

Guida all'installazione

Novell[®] Sentinel Log Manager

1.1

July 08, 2010

www.novell.com



Note legali

Novell, Inc. non rilascia alcuna dichiarazione e non fornisce alcuna garanzia in merito al contenuto o all'uso di questa documentazione e in particolare non riconosce alcuna garanzia, espressa o implicita, di commerciabilità o idoneità per uno scopo specifico. Novell, Inc. si riserva inoltre il diritto di aggiornare la presente pubblicazione e di modificarne il contenuto in qualsiasi momento, senza alcun obbligo di notificare tali modifiche a qualsiasi persona fisica o giuridica.

Inoltre, Novell, Inc. non rilascia alcuna dichiarazione e non fornisce alcuna garanzia in merito a qualsiasi software e in particolare non riconosce alcuna garanzia, espressa o implicita, di commerciabilità o idoneità per uno scopo specifico. Novell, Inc. si riserva inoltre il diritto di modificare qualsiasi parte del software Novell in qualsiasi momento, senza alcun obbligo di notificare tali modifiche a qualsiasi persona fisica o giuridica.

Qualsiasi informazione tecnica o prodotto fornito in base a questo Contratto può essere soggetto ai controlli statunitensi relativi alle esportazioni e alla normativa sui marchi di fabbrica in vigore in altri paesi. L'utente si impegna a rispettare la normativa relativa al controllo delle esportazioni e a ottenere qualsiasi licenza o autorizzazione necessaria per esportare, riesportare o importare prodotti finali. L'utente si impegna inoltre a non esportare o riesportare verso entità incluse negli elenchi di esclusione delle esportazioni statunitensi o a qualsiasi paese sottoposto a embargo o che sostiene movimenti terroristici, come specificato nella legislazione statunitense in materia di esportazioni. L'utente accetta infine di non utilizzare i prodotti finali per utilizzi correlati ad armi nucleari, missilistiche o biochimiche. Per ulteriori informazioni sull'esportazione di software Novell, vedere la [pagina Web sui servizi commerciali internazionali di Novell \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/). Novell non si assume alcuna responsabilità relativa al mancato ottenimento, da parte dell'utente, delle autorizzazioni di esportazione necessarie.

Copyright © 2009-2010 Novell, Inc. Tutti i diritti riservati. È vietato riprodurre, fotocopiare, memorizzare su un sistema di recupero o trasmettere la presente pubblicazione o parti di essa senza l'espresso consenso scritto dell'editore.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Documentazione online: per accedere alla documentazione online più recente relativa a questo o ad altri prodotti Novell, vedere la [pagina Web della documentazione Novell \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Marchi di fabbrica di Novell

Per informazioni sui marchi di fabbrica di Novell, vedere [l'elenco di marchi di fabbrica e di servizio di Novell \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiali di terze parti

Tutti i marchi di fabbrica di terze parti appartengono ai rispettivi proprietari.

Sommario

Informazioni sulla Guida	7
1 Introduzione	9
1.1 Panoramica sul prodotto	9
1.1.1 Origini evento	11
1.1.2 Gestione origini eventi	12
1.1.3 Raccolta dei dati	12
1.1.4 Gestione servizi di raccolta	13
1.1.5 Memorizzazione dei dati	13
1.1.6 Ricerca e generazione di rapporti	14
1.1.7 Collegamento Sentinel	14
1.1.8 Interfaccia utente basata sul Web	14
1.2 Panoramica relativa all'installazione	15
2 Requisiti di sistema	17
2.1 Requisiti hardware	17
2.1.1 Server di Sentinel Log Manager	17
2.1.2 Server della Gestione servizi di raccolta	18
2.1.3 Stima dei requisiti per la memorizzazione dei dati	19
2.1.4 Ambiente virtuale	20
2.2 Sistemi operativi supportati	20
2.2.1 Sentinel Log Manager	20
2.2.2 Gestione servizi di raccolta	20
2.3 Browser supportati	21
2.3.1 Linux	21
2.3.2 Windows	21
2.4 Ambiente virtuale supportato	21
2.5 Connettori supportati	22
2.6 Origini evento supportate	22
3 Installazione su un sistema SLES 11 esistente	25
3.1 Istruzioni preliminari	25
3.2 Installazione standard	26
3.3 Installazione personalizzata	27
3.4 Installazione invisibile all'utente	29
3.5 Installazione non root	30
4 Installazione dell'applicazione	33
4.1 Istruzioni preliminari	33
4.2 Porte utilizzate	33
4.2.1 Porte aperte nel firewall	34
4.2.2 Porte utilizzate localmente	34
4.3 Installazione dell'applicazione VMware	35
4.4 Installazione dell'applicazione Xen	36
4.5 Installazione dell'applicazione sull'hardware	38
4.6 Configurazione post-installazione per l'applicazione	39

