Installationshandbuch

Novell®
Sentinel Log Manager

1.1

July 08, 2010

www.novell.com

Rechtliche Hinweise

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

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

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

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

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

Novell-Marken

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

Materialien von Drittanbietern

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

Inhalt

Informationen zu diesem Handbuch

Dieses Handbuch 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 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administrations-Anleitung).

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/)

Einführung

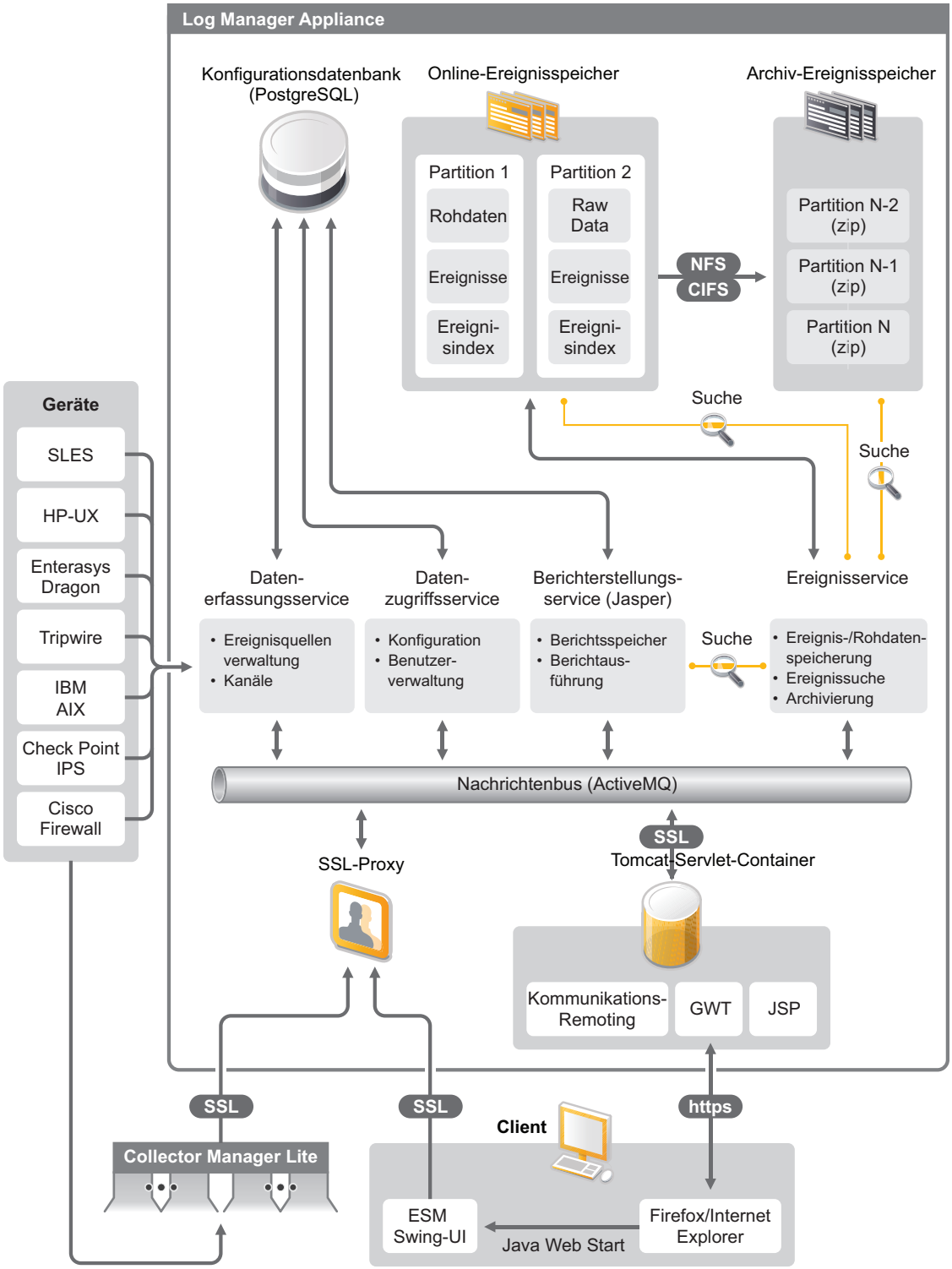
1

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 1.1 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 22.

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 Content-Website (http://support.novell.com/products/sentinel/sentinel61.html).

Weitere Informationen zum Konfigurieren der Datensammlung finden Sie unter „Configuring Data Collection“ (Konfigurieren der Datensammlung) im *Sentinel Log Manager 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administration-Anleitung).

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 Content-Website (http://support.novell.com/products/sentinel/sentinel61.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 54.

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 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administration-Anleitung).

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 1.1 Administration Guide* (Sentinel Log Manager 1.1. Administration-Anleitung).

Weitere Informationen zum Suchen von Ereignissen und Erstellen von Berichten finden Sie unter „Searching“ (Suchen) und „Reporting“ (Berichterstellung) in der *Sentinel Log Manager 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administration-Anleitung).

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-Betriebssystem installiert werden. Wird Sentinel Log Manager als Appliance installiert, erfolgt die Installation des Log Manager-Servers auf einem SLES 11-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 53.

Systemvoraussetzungen 2

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.

Hinweis: Die Anforderungen beziehen sich auf eine durchschnittliche Ereignisgröße von 300 Byte.

Die folgenden Hardwareanforderungen werden für ein Produktionssystem empfohlen, das 90 Tage Online-Daten speichert:

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
Maximale Ereignisquellen	Bis 1000	Bis 1000	Bis 2000
Maximale Ereignisrate	500	2500	7500

Anforderungen	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
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
Speicher	2 x 500 GB, 7,2 k RPM-Laufwerke (Hardware-RAID mit 256 MB Cache, RAID 1)	2 x 1 TB, 7,2 k RPM-Laufwerke (Hardware-RAID mit 256 MB Cache, RAID 1)	6 x 450 GB, 15 k RPM-Laufwerke (Hardware-RAID mit 512 MB Cache, RAID 10)

Hinweis:

- 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.
- Der vernetzte Speicherort muss als externes SAN (Storage Network Area) mit mehreren Laufwerken oder als NAS (Network-attached Storage) eingerichtet werden.
- 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.

