61.

29 Informationen zum Konfigurieren von Ereignisquellen für das Senden von Daten an Sentinel Log Manager finden Sie unter „Configuring Data Collection (Konfigurieren der Datensammlung)“ im *Sentinel Log Manager 1.2.2 Administration Guide (Sentinel Log Manager 1.2-Administrationshandbuch)*.

HINWEIS: Wenn Sie das System zum ersten Mal nach der Installation starten, kann es etwa 5 Minuten dauern, bis das System initialisiert ist und benutzt werden kann. Diese Verzögerung tritt nur beim ersten Systemstart nach der Installation oder nach einer Aktualisierung auf.

3.4 Automatische Installation

Die automatische oder unbeaufsichtigte Installation von Sentinel Log Manager ist nützlich, wenn Sie mehr als einen Sentinel Log Manager-Server in Ihrer Bereitstellung installieren möchten. In diesem Fall können Sie die Installationsparameter bei der Erstinstallation aufzeichnen und die aufgezeichnete Datei auf allen anderen Servern ausführen.

1 Laden Sie die Installationsdateien von der Novell-Download-Website herunter und kopieren Sie sie.

2 Melden Sie sich als `root` an dem Server an, auf dem Sie Sentinel Log Manager installieren möchten.

3 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.

4 Wechseln Sie in das Verzeichnis, in das die Installationsdatei extrahiert wird.

5 Geben Sie den folgenden Befehl ein, um das Skript `install-slm` zum Installieren von Sentinel Log Manager im Automatikmodus auszuführen:

```
./install-slm -u responseFile
```

Informationen zum Erstellen der Antwortdatei finden Sie unter Abschnitt 3.2, „Standardinstallation“, auf Seite 33. Die Installation wird mit den in der Antwortdatei gespeicherten Werten fortgesetzt.

6 Verwenden Sie zum Anmelden am Sentinel Log Manager-Server die in der Installationsausgabe angegebene URL. Die URL lautet beispielsweise `https://10.0.0.1:8443/novelllogmanager`.

Weitere Informationen zur Anmeldung am Server finden Sie unter Kapitel 6, „Anmelden an der Weboberfläche“, auf Seite 61.

7 Informationen zum Konfigurieren von Ereignisquellen für das Senden von Daten an Sentinel Log Manager finden Sie unter „Configuring Data Collection (Konfigurieren der Datensammlung)“ im „Sentinel Log Manager 1.2.2 Administration Guide (Sentinel Log Manager 1.2-Administrationshandbuch)“.

HINWEIS: Wenn Sie das System zum ersten Mal nach der Installation starten, kann es etwa 5 Minuten dauern, bis das System initialisiert ist und benutzt werden kann. Diese Verzögerung tritt nur beim ersten Systemstart nach der Installation oder nach einer Aktualisierung auf.

3.5 Nicht-Root-Installation

Wenn Ihre Unternehmensrichtlinie eine vollständige Installation von Sentinel Log Manager als `root` nicht zulässt, können Sie die meisten Installationsschritte als Nicht-Root-Benutzer (`novell`) ausführen.

1 Laden Sie die Installationsdateien von der Novell-Download-Website herunter und kopieren Sie sie.

2 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.

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

4 Wechseln Sie in das Verzeichnis, in das die Installationsdatei extrahiert wird.

5 Geben Sie folgenden Befehl ein:

```
./bin/root_install_prepare
```

Es wird eine Liste der Befehle angezeigt, die mit root-Berechtigungen ausgeführt werden.

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

6 Akzeptieren Sie die Liste der Befehle.

Die angezeigten Befehle werden ausgeführt.

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

```
su novell
```

8 Geben Sie folgenden Befehl ein:

```
./install-slm
```

9 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.

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 Standardinstallation auswählen, fahren Sie fort mit Schritt 8 in Abschnitt 3.2, „Standardinstallation“, auf Seite 33.
- Wenn Sie die benutzerdefinierte Installation auswählen, fahren Sie fort mit Schritt 8 in Abschnitt 3.3, „Benutzerdefinierte Installation“, auf Seite 34.

Die Installation von Sentinel Log Manager wird beendet und der Server gestartet.

12 Geben Sie den folgenden Befehl ein, um zum Benutzer `root` zu wechseln:

```
su root
```

13 Geben Sie den folgenden Befehl ein, um die Installation abzuschließen:

```
./bin/root_install_finish
```

14 Verwenden Sie zum Anmelden am Sentinel Log Manager-Server die in der Installationsausgabe angegebene URL. Die URL lautet beispielsweise `https://10.0.0.1:8443/novelllogmanager`.

Weitere Informationen zur Anmeldung am Server finden Sie unter Kapitel 6, „Anmelden an der Weboberfläche“, auf Seite 61.

HINWEIS: Wenn Sie das System zum ersten Mal nach der Installation starten, kann es etwa 5 Minuten dauern, bis das System initialisiert ist und benutzt werden kann. Diese Verzögerung tritt nur beim ersten Systemstart nach der Installation oder nach einer Aktualisierung auf.

---

4 Installieren der Appliance

Mit Sentinel Log Manager Appliance kann die auf SUSE Studio aufsetzende Software-Appliance ausgeführt werden. Diese kombiniert ein SUSE Linux Enterprise Server (SLES) 11 SP1-Betriebssystem mit verstärkter Sicherheit mit dem in der Novell Sentinel Log Manager-Software integrierten Aktualisierungsservice. Dadurch wird nicht nur die Benutzerfreundlichkeit gewährleistet, sondern die Kunden können außerdem vorhandene Investitionen nutzen. Die Software-Appliance kann entweder auf der Hardware oder in einer virtuellen Umgebung installiert werden.

4.1 Vor dem Beginn

- Stellen Sie sicher, dass die Hardwareanforderungen erfüllt sind. Weitere Informationen finden Sie unter Abschnitt 2.1, „Hardwareanforderungen“, auf Seite 17.
- Wenden Sie sich an den Novell Kundenservice (http://www.novell.com/center), um Ihren Lizenzschlüssel zu erhalten und eine lizenzierte Version zu installieren.
- Ihren Registrierungscode, mit dem Sie sich für Softwareaktualisierungen registrieren können, erhalten Sie ebenfalls vom Novell Kundenservice (http://www.novell.com/center).
- Synchronisieren Sie die Zeit mit NTP (Network Time Protocol).
- (Bedingt) Wenn Sie beabsichtigen, VMware zu verwenden, stellen Sie sicher, dass Sie über VMware Converter verfügen, um das Image gleichzeitig auf den VMware ESX-Server hochzuladen und in ein Format zu konvertieren, das auf dem ESX-Server ausgeführt werden kann.

4.2 Verwendete Ports

Novell Sentinel Log Manager Appliance verwendet die folgenden Ports zur Kommunikation. Einige dieser Ports werden in der Firewall geöffnet:

- Abschnitt 4.2.1, „In der Firewall geöffnete Ports“, auf Seite 40
- Abschnitt 4.2.2, „Lokal verwendete Ports“, auf Seite 41

4.2.1 In der Firewall geöffnete Ports

Tabelle 4-1 *Von Sentinel Log Manager verwendete Netzwerk-Ports*

Ports	Beschreibung
TCP 1289	Wird für Novell Audit-Verbindungen verwendet.
TCP 289	Wird für Novell Audit-Verbindungen an 1289 weitergeleitet.
TCP 22	Wird für sicheren Shell-Zugriff auf die Sentinel Log Manager Appliance verwendet.
UDP 1514	Wird für Syslog-Meldungen verwendet.
UDP 514	Wird für Syslog-Meldungen an 1514 weitergeleitet.
TCP 8080	Wird für die HTTP-Kommunikation verwendet.
TCP 80	Wird für den Sentinel Log Manager-Webserver zur HTTP-Kommunikation an 8080 weitergeleitet.
TCP 8443	Wird für die HTTPS-Kommunikation verwendet.
TCP 1443	Wird für SSL-verschlüsselte Syslog-Meldungen verwendet.
TCP 443	Wird für den Sentinel Log Manager-Webserver zur HTTPS-Kommunikation an 8443 weitergeleitet. Wird außerdem von der Sentinel Log Manager Appliance für den Aktualisierungsservice verwendet.
TCP 61616	Dient zur Kommunikation zwischen Collector-Manager-Instanzen und dem Server.
TCP 10013	Wird vom SSL-Proxy der Ereignisquellenverwaltungs-Schnittstelle verwendet.
TCP 54984	Wird von der Verwaltungskonsole von Sentinel Log Manager Appliance (WebYaST) verwendet.
TCP 1468	Wird für Syslog-Meldungen verwendet.