4.7	Configurazione di WebYaST	39
4.8	Registrazione degli aggiornamenti	41
5	Effettuare il login all'interfaccia Web	45
6	Esecuzione dell'upgrade di Sentinel Log Manager	49
6.1	Esecuzione dell'upgrade dalla versione 1.0 alla versione 1.1	49
6.2	Esecuzione dell'upgrade della Gestione dei servizi di raccolta	50
6.3	Esecuzione della migrazione dall'applicazione 1.0 a 1.1	51
7	Installazione di Gestioni servizi di raccolta aggiuntive	53
7.1	Istruzioni preliminari	53
7.2	Vantaggi apportati dalla presenza di più Gestioni servizi di raccolta	53
7.3	Installazione di Gestioni servizi di raccolta aggiuntive	54
8	Disinstallazione di Sentinel Log Manager	55
8.1	Disinstallazione dell'applicazione	55
8.2	Disinstallazione da un sistema SLES 11 esistente	55
8.3	Disinstallazione di Gestione servizi di raccolta	56
8.3.1	Disinstallazione della Gestione servizi di raccolta su Linux	56
8.3.2	Disinstallazione della Gestione servizi di raccolta su Windows	56
8.3.3	Pulizia manuale delle directory	57
A	Risoluzione dei problemi relativi all'installazione	59
A.1	Installazione non riuscita a causa di una configurazione della rete non corretta	59
A.2	Problema di configurazione della rete con VMware Player 3 in SLES 11	59
A.3	Esecuzione dell'upgrade di Gestione log installata come utente non root diverso dall'utente novell	60
	Terminologia di Sentinel	61

Informazioni sulla Guida

In questa guida viene fornita una panoramica di Novell Sentinel Log Manager e della relativa procedura di installazione.

- ◆ Capitolo 1, “Introduzione”, a pagina 9
- ◆ Capitolo 2, “Requisiti di sistema”, a pagina 17
- ◆ Capitolo 3, “Installazione su un sistema SLES 11 esistente”, a pagina 25
- ◆ Capitolo 4, “Installazione dell'applicazione”, a pagina 33
- ◆ Capitolo 5, “Effettuare il login all'interfaccia Web”, a pagina 45
- ◆ Capitolo 6, “Esecuzione dell'upgrade di Sentinel Log Manager”, a pagina 49
- ◆ Capitolo 7, “Installazione di Gestioni servizi di raccolta aggiuntive”, a pagina 53
- ◆ Capitolo 8, “Disinstallazione di Sentinel Log Manager”, a pagina 55
- ◆ Appendice A, “Risoluzione dei problemi relativi all'installazione”, a pagina 59
- ◆ “Terminologia di Sentinel” a pagina 61

Destinatari

La presente Guida è rivolta agli amministratori e agli utenti finali della Gestione log di Novell Sentinel.

Feedback

È possibile inviare i propri commenti e suggerimenti relativi a questa guida e agli altri documenti forniti con questo prodotto. Utilizzare la funzione Commenti utente, presente in fondo a ogni pagina della documentazione online, oppure visitare il [sito Web relativo al feedback sulla documentazione di Novell](http://www.novell.com/documentation/feedback.html) (<http://www.novell.com/documentation/feedback.html>) e immettere i propri commenti.

Documentazione aggiuntiva

Per ulteriori informazioni sulla creazione di plug-in personalizzati (ad esempio, JasperReports), visitare la [pagina Web di Sentinel SDK](http://developer.novell.com/wiki/index.php/Develop_to_Sentinel) (http://developer.novell.com/wiki/index.php/Develop_to_Sentinel). L'ambiente di creazione per i plug-in dei rapporti di Sentinel Log Manager è identico a quanto documentato per Novell Sentinel.

Per ulteriori informazioni sulla documentazione relativa a Sentinel, fare riferimento al [sito Web della documentazione di Sentinel](http://www.novell.com/documentation/sentinel61/index.html) (<http://www.novell.com/documentation/sentinel61/index.html>).