Hinweis: 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-Server

- ❑ 1 Intel Xeon L5240 3 GHz (2 Core)-CPU
- ❑ 256 MB 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 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administration-Anleitung).

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:

- **Größe des Ereignisdatenspeichers:** {Anzahl Tage} x {Ereignisse pro Sekunde} x {durchschnittliche Ereignisgröße in Byte} x 0,000012 = erforderlicher Speicher in GB

  Ereignisgrößen bewegen sich üblicherweise in einem Bereich von 300 bis 1000 Byte.
- **Größe des Rohdatenspeichers:** {Anzahl Tage} x {Ereignisse pro Sekunde} x {durchschnittliche Rohdatengröße in Byte} x 0,000012 = erforderlicher Speicher in GB

  Die durchschnittliche Rohdatengröße für Syslog-Meldungen beträgt in der Regel 200 Byte.
- **Gesamtspeichergröße:** ({durchschnittliche Ereignisgröße in Byte} + {durchschnittliche Rohdatengröße in Byte}) x {Anzahl Tage} x {Ereignisse pro Sekunde} x 0,000012 = erforderlicher Gesamtspeicher in GB

Hinweis: Diese Zahlen stellen lediglich Schätzungen dar und hängen von der Größe Ihrer Ereignisdaten sowie von der Größe der komprimierten Daten ab.

Mit den oben genannten Formeln wird der Mindestspeicherplatz berechnet, der zum Speichern vollständig komprimierter Daten auf einem externen Speichersystem erforderlich ist. Wenn sich der lokale Speicher füllt, komprimiert Sentinel Log Manager die Daten und verschiebt sie von einem lokalen (teilweise komprimierten) in ein externes (vollständig komprimiertes) Speichersystem. Daher ist die Einschätzung der externen Speicherplatzanforderungen für die Datenaufbewahrung von entscheidender Bedeutung. Zur Verbesserung der Such- und Berichterstellungsleistung für aktuelle Daten können Sie den lokalen Speicherplatz über die Hardwareanforderungen von Sentinel Log Manager vergrößern. Dies ist jedoch nicht unbedingt erforderlich.

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

2.1.4 Virtuelle Umgebung

Sentinel Log Manager ist eingehend getestet und wird auf einem VMware ESX-Server vollständig unterstützt. Leistungsergebnisse in einer virtuellen Umgebung können mit den auf einem physischen Computer ermittelten Testergebnissen vergleichbar sein. Die virtuelle Umgebung sollte jedoch in Bezug auf Arbeitsspeicher, CPU, Speicherplatz und E/A mit den Empfehlungen für den physischen Computer identische Anforderungen erfüllen.

2.2 Unterstützte Betriebssysteme

Dieser Abschnitt enthält Informationen über unterstützte Betriebssysteme für den Sentinel Log Manager-Server und den Remote-Collector-Manager:

- Abschnitt 2.2.1, „Sentinel Log Manager“, auf Seite 20
- Abschnitt 2.2.2, „Collector Manager“, auf Seite 20

2.2.1 Sentinel Log Manager

Dieser Abschnitt ist nur relevant, wenn Sie Sentinel Log Manager auf einem vorhandenen Betriebssystem installieren.

- ❑ 64-Bit SUSE Linux Enterprise Server 11.
- ❑ 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 20
- „Windows“ auf Seite 21

Linux

- ❑ SUSE Linux Enterprise Server 10 SP2 (32- und 64-Bit)
- ❑ SUSE Linux Enterprise Server 11 (32- und 64-Bit)

Windows

- ❑ Windows Server 2003 (32- und 64-Bit)
- ❑ Windows Server 2003 SP2 (32-Bit und 64-Bit)
- ❑ Windows Server 2008 (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 21
- Abschnitt 2.3.2, „Windows“, auf Seite 21

2.3.1 Linux

- ❑ Mozilla Firefox 3.6

2.3.2 Windows

- ❑ Mozilla Firefox 3 (optimale Unterstützung für 3.6)
- ❑ Microsoft Internet Explorer 8 (optimale Unterstützung für 8.0)

Voraussetzungen für Internet Explorer 8

- Wenn die Sicherheitsstufe auf "Hoch" eingestellt ist, wird nach dem Anmelden in Novell 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. Nach diesem Vorgang werden die entsprechenden Ereignisquellen in der Sentinel Log Manager-Webkonsole unter der Registerkarte *Audit-Server* angezeigt.

Collectors, die zusätzliche Ereignisquellen unterstützen, können entweder über die Sentinel 6.1 Content-Website (http://support.novell.com/products/sentinel/sentinel61.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.

Installation auf einem vorhandenen SLES 11-System

3

In diesem Abschnitt wird die Installation von Sentinel Log Manager auf einem vorhandenen SUSE Linux Enterprise Server (SLES) 11-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 29.

Bevor Sie mit der Installation fortfahren, stellen Sie sicher, dass die in Kapitel 2, „Systemvoraussetzungen“, auf Seite 17 angegebenen Mindestanforderungen erfüllt sind.

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.
- ❑ 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

3.2 Standardinstallation

Bei der Standardinstallation wird Sentinel Log Manager mit allen Standardoptionen und einer 90-Tage-Probelizenz 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*> mit dem tatsächlichen Namen der Installationsdatei.
4. 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`
5. 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.
6. Lesen Sie die Endbenutzer-Lizenzvereinbarung und geben Sie `ja` oder `j` 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.
7. Geben Sie die Option zum Fortfahren mit der Standardinstallation an, wenn Sie dazu aufgefordert werden.