4.2.2 Lokal verwendete Ports

Tabelle 4-2 *Für die lokale Kommunikation verwendete Ports*

Ports	Beschreibung
TCP 61617	Dient zur internen Kommunikation zwischen Webserver und Server.
TCP 5556	Wird an der Schleifenbildungsschnittstelle zur internen Kommunikation mit dem internen Gateway-Server und dem internen Gateway verwendet. Dient zur Kommunikation zwischen der Agenten-Engine und dem Collector-Manager.
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).
Zwei zusätzliche, zufällig ausgewählte TCP-Ports	Dienen zur internen Kommunikation zwischen der Agenten-Engine und dem Collector-Manager.
TCP 8005	Dient zur internen Kommunikation mit Tomcat-Prozessen.
TCP 32000	Dienen zur internen Kommunikation zwischen der Agenten-Engine und dem Collector-Manager.

4.3 Installieren der VMware-Appliance

Um das Appliance-Image vom VMware ESX-Server auszuführen, importieren und installieren Sie das Image auf dem Server.

1. Laden Sie die Installationsdatei für die VMware-Appliance herunter.

   Die korrekte Datei für die VMware-Appliance enthält `vmx` im Dateinamen. Beispiel: *<sentinel_log_manager_vmx.tar.gz>*

2. 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.

3. 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.

4. Melden Sie sich am ESX-Server an.

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

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

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

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

9 Lesen und akzeptieren Sie die Novell Sentinel Log Manager-Endbenutzer-Lizenzvereinbarung.

10 Geben Sie im Bildschirm für den Hostnamen und den Domänennamen die entsprechenden Namen ein. Stellen Sie sicher, dass die Option *Hostname zur Loopback-ID zuweisen* ausgewählt ist.

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

12 Führen Sie einen der folgenden Vorgänge aus:

- Um die aktuellen Netzwerkeinstellungen zu verwenden, wählen Sie im Bildschirm *Netzwerkkonfiguration* die Option *Folgende Konfiguration verwenden* aus.
- Um die Netzwerkeinstellungen zu ändern, wählen Sie *Ändern* aus.

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

HINWEIS: 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 für Novell SUSE Enterprise Server fest und klicken Sie auf *Weiter*.

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

16 Legen Sie das admin-Passwort für Sentinel Log Manager und das dbauser-Passwort fest und klicken Sie auf *Weiter*.

17 Wählen Sie *Weiter*.

Die Installation wird fortgesetzt und abgeschlossen. Notieren Sie sich die IP-Adresse der Appliance, die in der Konsole angezeigt wird.

18 Fahren Sie mit Abschnitt 4.6, „Einrichtung der Appliance im Anschluss an die Installation“, auf Seite 45 fort.

HINWEIS: Wenn Sie das System zum ersten Mal nach der Installation starten, kann es etwa 5 Minuten dauern, bis das System initialisiert ist und benutzt werden kann. Diese Verzögerung tritt nur beim ersten Systemstart nach der Installation oder nach einer Aktualisierung auf.

4.4 Installieren der Xen-Appliance

1 Laden Sie die Installationsdatei für die virtuelle Xen-Appliance herunter und kopieren Sie sie in das Verzeichnis `/var/lib/xen/images`.

Der korrekte Dateiname für die virtuelle Xen-Appliance enthält die Buchstaben `xen`. Beispiel: *<sentinel_log_manager_xen.tar.gz>*

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

```
tar -xvzf <install_file>
```

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

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

- *<file_name>*.raw-Image-Datei
- *<file_name>*.xenconfig-Datei

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 Speicher ein.

Beispiel:

```
# -*- mode: python; -*-
name="Sentinel_Log_Manager_1.2.0.0_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.2.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.2.0.0_64_Xen.x86_64-0.777.0.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 virtuelle Maschine wird in der Liste angezeigt.

Wenn Sie z. B. name="Sentinel_Log_Manager_1.2.0.0_64" in der Datei .xenconfig konfiguriert haben, wird die virtuelle Maschine 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_Log_Manager_1.2.0.0_64
```

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 Novell SUSE Enterprise Server Software-Lizenzvereinbarung.

12 Lesen und akzeptieren Sie die Novell Sentinel Log Manager-Endbenutzer-Lizenzvereinbarung.

13 Geben Sie im Bildschirm für den Hostnamen und den Domänennamen die entsprechenden Namen ein. 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 im Bildschirm *Netzwerkkonfiguration* die Option *Folgende Konfiguration verwenden* aus.
- Um die Netzwerkeinstellungen zu ändern, wählen Sie *Ändern* aus.

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

HINWEIS: 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
```

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

18 Legen Sie das Sentinel Log Manager-Admin-Passwort und das dbauser-Passwort fest und klicken Sie auf *Weiter*.

Die Installation wird fortgesetzt und abgeschlossen. Notieren Sie sich die IP-Adresse der Appliance, die in der Konsole angezeigt wird.

19 Fahren Sie mit Abschnitt 4.6, „Einrichtung der Appliance im Anschluss an die Installation“, auf Seite 45 fort.

HINWEIS: Wenn Sie das System zum ersten Mal nach der Installation starten, kann es etwa 5 Minuten dauern, bis das System initialisiert ist und benutzt werden kann. Diese Verzögerung tritt nur beim ersten Systemstart nach der Installation oder nach einer Aktualisierung auf.

4.5 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.

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.

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

5 Lesen und akzeptieren Sie die Novell Sentinel Log Manager-Endbenutzer-Lizenzvereinbarung.

6 Wählen Sie *Weiter*.

7 Geben Sie im Bildschirm für den Hostnamen und den Domänennamen die entsprechenden Namen ein.

Stellen Sie sicher, dass die Option *Hostname der Loopback-ID zuweisen* ausgewählt ist.

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

9 Führen Sie einen der folgenden Vorgänge aus:

- Um die aktuellen Netzwerkeinstellungen zu verwenden, wählen Sie im Bildschirm „Netzwerkkonfiguration“ die Option *Folgende Konfiguration verwenden* aus.
- Um die Netzwerkeinstellungen zu ändern, wählen Sie *Ändern* aus.

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

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

HINWEIS: 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
```

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

13 Legen Sie das Sentinel Log Manager-Admin-Passwort und das dbauser-Passwort fest und klicken Sie auf *Weiter*.

14 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 `Passwort`.

15 Setzen Sie die Terminalkonfigurationen zurück:

```
reset
```

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

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

Die Installation wird fortgesetzt und abgeschlossen. Notieren Sie sich die IP-Adresse der Appliance, die in der Konsole angezeigt wird.

17 Fahren Sie mit Abschnitt 4.6, „Einrichtung der Appliance im Anschluss an die Installation“, auf Seite 45 fort.

HINWEIS: Wenn Sie das System zum ersten Mal nach der Installation starten, kann es etwa 5 Minuten dauern, bis das System initialisiert ist und benutzt werden kann. Diese Verzögerung tritt nur beim ersten Systemstart nach der Installation oder nach einer Aktualisierung auf.

4.6 Einrichtung der Appliance im Anschluss an die Installation

4.6.1 Installieren der VMware-Tools

Damit Sentinel Log Manager 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)..

4.6.2 Anmelden an der Appliance-Weboberfläche

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

1 Öffnen Sie einen Webbrowser und gehen Sie zu https://<*IP-Adresse*>: *:8443*. Die Sentinel Log Manager-Webseite wird angezeigt.

Die IP-Adresse der Appliance wird in der Appliance-Konsole angezeigt, nachdem die Installation abgeschlossen und der Server neu gestartet wurde.