Per la documentazione aggiuntiva sulla configurazione di Sentinel Log Manager, consultare la *Sentinel Log Manager 1.1 Administration Guide (Guida all'amministrazione di Sentinel Log Manager 1.1, in lingua inglese)*.

Come contattare Novell

- ◆ Sito Web di Novell (<http://www.novell.com>)
- ◆ Supporto tecnico Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)

- ◆ Autosupporto Novell (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- ◆ Sito per il download delle patch (<http://download.novell.com/index.jsp>)
- ◆ Supporto Novell 24 ore su 24, 7 giorni su 7 (<http://www.novell.com/company/contact.html>)
- ◆ TID di Sentinel (<http://support.novell.com/products/sentinel>)
- ◆ Forum di supporto della comunità di Sentinel (<http://forums.novell.com/novell-product-support-forums/sentinel/>)

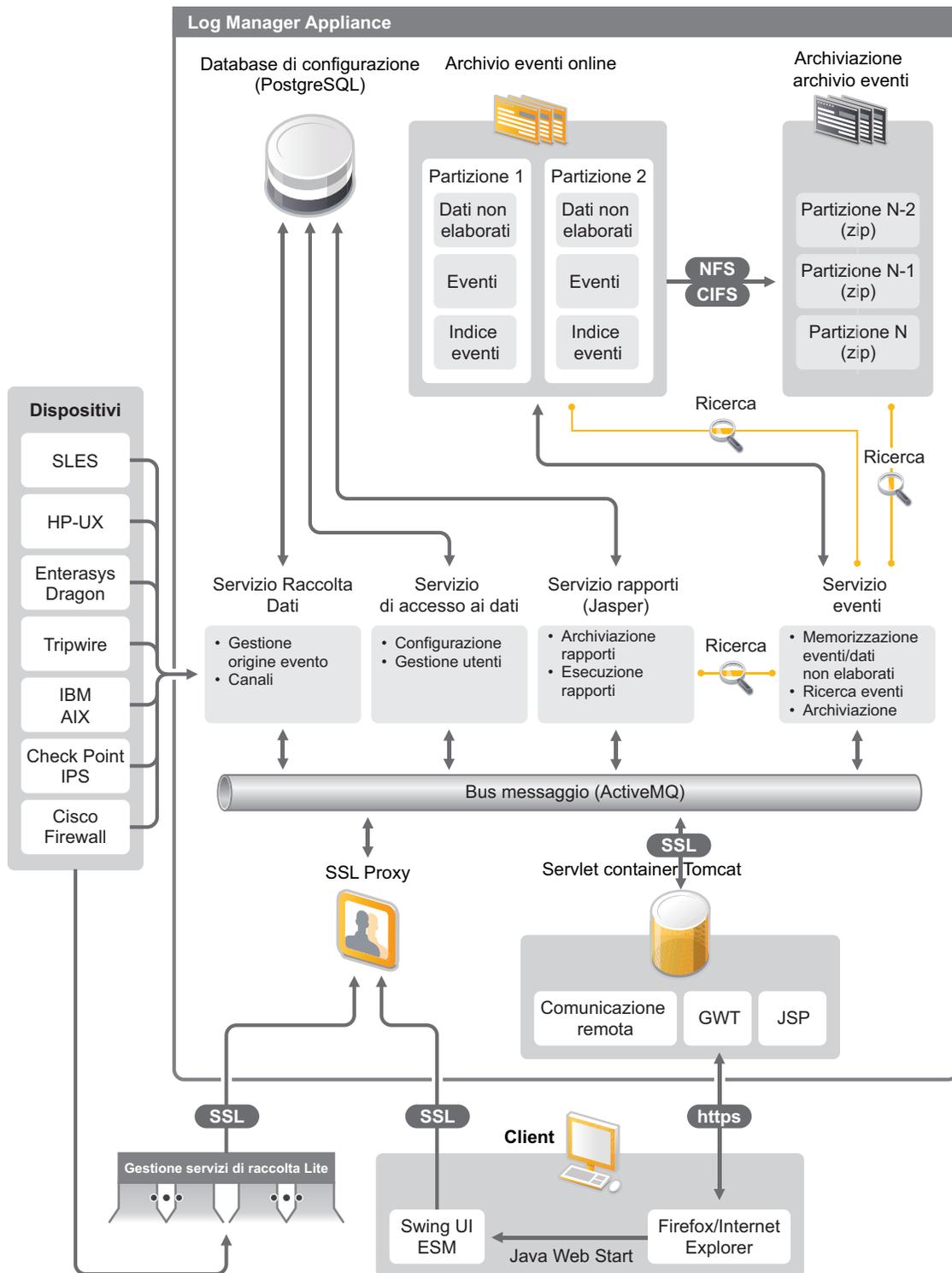
Novell Sentinel Log Manager consente di raccogliere e gestire dati da un'ampia gamma di dispositivi e applicazioni, compresi sistemi di rilevamento intrusioni, firewall, sistemi operativi, router, server Web, database, commutatori, mainframe e origini evento di antivirus. Novell Sentinel Log Manager offre elaborazioni ad alta frequenza di eventi, permanenza dei dati a lungo termine, permanenza dei dati basata sulle norme, aggregazione dei dati per area nonché la possibilità di eseguire ricerche e generare rapporti con estrema facilità per una vasta gamma di applicazioni e dispositivi.