   Der Installationsvorgang wird mit dem 90-Tage-Evaluierungsschlüssel, der im Installationsprogramm enthalten ist, fortgesetzt. Dieser Lizenzschlüssel aktiviert den vollständigen Satz an Produktfunktionen für einen Testzeitraum von 90 Tagen. Sie können die Evaluierungslizenz zu jedem beliebigen Zeitpunkt während des Testzeitraums oder danach durch einen gekauften Lizenzschlüssel ersetzen.

8 Geben Sie das Passwort für den Administrator an.

9 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.

10 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 5, „Anmelden an der Weboberfläche“, auf Seite 45.

11 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 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administration-Anleitung).

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 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administration-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*> mit dem tatsächlichen Namen der Installationsdatei.

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

```
./install-slm
```

5 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.

6 Lesen Sie die Endbenutzer-Lizenzvereinbarung und geben Sie `ja` oder `j` 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.

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

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

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

   Weitere Informationen zu Lizenzschlüsseln finden Sie unter „Managing License Keys“ (Verwalten von Lizenzschlüsseln) im *Sentinel Log Manager 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administration-Anleitung).

10 Geben Sie das Passwort für den Administrator an.

11 Bestätigen Sie das Passwort für den Administrator.

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

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

14 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.

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

16 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.

17 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.

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

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

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

21 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.

22 (Bedingt) Wenn Sie die anonyme Suche ausgewählt haben, geben Sie das Suchattribut an und fahren Sie mit Schritt 25 fort.

23 (Bedingt) Wenn Sie die anonyme Suche in Schritt 21 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.

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

25 Geben Sie den Basis-DN an.

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

27 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 5, „Anmelden an der Weboberfläche“, auf Seite 45.

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*> mit dem tatsächlichen Namen der Installationsdatei.

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

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

Informationen zum Erstellen der Antwortdatei finden Sie unter Abschnitt 3.2, „Standardinstallation“, auf Seite 26. Die Installation wird mit den in der Antwortdatei gespeicherten Werten fortgesetzt.

5 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 5, „Anmelden an der Weboberfläche“, auf Seite 45.

6 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 1.1 Administration Guide“ (Sentinel Log Manager 1.1 Administration-Anleitung).

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 ein anderer Benutzer 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 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.

5 Akzeptieren Sie die Liste der Befehle.

   Die angezeigten Befehle werden ausgeführt.

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

   ```
   su novell
   ```

7 Geben Sie folgenden Befehl ein:

   ```
   ./install-slm
   ```

8 Um mit einer Sprache Ihrer Wahl fortzufahren, wählen Sie die neben der gewünschten Sprache angegebene Nummer aus.

   Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.

9 Lesen Sie die Endbenutzer-Lizenzvereinbarung und geben Sie `ja` oder `j` 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.

10 Sie werden aufgefordert, den Installationsmodus anzugeben.

- Wenn Sie mit der Standardinstallation fortfahren möchten, führen Sie Schritt 8 bis Schritt 11 unter Abschnitt 3.2, „Standardinstallation“, auf Seite 26 aus.
- Wenn Sie mit der benutzerdefinierten Installation fortfahren möchten, führen Sie Schritt 8 bis Schritt 23 unter Abschnitt 3.3, „Benutzerdefinierte Installation“, auf Seite 27 aus.

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

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

```
su root
```

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

```
./bin/root_install_finish
```

13 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 5, „Anmelden an der Weboberfläche“, auf Seite 45.

Installieren der Appliance

4

Mit Novell Sentinel Log Manager Appliance kann die auf SUSE Studio aufsetzende Software-Appliance ausgeführt werden. Diese kombiniert ein SUSE Linux Enterprise Server (SLES) 11-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:

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. Wird außerdem von der Sentinel Log Manager Appliance für den Aktualisierungsservice verwendet.
TCP 80	Wird für den Sentinel Log Manager-Webserver zur HTTP-Kommunikation an 8080 weitergeleitet. Wird außerdem von der Sentinel Log Manager Appliance für den Aktualisierungsservice verwendet.
TCP 8443	Wird für die HTTPS-Kommunikation verwendet. Wird außerdem von der Sentinel Log Manager Appliance für den Aktualisierungsservice 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.

Ports	Beschreibung
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_1.1.0.0_64_VMX.x86_64-0.777.0.vmx.tar.gz`
2. Richten Sie eine ESX-Datenablage ein, auf der das Appliance-Image installiert werden kann.
3. Melden Sie sich als Administrator an dem Server an, auf dem Sie die Appliance installieren möchten.
4. Geben Sie den folgenden Befehl ein, um das komprimierte Appliance-Image von dem Computer, auf dem VM Converter installiert ist, zu extrahieren:

   `tar zxvf <install_file>`

   Ersetzen Sie <*install_file*> durch den tatsächlichen Dateinamen.
5. Um das VMware-Image auf den ESX-Server zu importieren, verwenden Sie den VMware Converter und folgen Sie den Anweisungen auf dem Bildschirm des Installationsassistenten.
6. Melden Sie sich am ESX-Server an.
7. Wählen Sie das importierte VMware-Image der Appliance und klicken Sie auf das Symbol *Einschalten*.
8. Wählen Sie die gewünschte Sprache aus und klicken Sie auf *Weiter*.
9. Wählen Sie das Tastatur-Layout aus und klicken Sie auf *Weiter*.
10. Lesen und akzeptieren Sie die Novell SUSE Enterprise Server Software-Lizenzvereinbarung.
11. Lesen und akzeptieren Sie die Novell Sentinel Log Manager-Endbenutzer-Lizenzvereinbarung.

12 Geben Sie im Bildschirm für den Hostnamen und den Domänennamen die entsprechenden Namen ein. Stellen Sie sicher, dass die Option *Hostname speichern unter /etc/hosts* ausgewählt ist.