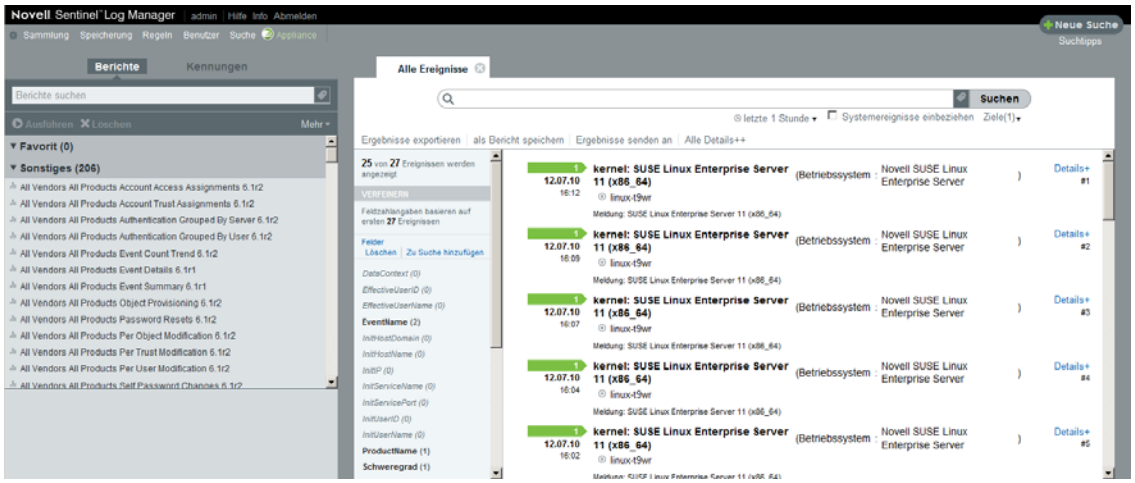
2 Sie können die Sentinel Log Manager Appliance für die Datenspeicherung und die Datensammlung konfigurieren. Weitere Informationen finden Sie im *Sentinel Log Manager 1.2.2 Administration Guide* (Sentinel Log Manager 1.2.2-Administrationshandbuch).

3 Informationen zum Registrieren für Aktualisierungen finden Sie unter Abschnitt 4.10, „Registrieren für Aktualisierungen“, auf Seite 50.

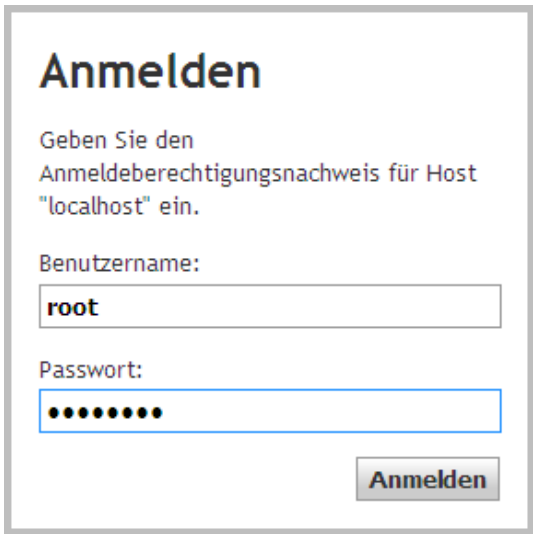
4.7 Konfigurieren von WebYaST

Die Benutzeroberfläche der Novell Sentinel Log Manager Appliance ist mit WebYaST ausgestattet. WebYaST ist eine webbasierte Fernkonsole zum Kontrollieren von Appliances, die auf SUSE Linux Enterprise basieren. Mit WebYaST können Sie auf Sentinel Log Manager 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 (http://www.novell.com/documentation/webyast/) (Benutzerhandbuch für WebYaST).

1 Melden Sie sich an der Sentinel Log Manager Appliance an.



2 Klicken Sie auf *Appliance*.



3 Konfigurieren Sie Sentinel Log Manager-Server zum Empfang von Aktualisierungen, wie in Abschnitt 4.10, „Registrieren für Aktualisierungen“, auf Seite 50 beschrieben.

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

4.8 Konfigurieren der Appliance mit SMT

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

4.8.1 Voraussetzungen

- Besorgen Sie die Anmeldedaten für das Novell Customer Center, damit Sentinel Log Manager 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.

4.8.2 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.

Führen Sie folgenden Befehl aus, um die Appliance-Repositorys zu aktivieren:

- **VMWare-Appliance-Image:**

  ```
  smt-repos -p sentinel_log_manager_1100_64_vmx_x86_64
  ```

- **Xen-Appliance-Image:**

  ```
  smt-repos -p sentinel_log_manager_1100_64_xen_x86_64
  ```

- **ISO:**

  ```
  smt-repos -p sentinel_log_manager_1100_64_xen_x86_64
  ```

4.8.3 Aufrüsten der Appliance

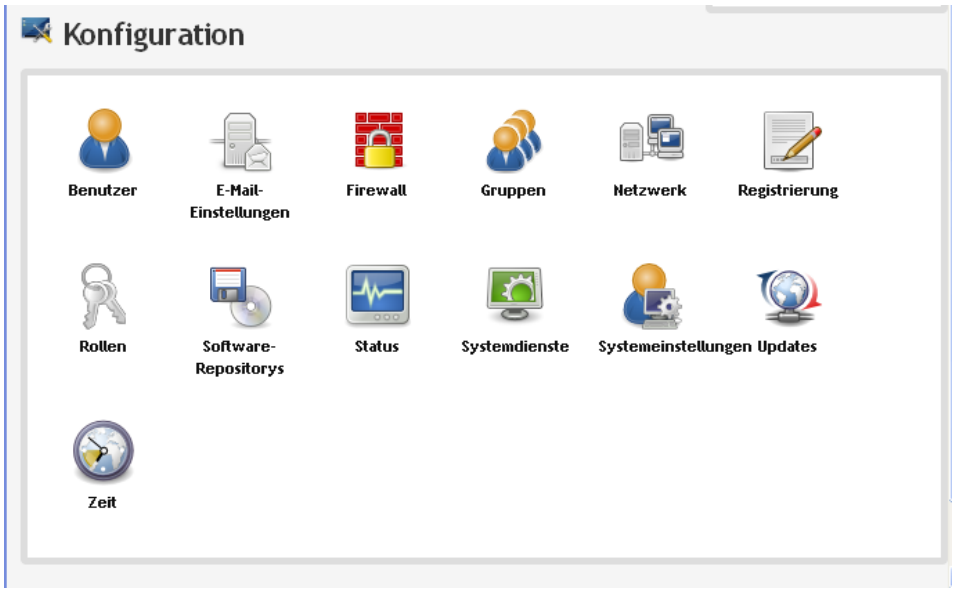
Informationen zur Aufrüstung der Appliance finden Sie unter Abschnitt 5.4.3, „Aufrüsten der Appliance mit SMT“, auf Seite 58.

4.9 Stoppen und Starten der Appliance über die Web-Benutzeroberfläche

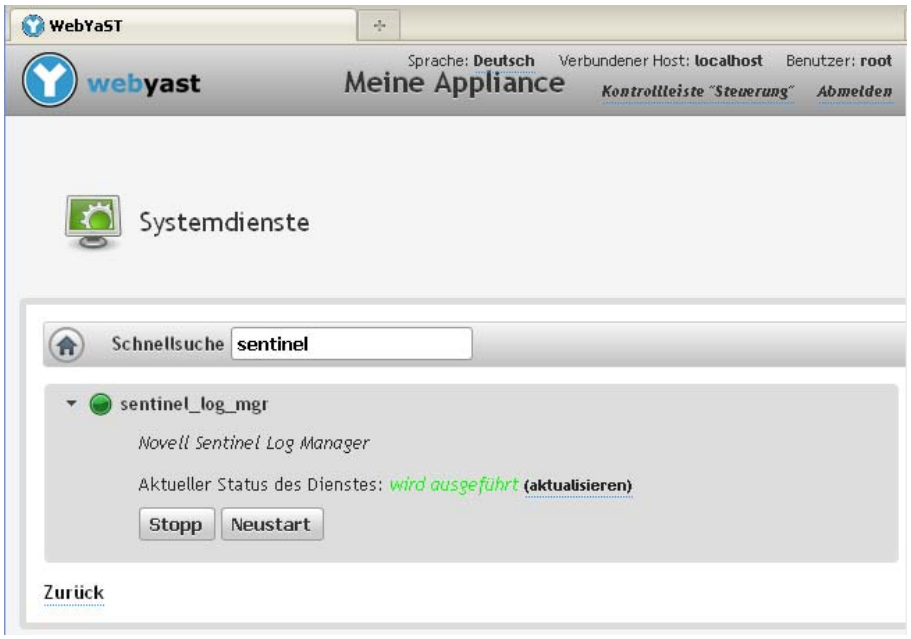
Sie können den Sentinel Log Manager-Server folgendermaßen über die Web-Benutzeroberfläche starten und stoppen:

1. Melden Sie sich an der Sentinel Log Manager Appliance an.

   Die Sentinel Log Manager-Web-Benutzeroberfläche wird angezeigt.
2. Klicken Sie auf *Appliance*, um WebYaST zu starten.



3. Klicken Sie auf *Systemdienste*.



4 Um den Sentinel Log Manager-Server zu stoppen, klicken Sie auf *stop* („stoppen“).

5 Um den Sentinel Log Manager-Server zu starten, klicken Sie auf *start* („starten“).

4.10 Registrieren für Aktualisierungen

1 Melden Sie sich an der Sentinel Log Manager Appliance an.
Die Sentinel Log Manager-Web-Benutzeroberfläche wird angezeigt.