- ♦ [Sezione 1.1, “Panoramica sul prodotto”, a pagina 9](#)
- ♦ [Sezione 1.2, “Panoramica relativa all'installazione”, a pagina 15](#)

1.1 Panoramica sul prodotto

Novell Sentinel Log Manager 1.1 offre alle aziende una soluzione di gestione dei log flessibile e scalabile. Novell Sentinel Log Manager è una soluzione di gestione dei log, creata per fornire tutte le attività principali di gestione e raccolta dei log e distribuire una risposta completa mirata a ridurre i costi, la complessità del rischio di gestione e a semplificare i requisiti di conformità.

Figura 1-1 Architettura di Novell Sentinel Log Manager



Novell Sentinel Log Manager dispone delle seguenti funzionalità:

- ♦ Le capacità di ricerca distribuita consentono ai clienti di eseguire le ricerche degli eventi raccolti non solo sul server locale di Sentinel Log Manager ma anche su uno o più server Sentinel Log Manager da un'unica console centralizzata.
- ♦ I rapporti di conformità esistenti semplificano il task di generazione dei rapporti di conformità per la revisione e l'analisi forense.
- ♦ Grazie all'utilizzo di tecnologia di memorizzazione non proprietaria, i clienti possono potenziare la propria infrastruttura esistente per gestire ulteriormente i costi.
- ♦ Un'interfaccia utente migliorata basata su browser supporta la raccolta, la memorizzazione, la generazione dei rapporti e la realizzazione delle ricerche dei dati di log per facilitare e rendere più efficaci i task di monitoraggio e gestione.
- ♦ I controlli e le personalizzazioni differenziati ed efficienti per amministratori IT, possibili grazie alle nuove funzionalità di autorizzazione per gruppi e utenti, forniscono una migliore trasparenza nell'intera attività dell'infrastruttura IT.

Questa sezione contiene le seguenti informazioni:

- ♦ [Sezione 1.1.1, “Origini evento”, a pagina 11](#)
- ♦ [Sezione 1.1.2, “Gestione origini eventi”, a pagina 12](#)
- ♦ [Sezione 1.1.3, “Raccolta dei dati”, a pagina 12](#)
- ♦ [Sezione 1.1.4, “Gestione servizi di raccolta”, a pagina 13](#)
- ♦ [Sezione 1.1.5, “Memorizzazione dei dati”, a pagina 13](#)
- ♦ [Sezione 1.1.6, “Ricerca e generazione di rapporti”, a pagina 14](#)
- ♦ [Sezione 1.1.7, “Collegamento Sentinel”, a pagina 14](#)
- ♦ [Sezione 1.1.8, “Interfaccia utente basata sul Web”, a pagina 14](#)

1.1.1 Origini evento

Novell Sentinel Log Manager raccoglie i dati dalle origini evento che generano i log per syslog, log degli eventi Windows, file, database, SNMP, Novell Audit, Security Device Event Exchange (SDEE), Check Point Open Platforms for Security (OPSEC) e altri meccanismi e protocolli di memorizzazione.

Sentinel Log Manager supporta tutte le origini evento, sempre che siano servizi di raccolta compatibili per l'analisi dei dati provenienti da tutte le origini evento menzionate. Novell Sentinel Log Manager fornisce i servizi di raccolta per numerose origini evento. Il Servizio di raccolta eventi generico raccoglie ed elabora i dati provenienti da origini evento sconosciute dotate di servizi di raccolta compatibili.