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

14 Führen Sie einen der folgenden Vorgänge aus:

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

15 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
```

---

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

17 Legen Sie das `root`-Passwort 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*.

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

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

20 Fahren Sie mit Abschnitt 4.6, „Einrichtung der Appliance im Anschluss an die Installation“, auf Seite 39 fort.

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_1.1.0.0_64_Xen.x86_64-0.777.0.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_1.1.0.0_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.1.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.1.0.0_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_1.1.0.0_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_1.1.0.0_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 speichern unter /etc/hosts* 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 II* 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 39 fort.

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 speichern unter /etc/hosts* 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 II" 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 verwenden Sie YaST an der Befehlszeile der Appliance. 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 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.

16 Fahren Sie mit Abschnitt 4.6, „Einrichtung der Appliance im Anschluss an die Installation“, auf Seite 39 fort.

4.6 Einrichtung der Appliance im Anschluss an die Installation

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.

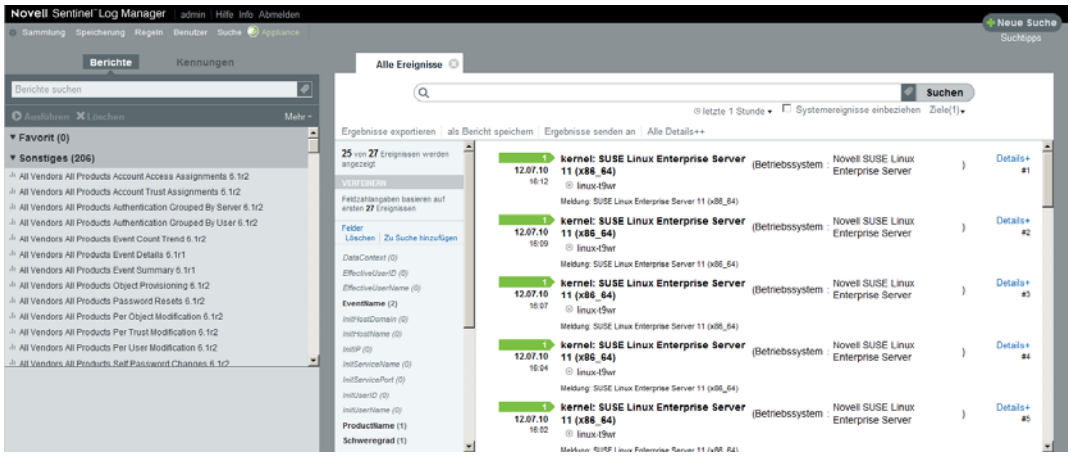
2 Sie können die Sentinel Log Manager Appliance für die Datenspeicherung und die Datensammlung konfigurieren. Weitere Informationen zum Konfigurieren der Appliance finden Sie im *Sentinel Log Manager 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administration-Anleitung).

3 Informationen zum Registrieren für Aktualisierungen finden Sie unter Abschnitt 4.8, „Registrieren für Aktualisierungen“, auf Seite 42.

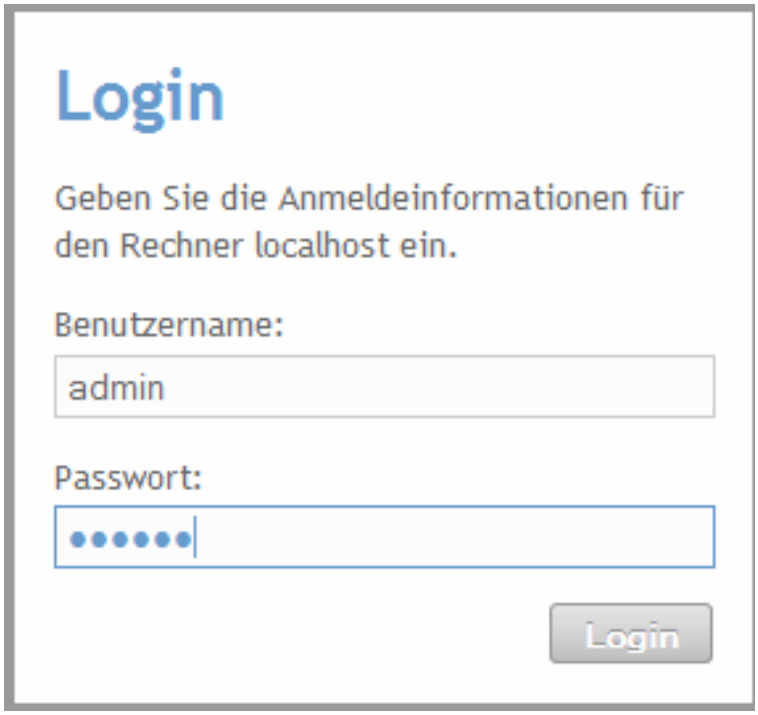
4.7 Konfigurieren von WebYaST

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).

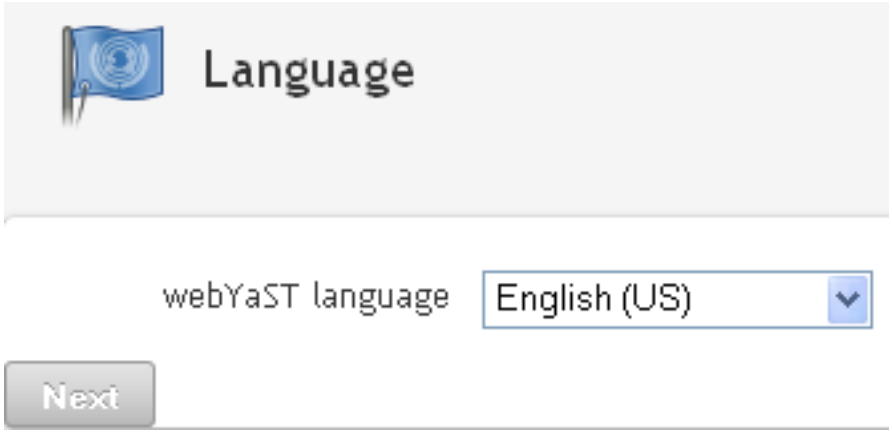
1 Melden Sie sich an der Sentinel Log Manager Appliance an.



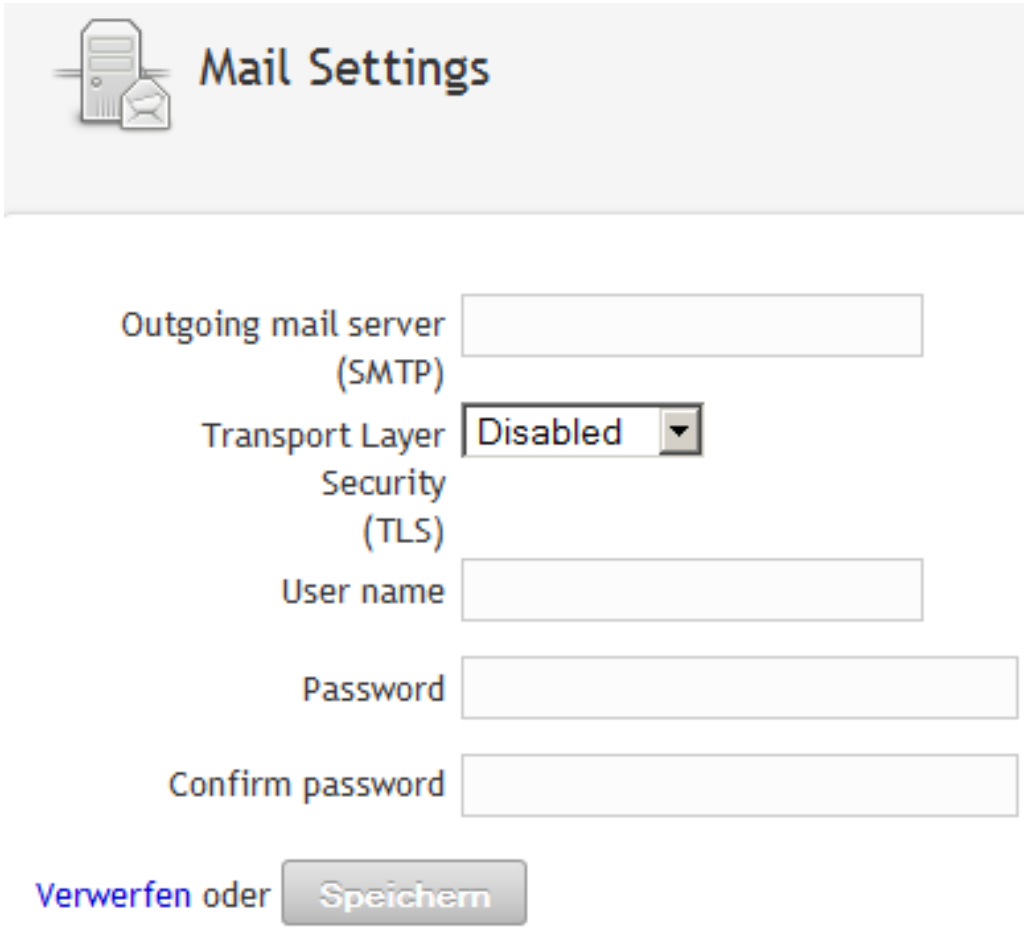
2 Klicken Sie auf *Appliance*.



3 Geben Sie die Anmeldeberechtigung für das System an und klicken Sie auf *Anmelden*.



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



5 Legen Sie Details zum Konfigurieren des Mailservers fest und klicken Sie auf *Speichern*.

Die Registrierungsseite wird angezeigt.