2 Klicken Sie auf *Appliance*, um WebYaST zu starten.

3 Klicken Sie auf *Registrierung*.

4. Geben Sie die E-Mail-Adresse zum Erhalt der Aktualisierungen, den Systemnamen und den Registrierungscode der Appliance ein.
5. Klicken Sie auf *Speichern*.

Weitere Informationen zur Aufrüstung der Appliance finden Sie unter Abschnitt 5.4, „Aufrüsten der Appliance“, auf Seite 56.

5 Aufrüsten von Sentinel Log Manager

Sentinel Log Manager 1.2.0.2 kann über Sentinel Log Manager 1.2 und höher installiert werden. Wenn Sie Sentinel Log Manager 1.1.*x* aufrüsten möchten, müssen Sie zuerst das Upgrade auf Sentinel Log Manager 1.2.0.1 ausführen und Sentinel Log Manager 1.2.0.2 dann auf dieser Version installieren.

HINWEIS: Nach der Aufrüstung bleiben alle Collector-Anpassungen erhalten, die mit dem benutzerdefinierten Ausführungsmodus und der Hilfsdateimethode ausgeführt wurden, die in der SDK-Dokumentation empfohlen werden.

5.1 Voraussetzungen

- Sentinel Log Manager 1.2 und höhere Versionen erfordern die SUSE Linux Enterprise Server (SLES) 11 SP 1-Plattform. Wenn Sie auf Sentinel Log Manager 1.2 oder eine höhere Version aufrüsten, stellen Sie zunächst sicher, dass das Betriebssystem auf SLES 11 SP1 aufgerüstet ist.
- Folgende RPMs oder höhere Versionen müssen installiert sein, damit Sentinel Log Manager 1.2 und höhere Versionen ordnungsgemäß auf SLES 11 SP1 arbeiten:
  - **Kernel-Patches:**
    - `kernel-default-2.6.32.29-0.3.1.x86_64.rpm`
    - `kernel-default-base-2.6.32.29-0.3.1.x86_64.rpm`
  - **Linux-util-RPMs:**
    - `libblkid1-2.16-6.11.1.x86_64.rpm`
    - `libuuid1-2.16-6.11.1.x86_64.rpm`
    - `util-linux-2.16-6.11.1.x86_64.rpm`
    - `util-linux-lang-2.16-6.11.1.x86_64.rpm`
    - `uuid-runtime-2.16-6.11.1.x86_64.rpm`

  Sentinel Log Manager 1.1.0.*x* verwendet die squashfs-Version 3.4-35.1. SLES 11 SP1 unterstützt jedoch squashfs 4.0 und höhere Versionen, die nicht rückwärtskompatibel sind und ein mit früheren squash-Versionen komprimiertes Dateisystem nicht öffnen können. Durch die Installation der oben genannten RPMs wird dieses Inkompatibilitätsproblem zwischen den squashfs-Versionen von Sentinel Log Manager 1.1.0.*x* und SLES 11 SP1 behoben.

Die RPMs sind über den SLES 11-Online-Aktualisierungskanal verfügbar. Weitere Informationen zur Aktualisierung des SLES-Systems finden Sie unter „YaST Online Update“ (http://www.novell.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html) (YaST-Onlineaktualisierung) im *SLES 11 SP1 Administration Guide (http://www.novell.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html)* (SLES 11 SP1-Administrationshandbuch).

HINWEIS: Die Installation wird erst fortgesetzt, wenn die oben aufgeführten Kernel-Patches und Linux-util-RPMs installiert sind.

- Wenn Sie Sentinel Log Manager 1.1.*x* aufrüsten möchten, müssen Sie zuerst das Upgrade auf Sentinel Log Manager 1.2.0.1 ausführen und Sentinel Log Manager 1.2.0.2 dann auf dieser Version installieren.
- Stellen Sie sicher, dass für folgende Ordner und Unterordner keine symbolischen Links verwendet wurden:
  - `opt/novell` (Basisordner)
  - `etc/opt/novell` (Konfigurationsordner)
  - `var/opt/novell` (Datenordner)

  Wenn symbolische Links verwendet wurden, entfernen Sie sie, d. h. verschieben Sie die Verzeichnisse zurück in die Standardinstallationsverzeichnisse.

5.2 Aufrüsten des Sentinel Log Manager-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).
2. Laden Sie das aktuelle Patch von der Novell-Download-Website (http://download.novell.com) herunter.
3. (Bedingt) Wenn Sie auf Sentinel Log Manager Hotfix 1 aufrüsten möchten, laden Sie das Patch von der Website Novell Patch Finder (http://download.novell.com/patch/finder/) herunter.
4. Melden Sie sich als `root` an dem Server an, auf dem Sie Sentinel Log Manager installieren möchten.
5. Geben Sie den folgenden Befehl an, um den Sentinel Log Manager-Server anzuhalten:

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

   Beispiel: `/opt/novell/sentinel_log_mgr/bin # ./server.sh stop`.
6. 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.
7. Wechseln Sie in das Verzeichnis, in das die Installationsdatei extrahiert wurde.
8. Geben Sie den folgenden Befehl ein, um das Skript `install-slm` zum Aufrüsten von Sentinel Log Manager auszuführen:

   ```
   ./install-slm
   ```
9. 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.

10 Lesen Sie die Endbenutzer-Lizenzvereinbarung, geben Sie `ja` oder `j` ein, um die Lizenzbedingungen zu akzeptieren, und setzen Sie die Installation fort.

11 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.

Wenn Sie von einem Sentinel Log Manager 1.1-System aufrüsten, das von Sentinel Log Manager 1.0 aufgerüstet wurde, bleibt die vorhandene Installation von Sentinel Log Manager 1.0 bis auf folgende Ausnahmen unberührt:

- Wenn sich das Datenverzeichnis für die Version 1.0 (z. B. `/opt/novell/sentinel_log_manager_1.0_x86-64/data`) und das Datenverzeichnis für die Version 1.1 (z. B. `/var/opt/novell/sentinel_log_mgr/data`) im selben Dateisystem befinden, werden die Unterverzeichnisse `<1.0>/data/eventdata` und `<1.0>/data/rawdata` an den Standort der Version 1.1 verschoben, da die Verzeichnisse „eventdata“ und „rawdata“ üblicherweise groß sind. Befinden sich die Datenverzeichnisse für 1.0 und 1.1 in verschiedenen Dateisystemen, werden die Unterverzeichnisse „eventdata“ und „rawdata“ an den Standort der Version 1.1 kopiert und die Dateien der Version 1.0 bleiben unverändert.
- Wenn sich das vorhandene Datenverzeichnis für die Version 1.0 (z. B. `/opt/novell/sentinel_log_mgr_1.0_x86-64`) in einem separat eingehängten Dateisystem befindet und in dem Dateisystem, das das Datenverzeichnis für die Version 1.1 (`/var/opt/novell/sentinel_log_mgr/data`) enthält, nicht genügend Speicher zur Verfügung steht, können Sie zulassen, dass das Installationsprogramm das Dateisystem vom Standort für 1.0 wieder auf den Standort für 1.1 einhängt. Einträge in `/etc/fstab` werden ebenfalls aktualisiert. Wenn Sie nicht zulassen, dass das Installationsprogramm das vorhandene Dateisystem wieder einhängt, wird die Aufrüstung beendet. Sie können anschließend genügend Speicherplatz auf dem Dateisystem für das Datenverzeichnis für die Version 1.1 freigeben.

Nachdem die Sentinel Log Manager 1.2.0.2-Installation erfolgreich abgeschlossen und der Server funktionsfähig ist, führen Sie den folgenden Befehl aus, um das Sentinel Log Manager 1.0-Verzeichnis manuell zu entfernen:

```
rm -rf /opt/novell/slm_1.0_install_directory
```

Beispiel:

```
rm -rf /opt/novell/sentinel_log_mgr_x86-64
```

Durch Entfernen des Installationsverzeichnisses wird die Sentinel Log Manager 1.0-Installation dauerhaft gelöscht..

12 Geben Sie den folgenden Befehl an, um den Sentinel Log Manager-Server zu starten:

```
<install_directory>/bin/server.sh start
```

13 Stellen Sie sicher, dass alle Collector-Manager-Instanzen auf eine Version aufgerüstet werden, die mit der aufgerüsteten Version des Sentinel Log Manager-Servers kompatibel ist.