Le origini evento per la raccolta dei dati possono essere configurate utilizzando l'interfaccia Gestione origine eventi.

Per un elenco completo delle origini evento supportate, vedere [Sezione 2.6, “Origini evento supportate”, a pagina 22](#).

1.1.2 Gestione origini eventi

Grazie all'interfaccia Gestione origine eventi è possibile importare e configurare i connettori e i servizi di raccolta di Sentinel 6.0 e 6.1.

I seguenti task possono essere realizzati mediante la visualizzazione in diretta della finestra Gestione origini eventi:

- ◆ Aggiungere o modificare le connessioni alle origini evento mediante le configurazioni guidate.
- ◆ Visualizzare in tempo reale lo stato delle connessioni alle origini evento.
- ◆ Importare o esportare le configurazioni delle origini evento dalla o alla visualizzazione in diretta.
- ◆ Visualizzare e configurare i connettori e i servizi di raccolta installati con Sentinel.
- ◆ Importare o esportare i connettori e i servizi di raccolta da o a un archivio centralizzato.
- ◆ Controllare il flusso dei dati tramite i connettori e i servizi di raccolta configurati.
- ◆ Visualizzare le informazioni sui dati non elaborati.
- ◆ Progettare, configurare e creare i componenti di gerarchia dell'origine evento ed eseguire le azioni necessarie mediante tali componenti.

Per ulteriori informazioni, consultare la sezione relativa alla Gestione origini eventi della *Guida dell'utente di Sentinel* (<http://www.novell.com/documentation/sentinel61/#admin>).

1.1.3 Raccolta dei dati

Novell Sentinel Log Manager raccoglie i dati dalle origini evento configurate mediante il supporto dei connettori e dei servizi di raccolta.

I servizi di raccolta sono degli script che analizzano sintatticamente i dati, i quali provengono da origini evento di vario tipo, nella struttura eventi normalizzata di Sentinel oppure, in alcuni casi, raccolgono dati di formato diverso provenienti da origini evento esterne. Ogni servizio di raccolta deve essere installato insieme a un connettore compatibile. I connettori semplificano la connettività tra i servizi di raccolta di Sentinel Log Manager e le origini evento o le origini dati.

Grazie al supporto fornito mediante un'interfaccia utente basata su Web migliorata per syslog e Novell Audit, Novell Sentinel Log Manager consente di raccogliere i log da origini evento diverse in modo molto più semplice.

Novell Sentinel Log Manager consente di raccogliere i dati utilizzando una vasta gamma di metodi di connessione:

- ◆ Il connettore Syslog accetta e configura automaticamente le origini dati syslog che inviano i dati mediante i protocolli User Datagram Protocol (UDP), Transmission Control Protocol (TCP) oppure mediante il protocollo sicuro Transport Layer System (TLS).
- ◆ Il connettore Audit accetta e configura automaticamente le origini dati Novell abilitate per la revisione.
- ◆ Il connettore di file legge i file di log.
- ◆ Il connettore SNMP riceve i trap SNMP.
- ◆ Il connettore JDBC legge i dati provenienti dalle tabelle del database.
- ◆ Il connettore WMS effettua l'accesso ai log degli eventi Windows sui desktop e sui server.

- ♦ Il connettore SDEE connette i dispositivi che supportano il protocollo SDEE come, ad esempio, i dispositivi Cisco.
- ♦ Il connettore Log Export API (LEA) per i dispositivi Check Point consente l'integrazione tra i servizi di raccolta Sentinel e i server firewall Check Point.
- ♦ Il connettore di collegamento a Sentinel accetta i dati provenienti da altri server di Novell Sentinel Log Manager.
- ♦ Il connettore dei processi accetta i dati provenienti dai processi personalizzati che restituiscono i log degli eventi.

È possibile acquistare anche un'ulteriore licenza per effettuare il download dei connettori per SAP e i sistemi operativi mainframe.

Per ottenere la licenza, chiamare il numero 1-800-529-3400 oppure contattare il [supporto tecnico Novell \(http://support.novell.com\)](http://support.novell.com).

Per ulteriori informazioni sulla configurazione dei connettori, fare riferimento alla relativa documentazione nel [sito Web del contenuto di Sentinel \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html).