6 Konfigurieren Sie Sentinel Log Manager-Server zum Empfang von Aktualisierungen, wie in Abschnitt 4.8, „Registrieren für Aktualisierungen“, auf Seite 42 beschrieben.

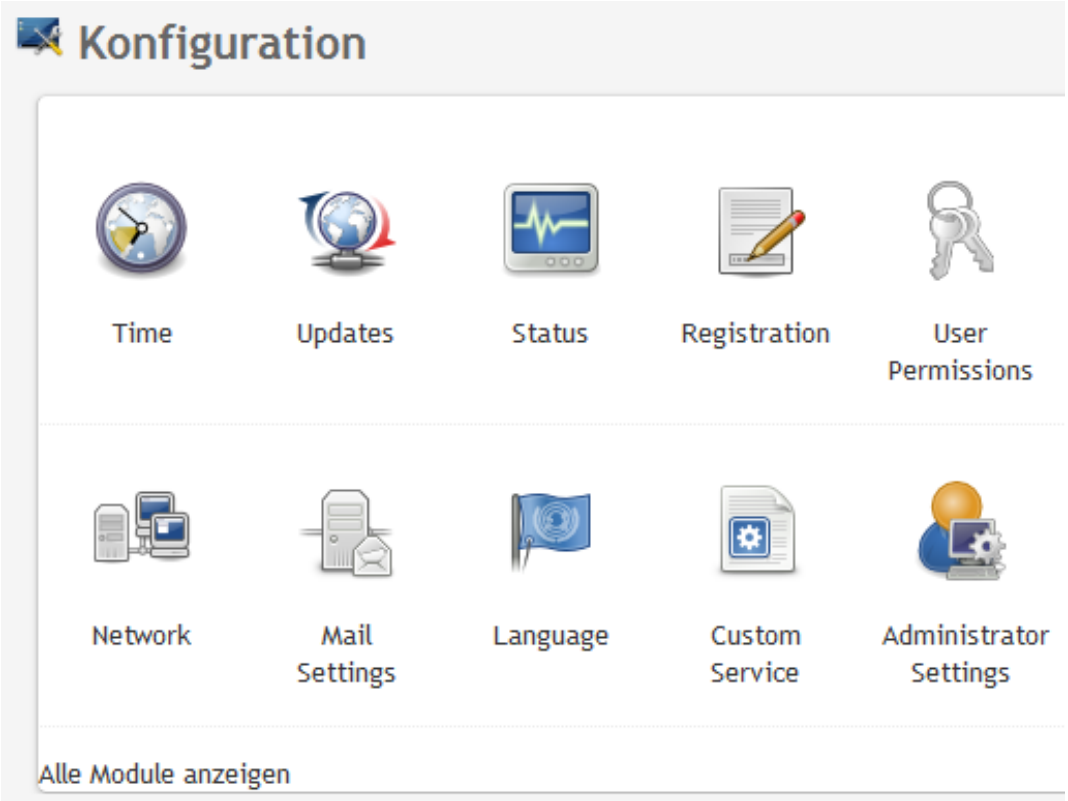
7 Klicken Sie auf *Weiter*, um die Ersteinrichtung fertig zu stellen.

4.8 Registrieren für Aktualisierungen

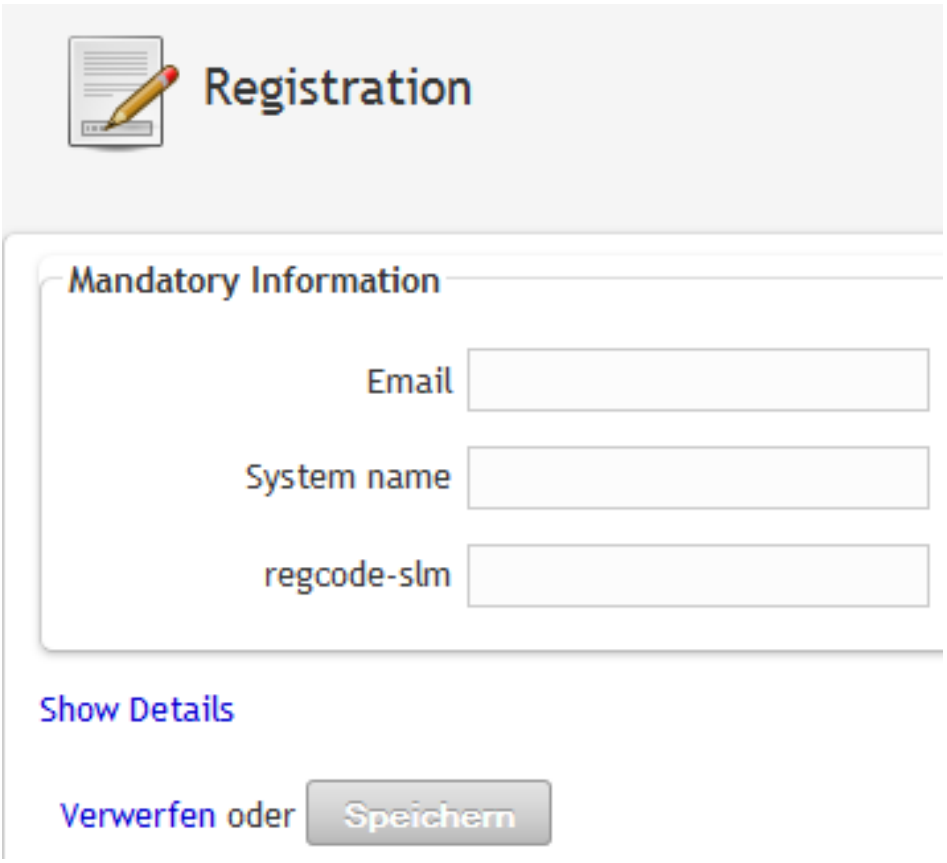
1 Melden Sie sich an der Sentinel Log Manager Appliance an.

Die Sentinel Log Manager-Web-Benutzeroberfläche wird angezeigt.

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



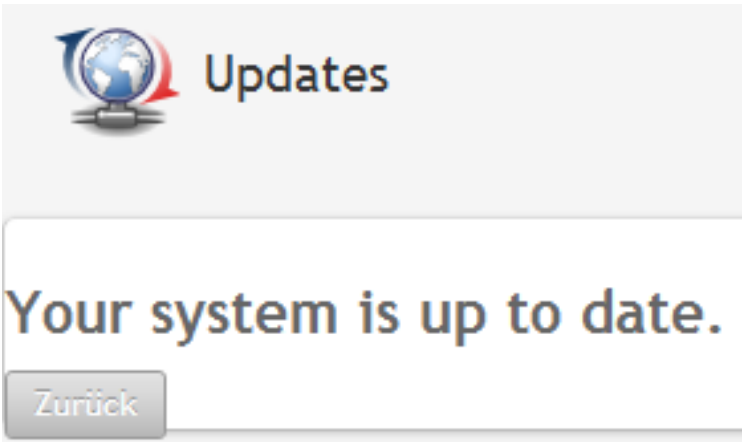
3 Klicken Sie auf *Registrierung*.



4 Geben Sie den Registrierungscode für die Appliance an.

5 Klicken Sie auf *Speichern*.

6 Klicken Sie auf *Aktualisieren*, um zu überprüfen, ob Aktualisierungen vorhanden sind. Die daraufhin angezeigte Seite gibt an, ob Aktualisierungen vorhanden sind.

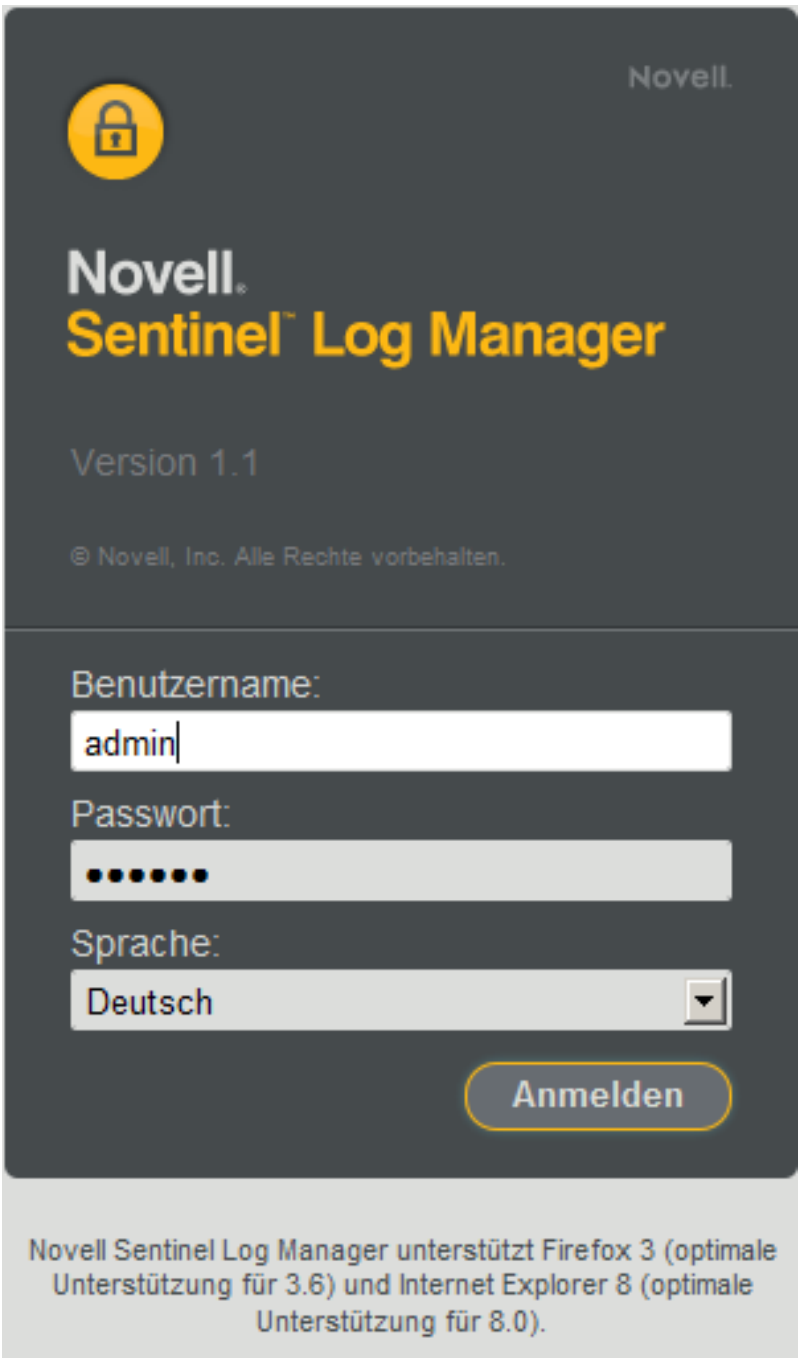


Anmelden an der Weboberfläche

5

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 21.
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.



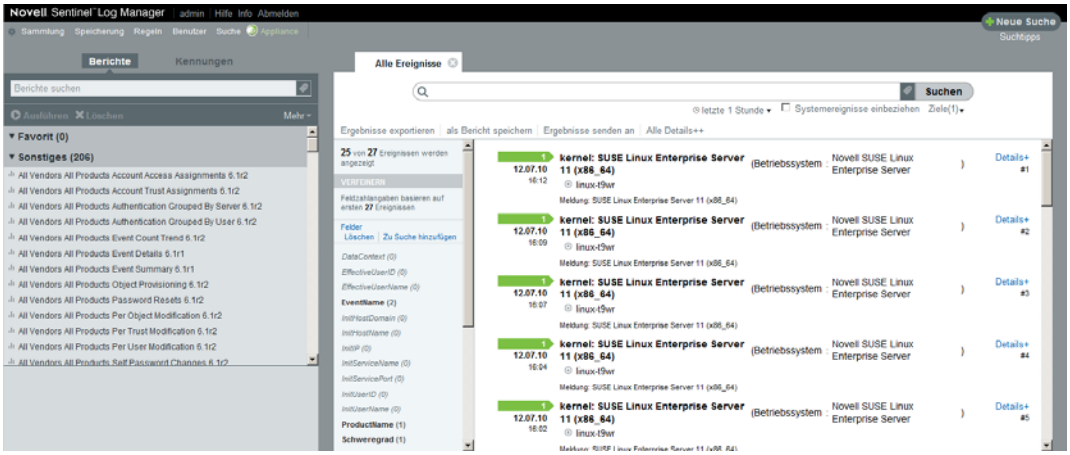
4 Geben Sie den Benutzernamen und das Passwort für den Sentinel Log Manager-Administrator ein.

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.



Aufrüsten von Sentinel Log Manager

6

Sie können Novell Sentinel Log Manager von 1.0.0.4 oder höher auf Sentinel Log Manager 1.1 aufrüsten. Verwenden Sie dazu das Aufrüstungs-Skript.

6.1 Aufrüsten von Version 1.0 auf Version 1.1