Weitere Informationen zum Aufrüsten von Collector-Manager-Instanzen finden Sie unter Abschnitt 5.3, „Aktualisieren des Collector-Managers“, auf Seite 56.

HINWEIS: Wenn Sie das System zum ersten Mal nach der Aufrüstung starten, kann es etwa 5 Minuten dauern, bis das System initialisiert ist und benutzt werden kann. Diese Verzögerung tritt nur beim ersten Systemstart nach der Installation oder nach einer Aufrüstung auf.

5.3 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 *Sentinel Log Manager 1.2.2 Administration Guide* (Sentinel Log Manager 1.2-Administrationshandbuch).
2. Melden Sie sich als Administrator bei Sentinel Log Manager an.
3. Wählen Sie *Sammlung* > *Erweitert*.

   Auf dieser Seite können Sie das neueste Installationsprogramm für die Aufrüstung von Collector-Manager herunterladen, das mit Sentinel Log Manager kompatibel ist.
4. Klicken Sie im Abschnitt zum Installationsprogramm für die Collector-Manager-Aufrüstung auf den Link *Installationsprogramm herunterladen*.

   Es wird ein Fenster mit der Option angezeigt, die Datei `scm_upgrade_installer.zip` 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 `.zip`-Datei.
8. Führen Sie eines der folgenden Skripte aus:
   - Zum Aufrüsten von Windows Collector-Manager führen Sie `service_pack.bat` aus.
   - Zum Aufrüsten von Linux Collector-Manager führen Sie `service_pack.sh` aus.
9. Befolgen Sie die Anweisungen auf dem Bildschirm bis zum Abschluss der Installation.

5.4 Aufrüsten der Appliance

Sie können die Sentinel Log Manager-Appliance entweder mit WebYaST oder mit SMT aufrüsten.

- Abschnitt 5.4.1, „Aufrüsten der Appliance über WebYaSt“, auf Seite 56
- Abschnitt 5.4.2, „Aufrüsten der Appliance mit zypper“, auf Seite 57
- Abschnitt 5.4.3, „Aufrüsten der Appliance mit SMT“, auf Seite 58

5.4.1 Aufrüsten der Appliance über WebYaSt

HINWEIS: Zur Aufrüstung der Sentinel Log Manager-Appliance auf einem Betriebssystem vor SLES 11 SP3 müssen Sie das Befehlszeilenprogramm zypper verwenden, da für dieses Upgrade die Interaktion des Benutzers erforderlich ist. In WebYaST ist die hierfür erforderliche Benutzerinteraktion nicht möglich. Informationen zur Verwendung von zypper für die Aufrüstung der Appliance finden Sie unter Abschnitt 5.4.2, „Aufrüsten der Appliance mit zypper“, auf Seite 57.

1. Geben Sie die URL von Sentinel Log Manager an, über die WebYaST über Port 4984 gestartet wird.
2. Melden Sie sich mit den Berechtigungsnachweisen der Appliance bei WebYast an.
3. 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).

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

   Weitere Informationen finden Sie unter Abschnitt 4.10, „Registrieren für Aktualisierungen“, auf Seite 50.

   Wenn die Appliance nicht registriert ist, wird in WebYast eine gelbe Warnmeldung angezeigt, die auf diesen Zustand hinweist.

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

   Die verfügbaren Aktualisierungen werden angezeigt.

6 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 Log Manager-Service. Nach dem Abschluss der Aufrüstung müssen Sie diesen Service manuell neu starten.

7 Starten Sie den Sentinel Log Manager-Server über die Web-Benutzeroberfläche.

   Weitere Informationen finden Sie unter Abschnitt 4.9, „Stoppen und Starten der Appliance über die Web-Benutzeroberfläche“, auf Seite 49.

5.4.2 Aufrüsten der Appliance mit zypper

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

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).

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

   Weitere Informationen finden Sie unter Abschnitt 4.10, „Registrieren für Aktualisierungen“, auf Seite 50.

   Wenn die Appliance nicht registriert ist, wird in WebYast eine gelbe Warnmeldung angezeigt, die auf diesen Zustand hinweist.

3 Melden Sie sich in der Appliance-Konsole als Benutzer `root` an.

4 Führen Sie den folgenden Befehl aus:

```
usr/bin/zypper patch
```

5 (Bedingt) Wenn Sie Sentinel Log Manager vor Version 1.2 aufrüsten, erhalten Sie eine Nachricht zu einem squashfs-Versionskonflikt. Geben Sie `1` ein, um auf die squashfs-Version 4.0-1.2.10 aufzurüsten und den Händlerwechsel zu akzeptieren.

   Sentinel Log Manager 1.1. verwendet die squashfs-Version 3.4. Sentinel Log Manager 1.2 und höher verwenden die squashfs-Version 4.0. Außerdem wird das squashfs-yast2-live-Installationsprogramm von einem anderen Händler (SLES statt OpenSUSE) verwendet. Um mit der Aufrüstung fortzufahren, müssen Sie zunächst squashfs aufrüsten und den neuen Händler akzeptieren.

6 Klicken Sie auf `J`, um fortzufahren.

7 (Bedingt) Wenn Sie Sentinel Log Manager vor Version 1.2 aufrüsten, wird die Endbenutzer-Lizenzvereinbarung für Sentinel Log Manager angezeigt. Geben Sie `Ja` ein, um die Lizenzvereinbarung zu akzeptieren.

Die Lizenzvereinbarung für Sentinel Log Manager 1.2 und höher unterscheidet sich von der Lizenzvereinbarung für Sentinel Log Manager 1.1. Um Sentinel Log Manager 1.1 oder höher auf die Version 1.2 oder höher aufzurüsten, müssen Sie die neue Lizenzvereinbarung akzeptieren.

8 (Bedingt) Wenn Sie die Sentinel Log Manager-Appliance auf einem Betriebssystem vor SLES 11 SP3 aufrüsten, wird die Endbenutzer-Lizenzvereinbarung angezeigt. Geben Sie `Ja` ein, um die Lizenzvereinbarung zu akzeptieren.

   Die Sentinel Log Manager-Appliance wird erfolgreich aufgerüstet.

9 (Bedingt) Wenn Sie Sentinel Log Manager vor Version 1.2 aufrüsten, wird nach dem Upgrade die Warnung angezeigt, dass diese Version veraltet ist.

   Die Warnmeldung wird angezeigt, weil Sentinel Log Manager 1.2.0.1 WebYaST 1.1 verwendet, die Sentinel Log Manager 1.1-Versionen jedoch WebYaST 1.0. Während der Aufrüstung wird das WebYaST 1.0-Sprachmodul in WebYaST 1.1 als veraltet erkannt. Die Warnmeldung hat jedoch keine Auswirkung auf die Aufrüstung.

10 Starten Sie die Sentinel Log Manager-Appliance neu.

5.4.3 Aufrüsten der Appliance mit SMT

In sicheren Umgebungen, wo die Appliance ohne direkten Internetzugriff ausgeführt werden muss, müssen Sie die Appliance mit dem Subscription Management Tool (SMT) konfigurieren, mit dem Sie die Appliance auf die neuesten verfügbaren Versionen aufrüsten können.

1 Stellen Sie sicher, dass die Appliance mit SMT konfiguriert wurde.

   Weitere Informationen finden Sie unter Abschnitt 4.8, „Konfigurieren der Appliance mit SMT“, auf Seite 47.