Per ulteriori informazioni sulla configurazione della raccolta di dati, consultare “[Configuring Data Collection \(Configurazione della raccolta dei dati\)](#)” nella *Guida all'amministrazione di Sentinel Log Manager 1.1*.

Nota: È necessario importare ed effettuare sempre il download della versione più recente dei servizi di raccolta e dei connettori. I servizi di raccolta e i connettori aggiornati vengono pubblicati periodicamente nel [sito Web di contenuto di Sentinel 6.1 \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html). Gli aggiornamenti ai connettori e ai servizi di raccolta comprendono correzioni, supporto per eventi aggiuntivi e miglioramenti da apportare alle prestazioni.

1.1.4 Gestione servizi di raccolta

La Gestione servizi di raccolta offre un punto di raccolta dei dati flessibile per Sentinel Log Manager. Durante l'installazione di Novell Sentinel Log Manager, di default viene installata anche un'istanza di Gestione servizi di raccolta. Tuttavia, le istanze di Gestione servizi di raccolta possono essere installate in modalità remota nelle posizioni della rete che si reputano più adatte. Tali istanze remote eseguono i connettori e i servizi di raccolta e inoltrano i dati raccolti a Novell Sentinel Log Manager affinché possano essere memorizzati ed elaborati.

Per informazioni sull'installazione di ulteriori istanze di Gestione servizi di raccolta, fare riferimento a “[Installazione di Gestioni servizi di raccolta aggiuntive](#)” a pagina 54.

1.1.5 Memorizzazione dei dati

I dati procedono dai componenti della raccolta di dati verso quelli specifici per la memorizzazione dei dati. Tali componenti utilizzano un sistema di memorizzazione dei dati e indicizzazione basato su file per mantenere i dati di log dei dispositivi raccolti e un database PostgreSQL che consente di conservare i dati di configurazione di Novell Sentinel Log Manager.

I dati vengono memorizzati in un formato compresso nel file system del server, quindi vengono memorizzati in un'ubicazione configurata per la memorizzazione a lungo termine. I dati possono essere memorizzati localmente oppure in una condivisione SMB (CIFS) o NFS il cui montaggio sia

stato realizzato in modalità remota. I file di dati vengono eliminati dalle ubicazioni di memorizzazione in rete o locali in base alla pianificazione configurata nella norma di permanenza dei dati

Le norme di permanenza dei dati possono essere configurate in modo che i dati vengano eliminati dall'ubicazione di memorizzazione nell'eventualità che sia stato superato il limite del periodo di permanenza per quei dati specifici oppure che lo spazio a disposizione sia diminuito superando i limiti specificati dal valore dello spazio su disco.

Per ulteriori informazioni sulla configurazione della memorizzazione dei dati, consultare [“Configuring Data Storage \(Configurazione della memorizzazione dei dati\)”](#) nella *Guida all'amministrazione di Sentinel Log Manager 1.1*.

1.1.6 Ricerca e generazione di rapporti

I componenti per la realizzazione delle ricerche e la generazione dei rapporti facilitano la ricerca e la creazione di rapporti dei dati del log degli eventi nei sistemi di memorizzazione e indicizzazione dei dati sia locali che in rete. È possibile effettuare la ricerca dei dati evento memorizzati in modo generico oppure in base a campi evento specifici come, ad esempio, il nome utente di origine. I risultati di tali ricerche possono essere ottimizzati o filtrati ulteriormente e salvati come un modello di rapporto per un utilizzo successivo.

Sentinel Log Manager dispone di rapporti preinstallati. È possibile anche effettuare l'upload di ulteriori rapporti. I rapporti possono essere generati in base a una pianificazione o a esigenze più specifiche.

Per ulteriori informazioni sull'elenco dei rapporti di default, consultare [“Generazione di rapporti”](#) nella *Guida all'amministrazione di Sentinel Log Manager 1.1*.

Per ulteriori informazioni sulla ricerca di eventi e sulla generazione di rapporti, consultare [“Ricerca”](#) e [“generazione di rapporti”](#) nella *Guida all'amministrazione di Sentinel Log Manager 1.1*.