1. Wenn Ihre Sentinel Log Manager-Serverversion älter als Version 1.0.0.4. ist, müssen Sie sie zunächst auf Version 1.0.0.4 oder höher aufrüsten.
2. Laden Sie die Installationsdateien von der Novell-Download-Website herunter und kopieren Sie sie.
3. Melden Sie sich als `root` an dem Server an, auf dem Sie Sentinel Log Manager installieren möchten.
4. 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_1.0_x86-64/bin/server.sh stop`
5. 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.
6. Geben Sie den folgenden Befehl ein, um das Skript `install-slm` zum Aufrüsten von Sentinel Log Manager auszuführen:

   `./install-slm`
7. Um mit einer Sprache Ihrer Wahl fortzufahren, wählen Sie die neben der gewünschten Sprache angegebene Nummer aus.

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

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

Die vorhandene Sentinel Log Manager 1.0-Installation bleibt bis auf folgende Ausnahmen unverändert:

- 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/eventuate` und `<1.0>/data/rawdata` an den Standort der Version 1.1 verschoben, da die Verzeichnisse "eventdata" und "rawdata" üblicherweise sehr 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.

10 Wenn die Sentinel Log Manager 1.1-Installation erfolgreich abgeschlossen wird und der Server funktionsfähig ist, müssen Sie den folgenden Befehl ausführen, 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_1.0_x86-64
```