2 Melden Sie sich in der Appliance-Konsole als Benutzer `root` an.

3 Aktualisieren Sie das Repository für die Aufrüstung:

```
zypper ref -s
```

4 Überprüfen Sie, ob die Appliance für die Aufrüstung aktiviert ist:

```
zypper lr
```

5 (Optional) Überprüfen Sie die verfügbaren Aktualisierungen für die Appliance:

```
zypper lu
```

6 (Optional) Überprüfen Sie die Pakete, die die verfügbaren Aktualisierungen für die Appliance beinhalten:

```
zypper lp -r SMT-http_<smt_server_ipaddress>:SLM-1.1.0.0-ISO
```

7 Aktualisieren Sie die Appliance:

```
zypper up -t patch -r SMT-http_<smt_server_ipaddress>:SLM-1.1.0.0-ISO
```

8 Starten Sie die Appliance neu.

```
rcsentinel_log_mgr restart
```

5.5 Aufrüsten von Sentinel-Plugins

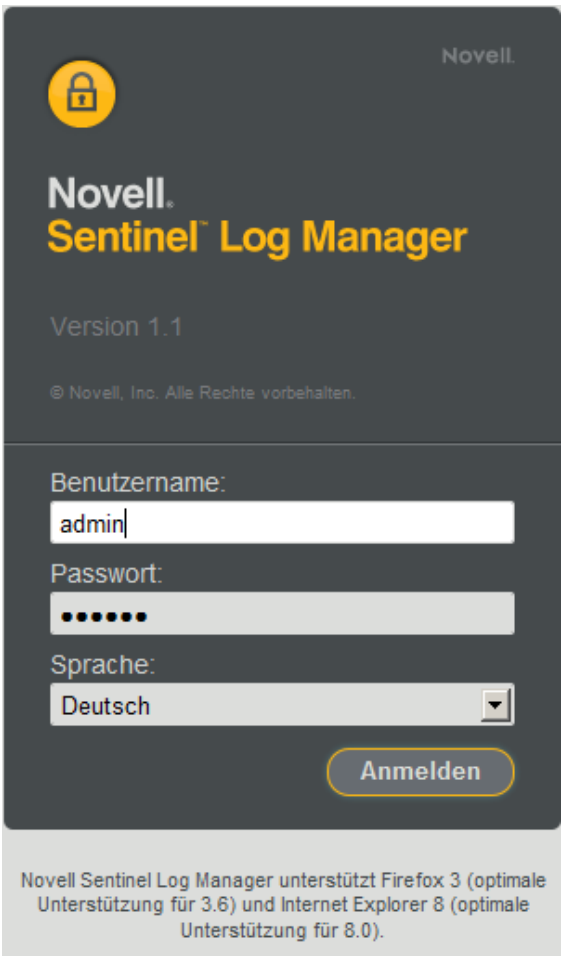
Neue und aktualisierte Sentinel-Plugins werden regelmäßig auf die Sentinel -Plugins-Website (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) hochgeladen. Laden Sie die aktuellste Version eines Plugins herunter, um die neuesten Fehlerpatches,

Dokumentationsaktualisierungen und Verbesserungen für das entsprechende Plugin zu erhalten. Informationen zur Installation und zur Aufrüstung eines Plugins finden Sie in der separaten Plugin-Dokumentation.

6 Anmelden an der Weboberfläche

Der bei der Installation als Administrator erstellte Benutzer kann sich an der Weboberfläche anmelden, um Sentinel Log Manager zu konfigurieren und zu verwenden:

1. Öffnen Sie einen unterstützten Webbrowser. Weitere Informationen finden Sie unter Abschnitt 2.3, „Unterstützte Browser“, auf Seite 22.
2. Geben Sie die URL für die Novell Sentinel Log Manager-Seite an (z. B. `https://10.0.0.1:8443/novelllogmanager`) und drücken Sie die Eingabetaste.
3. (Bedingt) Beim ersten Anmelden bei Sentinel Log Manager werden Sie aufgefordert, ein Zertifikat zu akzeptieren. Sobald Sie das Zertifikat akzeptieren, wird die Sentinel Log Manager-Anmeldeseite angezeigt.



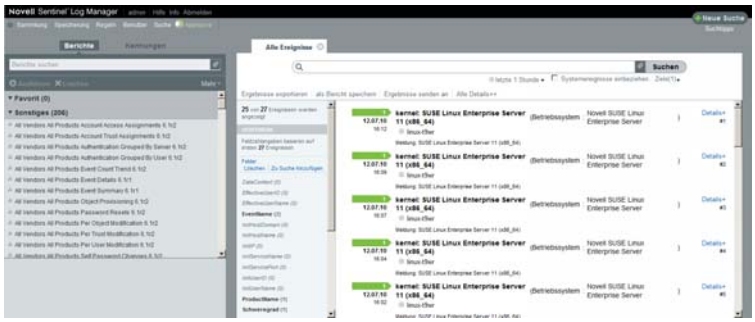
4. Geben Sie den Benutzernamen und das Passwort für den Sentinel Log Manager-Administrator ein.

5 Wählen Sie die Sprache für die Sentinel Log Manager-Benutzeroberfläche aus.

Die Sentinel Log Manager-Benutzeroberfläche ist in den Sprachen Englisch, Portugiesisch, Französisch, Italienisch, Deutsch, Spanisch, Japanisch, Chinesisch (traditionell) und Chinesisch (vereinfacht) verfügbar.

6 Klicken Sie auf *Anmelden*.

Die Sentinel Log Manager-Web-Benutzeroberfläche wird angezeigt.



7 Installieren zusätzlicher Collector-Manager-Instanzen

Die Collector-Manager-Instanzen verwalten die gesamte Datensammlung und die Datenanalyse für Novell Sentinel Log Manager. Bei der Installation von Sentinel Log Manager wird standardmäßig ein Collector-Manager auf dem Sentinel Log Manager-Server installiert. Sie können jedoch mehrere Collector-Manager-Instanzen in einer verteilten Einrichtung installieren.

7.1 Vor dem Beginn

- Stellen Sie sicher, dass die Hardware und die Software den in Kapitel 2, „Systemvoraussetzungen“, auf Seite 17 angegebenen Mindestanforderungen entsprechen.
- Synchronisieren Sie die Zeit mit NTP (Network Time Protocol).
- Ein Collector-Manager erfordert Netzwerkkonnektivität zum Port für den Nachrichtenbus (61616) auf dem Sentinel Log Manager-Server. Stellen Sie vor dem Installieren des Collector-Managers sicher, dass alle Firewall- und anderen Netzwerkeinstellungen über diesen Port kommunizieren dürfen.
- Zur Installation des Collector-Managers unter RHEL 6 müssen folgendes Skript und folgende Pakete installiert sein:
  - Installieren Sie das ksh-Skript:

    ```
    install ksh-20100621-2.el6.x86_64
    ```

  - Um das Installationsprogramm im Konsolenmodus auszuführen, müssen folgende Pakete installiert sein:
    - glibc-2.12-1.7.el6.i686
    - nss-softokn-freebl-3.12.7-1.1.el6.i686
  - Um das Installationsprogramm im GUI-Modus auszuführen, müssen folgende Pakete installiert sein:
    - glibc-2.12-1.7.el6.i686
    - libX11-1.3-2.el6.i686
    - libXau-1.0.5-1.el6.i686
    - libxcb-1.5-1.el6.i686
    - libXext-1.1-3.el6.i686
    - libXi-1.3-3.el6.i686

- libXtst-1.0.99.2-3.el6.i686
- nss-softokn-freebl-3.12.7-1.1.el6.i686

7.2 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 so die Systemleistung steigern.
- **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.
- **Fähigkeit zur Erfassung von Daten von zusätzlichen Betriebssystemen:** Sie können beispielsweise einen Collector-Manager unter Microsoft Windows installieren, um die Datenerfassung über das WMI-Protokoll zu aktivieren.
- **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 ein Vorteil bei Protokollen wie Syslog, die nicht von vornherein ein Ereignis-Caching unterstützen.

7.3 Installieren zusätzlicher Collector-Manager-Instanzen

1. Melden Sie sich als Administrator bei Sentinel Log Manager an.
2. Wählen Sie *Erfassung* > *Erweitert*.
3. Klicken Sie auf den Link *Installationsdatei herunterladen* im Bereich des Installationsprogramms für die Aufrüstung von Collector-Manager.

   Es wird ein Fenster mit der Option angezeigt, die Datei `scm_installer.zip` entweder zu öffnen oder auf dem lokalen Computer zu speichern. Speichern Sie die Datei.
4. Kopieren und extrahieren Sie die Datei in den Speicherort, in dem Sie den Collector-Manager installieren möchten.
5. Führen Sie abhängig von Ihrem Betriebssystem eine der folgenden Installationsdateien aus:
   - Zum Installieren des Collector-Managers auf einem Windows-System führen Sie die Datei `setup.bat` aus.
   - Zum Installieren des Collector-Managers auf einem Linux-System führen Sie die Datei `setup.sh` aus.
6. Wählen Sie eine Sprache aus und klicken Sie auf *OK*.

   Der Installationsbildschirm wird angezeigt.
7. Klicken Sie auf "OK".
8. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf *Weiter*.
9. Sie können entweder mit dem Standardinstallationsverzeichnis fortfahren oder auf "Durchsuchen" klicken und das Verzeichnis auswählen. Klicken Sie dann auf *Weiter*.
10. Behalten Sie den standardmäßigen Nachrichtenbus-Port (61616) bei und geben Sie den Hostnamen/die IP-Adresse des Sentinel Log Manager-Servers an.

11 Klicken Sie auf *Weiter*, um mit der standardmäßigen automatischen Konfiguration des Arbeitsspeichers (256 MB) fortzufahren.