1.1.7 Collegamento Sentinel

Collegamento Sentinel può essere utilizzato per inoltrare i dati evento da un Sentinel Log Manager a un altro. Con una serie gerarchica di Sentinel Log Manager, è possibile conservare log completi in più ubicazioni per area, mentre gli eventi più importanti vengono inoltrati a un singolo Sentinel Log Manager per l'esecuzione delle ricerche e la generazione di rapporti in modo centralizzato.

Collegamento Sentinel consente anche di inoltrare eventi importanti a Novell Sentinel, un sistema SIEM (Security Information Event Management) completo per la correlazione avanzata, la soluzione dei casi e l'immissione di informazioni contestuali di valore elevato come informazioni sulla criticità o sull'identità del server da un sistema di gestione delle identità.

1.1.8 Interfaccia utente basata sul Web

Novell Sentinel Log Manager è dotato di un'interfaccia utente basata sul Web che facilita la configurazione e l'utilizzo della Gestione log di Sentinel. La funzionalità dell'interfaccia utente viene fornita da un server Web e da un'interfaccia grafica basata su Java Web Start. Tutte le interfacce utente comunicano con il server mediante una connessione cifrata.

È possibile utilizzare l'interfaccia Web di Novell Sentinel Log Manager per eseguire i seguenti task:

- ◆ Ricerca di eventi
- ◆ Salvataggio dei criteri di ricerca come modello di rapporto
- ◆ Visualizzazione e gestione dei rapporti
- ◆ Avvio dell'interfaccia Gestione origine eventi per configurare la raccolta dei dati per le origini dati diverse da syslog e dalle applicazioni Novell. (solo amministratori)
- ◆ Configurazione dell'inoltro dei dati (solo amministratori)
- ◆ Esecuzione del download del programma di installazione della Gestione servizi di raccolta per l'installazione remota (solo amministratori)
- ◆ Visualizzazione dello stato delle origini evento (solo amministratori)
- ◆ Configurazione della raccolta dei dati per syslog e le origini evento Novell (solo amministratori)
- ◆ Configurazione della memorizzazione dei dati e visualizzazione dello stato del database (solo amministratori)
- ◆ Configurazione dell'archiviazione dei dati (solo amministratori)
- ◆ Configurazione delle azioni associate per l'invio dei dati evento corrispondenti ai canali di output (solo amministratori)
- ◆ Gestione degli account utente e delle autorizzazioni (solo amministratori)

1.2 Panoramica relativa all'installazione

Novell Sentinel Log Manager può essere installato come applicazione oppure su un sistema operativo SUSE Linux Enterprise Server (SLES) 11 esistente. Quando Sentinel Log Manager viene installato come applicazione, il server di Sentinel Log Manager viene installato in un sistema operativo SLES 11.

Di default, Novell Sentinel Log Manager installa i seguenti componenti:

- ◆ Server di Sentinel Log Manager
- ◆ Server di comunicazioni
- ◆ Server Web e interfaccia utente basata sul Web
- ◆ Server per la generazione di rapporti
- ◆ Gestione servizi di raccolta

Per alcuni di questi componenti è necessaria un'ulteriore configurazione.

Di default, Novell Sentinel Log Manager installa un'istanza di Gestione servizi di raccolta. Se si desidera disporre di più istanze della Gestione servizi di raccolta, è possibile installarle separatamente su computer remoti. Per ulteriori informazioni, consultare [Capitolo 7, “Installazione di Gestioni servizi di raccolta aggiuntive”](#), a pagina 53.

Requisiti di sistema

Nella seguente sezione vengono descritti i requisiti relativi a hardware, sistema operativo, browser, connettori supportati e compatibilità delle origini evento per Novell Sentinel Log Manager.

- ♦ Sezione 2.1, “Requisiti hardware”, a pagina 17
- ♦ Sezione 2.2, “Sistemi operativi supportati”, a pagina 20
- ♦ Sezione 2.3, “Browser supportati”, a pagina 21
- ♦ Sezione 2.4, “Ambiente virtuale supportato”, a pagina 21
- ♦ Sezione 2.5, “Connettori supportati”, a pagina 22
- ♦ Sezione 2.6, “Origini evento supportate”, a pagina 22

2.1 Requisiti hardware

- ♦ Sezione 2.1.1, “Server di Sentinel Log Manager”, a pagina 17
- ♦ Sezione 2.1.2, “Server della Gestione servizi di raccolta”, a pagina 18
- ♦ Sezione 2.1.3, “Stima dei requisiti per la memorizzazione dei dati”, a pagina 19
- ♦ Sezione 2.1.4, “Ambiente virtuale”, a pagina 20

2.1.1 Server di Sentinel Log Manager

Novell Sentinel Log Manager è supportato da processori Intel Xeon e AMD Opteron a 64 bit, ma non da processori Itanium.