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

6.2 Aktualisieren des Collector-Managers

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_upgrade_installer.zip` entweder zu öffnen oder auf dem lokalen Computer zu speichern. Speichern Sie die Datei.

4 Kopieren Sie die Datei an einen temporären Speicherort.

5 Extrahieren Sie den Inhalt der `.zip`-Datei.

6 Führen Sie als Eigentümer der Collector-Manager-Installation abhängig von Ihrem Betriebssystem eine der folgenden Aufrüstungsdateien 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.

7 Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation abzuschließen.

8 Führen Sie einen Neustart Ihres Computers durch.

6.3 Migrieren von 1.0 auf 1.1 Appliance

Wenn Sie Sentinel Log Manager 1.0 installiert haben und auf Sentinel Log Manager Appliance 1.1 migrieren möchten, führen Sie die unten angegebenen Schritte aus, um Daten und Konfiguration zu migrieren.

1 (Bedingt) Wenn die Version des installierten Sentinel Log Manager niedriger ist als 1.0 hotfix 4, rüsten Sie sie auf Sentinel Log Manager 1.0 hotfix 5 auf. Dies ist der aktuell verfügbare Hotfix. Laden Sie den Hotfix von der Novell Patch Download-Website (http://download.novell.com/protected/Summary.jsp?buildid=VgZ3aerzjYc~) herunter.

Hinweis: Zum Herunterladen von Patches müssen Sie als Benutzer registriert sein. Falls Sie nicht registriert sind, klicken Sie auf "Registrieren", um ein Benutzerkonto auf der Patch-Download-Website zu erstellen.

---

2 Rüsten Sie auf Sentinel Log Manager 1.1 auf. Weitere Informationen finden Sie in Abschnitt 6.1, „Aufrüsten von Version 1.0 auf Version 1.1“, auf Seite 49.

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

```
su -novell
```

4 Geben Sie den folgenden Befehl ein, um das Verzeichnis `/bin` zu ändern:

```
cd /opt/novell/sentinel_log_mgr/bin
```

5 Führen Sie den folgenden Befehl aus, um eine vollständige Sicherung der Daten und Konfiguration von Sentinel Log Manager 1.1 zu erstellen.

```
./backup_util.sh -m backup -c -e -l -r -s -w -f $APP_HOME/data/
<backupfilename>
```

Ersetzen Sie <*backupfilename*> durch einen Dateinamen zum Speichern der Sicherungsdaten.

Weitere Informationen zum Sichern von Daten finden Sie unter „Backup and Restoring Data“ (Sichern und Wiederherstellen von Daten).

6 Installieren Sie Sentinel Log Manager Appliance 1.1 auf einem separaten Computer. Weitere Informationen finden Sie unter Kapitel 4, „Installieren der Appliance“, auf Seite 33.

7 Kopieren Sie die Datei mit den gesicherten Daten auf eine neu installierte Sentinel Log Manager 1.1-Appliance.

8 Geben Sie folgenden Befehl ein:

```
chown novell:novell <backfupfilename>
```

9 Geben Sie den folgenden Befehl ein, um das Verzeichnis `/bin` zu ändern:

```
cd /opt/novell/sentinel_log_mgr/bin
```

10 Führen Sie den folgenden Befehl aus, um die von der Sentinel Log Manager 1.1-Anwendung gesicherten Daten vollständig wiederherzustellen:

```
./backup_util.sh -m restore -f $APP_HOME/data/<backupfilename>
```

Weitere Informationen finden Sie unter „Backing Up and Restoring Data“ (Sichern und Wiederherstellen von Daten).

Installieren zusätzlicher Collector-Manager-Instanzen

7

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.

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:** Wenn Sie Datei-Caching aktivieren, kann der Remote-Collector-Manager 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 *Sammlung* > *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. Lassen Sie den Standardport für den Nachrichtenbus (61616) unverändert und geben Sie den Hostnamen des Kommunikationsservers an. Klicken Sie anschließend auf *Weiter*.
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.

    Hinweis: 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.

    ---
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.

Deinstallieren von Sentinel Log Manager

8

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 1.1 Administration Guide* (Sentinel Log Manager 1.1 Administration-Anleitung).

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 einem vorhandenen SLES 11-System

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/_unist
   ```
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“ auf Seite 57
- „Windows“ auf Seite 57

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`.

Fehlersuche bei der Installation

A

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

A.1 Installationsfehler aufgrund einer falschen Netzwerkkonfiguration

Beim ersten Booten stellt das Installationsprogramm fest, dass die Netzwerkeinstellungen falsch sind. Es wird eine Fehlermeldung angezeigt. Wenn das Netzwerk nicht verfügbar ist, tritt beim Installieren von Sentinel Log Manager auf der Appliance ein Fehler auf.

Zur Behebung dieses Problems müssen die Netzwerkeinstellungen ordnungsgemäß konfiguriert werden. Beim Prüfen der Konfiguration sollte der Befehl `ifconfig` die gültige IP-Adresse und der Befehl `hostname -f` den gültigen Hostnamen zurückgeben.

A.2 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 Schritt 2 kopierte MAC-Adresse.

6 Speichern und schließen Sie die Datei.

7 Öffnen Sie die virtuelle Maschine in VMware Player.

A.3 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 Ändern Sie den Eintrag ESEC_USER im Verzeichnis `config/esecuser.properties` in `novell`.

4 Melden Sie sich als `root`-Benutzer an und rüsten Sie auf Sentinel Log Manager 1.1 auf. Weitere Informationen zum Aufrüsten finden Sie in Abschnitt 6.1, „Aufrüsten von Version 1.0 auf Version 1.1“, auf Seite 49.

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.