   Eine Zusammenfassung der Installation wird angezeigt.

12 Klicken Sie auf *Installieren*.

13 Geben Sie den Benutzernamen und das Passwort für den Collector-Manager an.

   Der Benutzername und das Passwort werden in der Datei `/etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties` auf dem Sentinel Log Manager-Server gespeichert.

   Siehe folgende Zeile in der Datei `activemqusers.properties`:

   ```
   collectormanager=<password>
   ```

   `collectormanager` ist der Benutzername und der entsprechende Wert ist das Passwort.

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

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

16 Führen Sie einen Neustart Ihres Computers durch.

   Für den Fall, dass der Collector-Manager unter Windows 2008 ausgeführt wird und in der Datei `collector_manager0.0.log` nach dem Neustart Ausnahmen protokolliert sind, finden Sie unter Abschnitt A.4, „Der Collector-Manager erzeugt eine Ausnahme in Windows 2008, wenn UAC aktiviert ist“, auf Seite 73 Informationen zur Fehlersuche.

8 Deinstallation

In diesem Abschnitt werden die Schritte zum Deinstallieren von Novell Sentinel Log Manager-Server und des Collector-Managers beschrieben.

8.1 Deinstallieren der Appliance

Wenn Sie Log Manager-Daten aufbewahren möchten, müssen Sie die Daten vor dem Deinstallieren der Appliance sichern, sodass Sie sie später wiederherstellen können. Weitere Informationen finden Sie im Abschnitt „Backing Up and Restoring Data“ (Sichern und Wiederherstellen von Daten) im *Sentinel Log Manager 1.2.2 Administration Guide* (Sentinel Log Manager 1.2-Administrationshandbuch).

Wenn Sie keine Daten aufbewahren müssen, deinstallieren Sie die Appliance wie folgt:

- **VMware ESX-Appliance:** Wenn die virtuelle Maschine ausschließlich für Novell Sentinel Log Manager verwendet wurde und Sie keinerlei Daten aufbewahren müssen, können Sie die Log Manager Virtual Appliance deinstallieren, indem Sie die virtuelle Maschine löschen.
- **Xen-Appliance:** Wenn die virtuelle Xen-Maschine ausschließlich für Novell Sentinel Log Manager verwendet wurde und Sie keinerlei Daten aufbewahren müssen, löschen Sie die virtuelle Maschine, um die Log Manager Virtual Appliance zu deinstallieren.
- **Hardware-Appliance:** Wenn das System ausschließlich für Novell Sentinel Log Manager verwendet wurde und Sie keinerlei Daten aufbewahren müssen, genügt es, die Festplatte neu zu formatieren, um den Log Manager von einem physischen Computer zu deinstallieren.

8.2 Deinstallieren von Sentinel Log Manager

1. Melden Sie sich beim Sentinel Log Manager-Server als `root` an.
2. Geben Sie den folgenden Befehl ein, um das Deinstallationsskript auszuführen:

   ```
   /opt/novell/sentinel_log_mgr/setup/uninstall-slm
   ```

3. Wenn Sie aufgefordert werden, zu bestätigen, dass Sie mit der Deinstallation fortfahren möchten, drücken Sie "j".

   Der Sentinel Log Manager-Server wird zunächst angehalten und anschließend deinstalliert.

8.3 Deinstallieren des Collector-Managers

In diesem Abschnitt werden die Schritte zum Deinstallieren des Sentinel Collector-Managers unter Windows oder Linux beschrieben:

8.3.1 Deinstallieren des Linux Collector-Managers

1. Melden Sie sich als `root`-Benutzer an.
2. Wechseln Sie auf dem Computer, auf dem der Collector-Manager installiert ist, zu folgendem Speicherort:

   `$ESEC_HOME/_uninst`
3. Führen Sie den folgenden Befehl aus:

   `./uninstall.bin`
4. Wählen Sie eine Sprache aus und klicken Sie auf *OK*.
5. Klicken Sie im Installationsassistenten auf *Weiter*.
6. Wählen Sie die Funktionen aus, die Sie deinstallieren möchten, und klicken Sie auf *Weiter*.
7. Halten Sie alle aktiven Sentinel Log Manager-Anwendungen an und klicken Sie auf *Weiter*.
8. Klicken Sie auf *Deinstallieren*.
9. Klicken Sie auf *Fertig stellen*.
10. Wählen Sie *System neu booten* aus und klicken Sie auf *Fertig stellen*.

8.3.2 Deinstallieren des Windows Collector-Managers

1. Melden Sie sich als Administrator an.
2. Halten Sie den Sentinel Log Manager-Server an.
3. Klicken Sie auf “Start” > “Ausführen”.
4. Geben Sie hierzu Folgendes an:

   `%Esec_home%\_uninst`
5. Doppelklicken Sie auf die Datei `uninstall.exe`, um sie auszuführen.
6. Wählen Sie eine Sprache aus und klicken Sie auf *OK*.

   Der Installationsassistent wird angezeigt.
7. Klicken Sie auf „Weiter“.
8. Wählen Sie die Funktionen aus, die Sie deinstallieren möchten, und klicken Sie auf *Weiter*.
9. Halten Sie alle aktiven Sentinel Log Manager-Anwendungen an und klicken Sie auf *Weiter*.
10. Klicken Sie auf *Deinstallieren*.
11. Klicken Sie auf *Fertig stellen*.
12. Wählen Sie *System neu booten* aus und klicken Sie auf *Fertig stellen*.

8.3.3 Manuelles Bereinigen von Verzeichnissen

Linux

1. Melden Sie sich als `root`-Benutzer bei dem Computer an, von dem der Collector-Manager deinstalliert wurde.
2. Halten Sie alle Sentinel Log Manager-Prozesse an.
3. Entfernen Sie den Inhalt des Verzeichnisses `/opt/novell/sentinel6`.

Windows

1. Melden Sie sich als Administrator bei dem Computer an, von dem der Collector-Manager deinstalliert wurde.
2. Löschen Sie den Ordner `%CommonProgramFiles%\InstallShield\Universal` und seinen gesamten Inhalt.
3. Löschen Sie den Ordner `%ESEC_HOME%` . Dies ist standardmäßig `C:\Programme\Novell\Sentinel6`.

A Fehlersuche bei der Installation

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

A.1 Die Aufrüstung von Sentinel Log Manager schlägt fehl, wenn das dbauser-Passwort nicht mit dem in der Datei .pgpass gespeicherten dbauser-Passwort übereinstimmt

Problem:

Das Datenbankupgrade schlägt bei der Aufrüstung von Sentinel Log Manager fehl, wenn das dbauser-Passwort nicht mit dem in der Datei `.pgpass` gespeicherten Passwort übereinstimmt.

Dabei unterscheidet sich das Verhalten von der Art der Installation:

Standardinstallation: Die Aufrüstung wird nicht fortgesetzt und eine entsprechende Meldung mit der Fehlerursache und einer Behelfslösung wird angezeigt.

Appliance-Konsole: Die folgende Fehlermeldung wird angezeigt:

```
Installing: novell-SLMdb-1.2.0.2-954 [error]
Installation of novell-SLMdb-1.2.0.2-954 failed:
(with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Unable to
login to the database, cannot continue with the upgrade. Check if the dbauser
password specified in /home/novell/.pgpass is correct and try again.
error: %pre(novell-SLMdb-1.2.0.2-954.x86_64) scriptlet failed, exit status 2
error:   install: %pre scriptlet failed (2), skipping novell-SLMdb-1.2.0.2-954

Abort, retry, ignore? [a/r/i] (a):
```

WebYaST: WebYaST zeigt weiterhin an, dass eine Aktualisierung verfügbar ist. Die Fehlerursache finden Sie in diesem Fall in der Datei `/var/opt/novell/sentinel_log_mgr/log/install.log` heraus.

Behelfslösung:

Geben Sie in der Datei `.pgpass` das aktuelle dbauser-Passwort ein und fahren Sie mit der Aufrüstung fort. Informationen zur Datei `.pgpass` finden Sie in der PostgreSQL-Dokumentation.

Bei Verwendung der Appliance-Konsole zur Aufrüstung führen Sie einen der folgenden Schritte aus:

- Geben Sie zum Abbruch der Installation `a` ein, ändern Sie das Passwort in der Datei `/home/novell/.pgpass` und führen Sie dann das `zypper-Patch` aus, um die Aufrüstung fortzusetzen.
- Öffnen Sie eine weitere Konsole und ändern Sie das Passwort in der Datei `/home/novell/.pgpass`. Geben Sie in der Konsole, in der die Aufrüstung ausgeführt wird, `r` ein, um mit der Aufrüstung fortzufahren.
- Geben Sie `i` ein, um die Fehlermeldung zu ignorieren und mit der Installation fortzufahren. Ändern Sie nach der Durchführung der Aufrüstung das Passwort in der Datei `/home/novell/.pgpass` und führen Sie dann in der Konsole das `zypper-Patch` aus, um die Aufrüstung erfolgreich abzuschließen.

Bei Verwendung von WebYaST zur Aufrüstung gehen Sie wie folgt vor:

1. Melden Sie sich bei der Appliance-Konsole an.
2. Ändern Sie das dbauser-Passwort in der Datei `/home/novell/.pgpass`.
3. Klicken Sie in WebYaST auf *Alles aktualisieren*, um mit der Aufrüstung fortzufahren.

   Nach Abschluss der Aufrüstung wird in WebYaST die Meldung `System ist auf dem neuesten Stand` angezeigt.

A.2 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 Log Manager auf der Appliance ein Fehler auf.

Dieses Problem beheben Sie durch die korrekte Konfiguration der Netzwerkeinstellungen. Achten Sie insbesondere darauf, dass das System eine gültige IP-Adresse und einen gültigen Hostnamen hat.

A.3 Probleme beim Konfigurieren des Netzwerks mit VMware Player 3 auf SLES 11

Bei dem Versuch, das Netzwerk mit VMware Player 3 auf SLES 11 zu konfigurieren, tritt möglicherweise folgender Fehler auf:

```
Jan 12 14:57:34.761: vmx| VNET: MACVNetPortOpenDevice: Ethernet0: can't open vmnet
device (No such device or address)
Jan 12 14:57:34.761: vmx| VNET: MACVNetPort_Connect: Ethernet0: can't open data fd
Jan 12 14:57:34.761: vmx| Msg_Post: Error
Jan 12 14:57:34.761: vmx| [msg.vnet.connectvnet] Could not connect Ethernet0 to
virtual network "/dev/vmnet0". More information can be found in the vmware.log
file.
Jan 12 14:57:34.761: vmx|[msg.device.badconnect] Failed to connect virtual device
Ethernet0.
Jan 12 14:57:34.761: vmx| --
```

Dieser Fehler gibt an, dass die VMX-Datei möglicherweise von einer anderen virtuellen Maschine (VM) geöffnet wurde. Zur Behebung dieses Problems müssen Sie die MAC-Adresse in der VMX-Datei wie folgt aktualisieren:

1. Öffnen Sie die VMX-Datei in einem Texteditor.
2. Kopieren Sie die MAC-Adresse im Feld `ethernet0.generatedAddress`.
3. Öffnen Sie die Datei `/etc/udev/rules.d/70-persistent-net.rules` im Gastbetriebssystem.
4. Kommentieren Sie die ursprüngliche Zeile aus und geben Sie dann eine `SUBSYSTEM`-Zeile wie folgt ein:

   ```
   SUBSYSTEM=="net", DRIVERS=="?*", ATTRS{address}==<MAC address>, NAME="eth0"
   ```

5. Ersetzen Sie <*MAC address*> durch die in Schritt 2 kopierte MAC-Adresse.
6. Speichern und schließen Sie die Datei.
7. Öffnen Sie die virtuelle Maschine in VMware Player.

A.4 Der Collector-Manager erzeugt eine Ausnahme in Windows 2008, wenn UAC aktiviert ist

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

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

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

Behelfslösung: Ändern Sie den Anmelden-Eigentümer für die Sentinel 6.1 Rapid Deployment-Dienste zum aktuellen Benutzer. Als Anmelden-Eigentümer ist standardmäßig Lokales Systemkonto festgelegt. So ändern Sie die Standardoption:

1. Führen Sie `services.msc` aus, um das Fenster Dienste zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf *Sentinel* und wählen Sie dann *Eigenschaften*.
3. Wählen Sie im Fenster „Eigenschaften von Sentinel“ die Registerkarte *Anmelden* aus.
4. Wählen Sie *Dieses Konto* aus, geben Sie dann den Berechtigungsnachweis für den aktuellen Benutzer ein, den Sie zum Installieren des Collector-Managers verwendet haben..

HINWEIS: Der Benutzer muss Mitglied der Administrator-Gruppe sein.

A.5 Aufrüsten von Log Manager in der Installation als ein anderer Nicht-Root-Benutzer als der Novell-Benutzer

Die Aufrüstung schlägt fehl, wenn Sie versuchen, den Novell Sentinel Log Manager 1.0-Server aufzurüsten, wenn Sie diesem unter einem anderen Nicht-Root-Benutzernamen als dem `novell`-Benutzer installiert haben. Dieses Problem tritt aufgrund der Dateiberechtigungen auf, die bei der Installation von Sentinel Log Manager 1.0 festgelegt wurden.

Führen Sie die folgenden Schritte aus, um den Sentinel Log Manager 1.0-Server aufzurüsten, den Sie unter einem anderen Nicht-Root-Benutzernamen als dem `novell`-Benutzer installiert haben:

1. Erstellen Sie den Benutzer `novell`.
2. Ändern Sie das Eigentum der Sentinel Log Manager 1.0-Installation in `novell:novell`.

   ```
   chown -R novell:novell /opt/novell/<install_directory>
   ```

   Ändern Sie das Verzeichnis *<install_directory>* in den Namen des Installationsverzeichnisses. Beispiel:

   ```
   chown -R novell:novell /opt/novell/sentinel_log_mgr_1.0_x86-64
   ```

3. Setzen Sie in der Datei `/etc/opt/novell/sentinel_log_mgr/config/esecuser.properties` den Wert für ESEC_USER auf `novell`.

A.6 UUID wird nicht für Collector-Manager-Instanzen erstellt, die aus einem Image wiederhergestellt wurden

Wenn Sie ein Image eines Collector-Manager-Servers erstellen (beispielsweise mit ZenWorks Imaging) und die Images auf unterschiedlichen Computern wiederherstellen, kann Sentinel Log Manager die neuen Collector-Manager-Instanzen nicht eindeutig identifizieren. Die Ursache hierfür liegt in UUID-Duplikaten.

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

1. Löschen Sie die Datei `host.id` bzw. `sentinel.id` im Ordner `/var/opt/novell/sentinel_log_mgr/data`.
2. Starten Sie den Collector-Manager neu.

   Der Collector-Manager generiert automatisch die UUID.

Sentinel-Terminologie

In diesen Abschnitt wird die in diesem Dokument verwendete Terminologie beschrieben.

Collectors. Ein Dienstprogramm, das die Daten analysiert und einen umfassenderen Ereignisdatenstrom bereitstellt, indem Taxonomie, Schwachstellenerkennung sowie Geschäftsrelevanz in den Datenstrom integriert werden, bevor Ereignisse korreliert, analysiert und an die Datenbank gesendet werden.

Connectors. Ein Dienstprogramm, das branchenübliche Standardmethoden nutzt, um die Verbindung zur Datenquelle herzustellen und Rohdaten zu beziehen.

Datenaufbewahrung. Eine Richtlinie, die die Dauer festlegt, für die die Ereignisse beibehalten werden, bevor sie vom Sentinel Log Manager-Server gelöscht werden.

Ereignisquelle. Die Anwendung oder das System, die bzw. das das Ereignis protokolliert.

Ereignisquellenverwaltung. ESM. Die Benutzeroberfläche, mit der Sie die Verbindungen zwischen Sentinel und seinen Ereignisquellen durch Sentinel-Connectors und Sentinel-Collectors verwalten und überwachen können.

Ereignisse pro Sekunde. EPS. Ein Wert, mit dem die Geschwindigkeit gemessen wird, mit der ein Netzwerk Daten aus seinen Sicherheitsgeräten und Anwendungen generiert. Der Begriff bezeichnet außerdem eine Rate, mit der Sentinel Log Manager Daten von den Sicherheitsgeräten sammeln und speichern kann.

Integrator. Plugins, die es Sentinel-Systemen ermöglichen, eine Verbindung zu externen Systemen herzustellen. JavaScript-Aktionen können Integratoren verwenden, um mit anderen Systemen zu interagieren.

Rohdaten . Die unverarbeiteten Ereignisse, die vom Connector empfangen werden und direkt an den Nachrichtenbus von Sentinel Log Manager gesendet werden. Anschließend werden sie auf den Datenträger auf dem Sentinel Log Manager-Server geschrieben. Die Rohdaten unterscheiden sich zwischen den einzelnen Connectors, weil auch das Format der auf dem Gerät gespeicherten Daten unterschiedlich ist.