Nota: Questi requisiti si riferiscono a una dimensione evento media di 300 byte.

I seguenti requisiti hardware sono consigliati per un sistema di produzione che conservi i dati online per almeno 90 giorni:

Tabella 2-1 *Requisiti hardware per Sentinel Log Manager*

Requisiti	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
Compressione	Fino a 10:1	Fino a 10:1	Fino a 10:1
Numero origini evento massimo	Fino a 1000	Fino a 1000	Fino a 2000
Numero frequenza evento massimo	500	2500	7500

Requisiti	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
CPU	Un Intel Xeon E5450 da 3 GHz (CPU a 4 core) oppure Due CPU Intel Xeon L5240 3 (CPU a 2 core, in totale: 4 core)	Un Intel Xeon E5450 da 3 GHz (CPU a 4 core) oppure Due CPU Intel Xeon L5240 3 (CPU a 2 core, in totale: 4 core)	Due Intel Xeon X5470 3,33 GHz (Cpu a 4 core, in totale: 8 core)
RAM (Random Access Memory)	4 GB	4 GB	8 GB
Memorizzazione	2 unità 7,2k RPM da 500 GB (hardware RAID con 256 MB di cache, RAID 1)	2 unità 7,2k RPM da 1 TB (hardware RAID con 256 MB di cache, RAID 1)	6 unità 15k RPM da 450 GB (hardware RAID con 512 MB di cache, RAID 10)

Nota:

- ♦ In un solo computer è possibile includere più origini evento. Ad esempio, in un server Windows possono essere incluse due origini evento Sentinel in quanto si può desiderare di raccogliere i dati sia dal sistema operativo Windows che dal database del server SQL ospitato nello stesso computer.
- ♦ È necessario configurare l'ubicazione della memorizzazione in rete in una SAN (storage network area) o NAS (network-attached storage) esterna dotata di più unità.
- ♦ Il volume dello stato stazionario consigliato è pari all'80% del numero massimo di EPS concessi in licenza. Nell'eventualità che venga raggiunto questo limite, Novell consiglia di installare ulteriori istanze di Sentinel Log Manager.

Nota: I limiti massimi fissati per le origini evento non sono rigidi, tuttavia rappresentano dei valori consigliati che si basano sulle verifiche relative alla prestazione realizzate da Novell e suppongono una frequenza eventi media bassa al secondo per origine evento (minore di 3 EPS). Frequenze EPS più elevate provocano un numero massimo di origini evento sostenibili più ridotto. Per arrivare ai limiti approssimativi per una frequenza EPS media specifica o numero di origini evento, sempre che il numero massimo di origini evento non superi i limiti indicati sopra, è possibile utilizzare l'equazione (numero massimo origini evento) x (media EPS per origine evento) = frequenza eventi massima.

2.1.2 Server della Gestione servizi di raccolta

- Un Intel Xeon L5240 3 GHz (CPU a 2 core)
- 256 MB di RAM
- 10 GB di spazio libero su disco.

2.1.3 Stima dei requisiti per la memorizzazione dei dati

Sentinel Log Manager viene utilizzato per conservare i dati non elaborati per un lungo periodo di tempo, in modo da poter soddisfare i requisiti legali e di altro tipo. Sentinel Log Manager sfrutta la tecnologia di compressione per facilitare un utilizzo più efficace dello spazio di memorizzazione disponibile sia localmente che in rete. Tuttavia, su un lungo periodo di tempo i requisiti relativi alla memorizzazione potrebbero divenire significativi.

Per superare tutti i problemi relativi ai vincoli di costo per sistemi di memorizzazione dei dati, è possibile utilizzare dei sistemi per la memorizzazione dei dati a lungo termine più economici. I sistemi di memorizzazione basati su nastro rappresentano la soluzione più comune e conveniente. Tuttavia, il supporto su nastro non consente l'accesso casuale ai dati memorizzati, necessario per elaborare ricerche più rapide. Per questo motivo, è preferibile un approccio misto alla memorizzazione dei dati a lungo termine, in cui i dati che si desidera ricercare siano disponibili in un sistema di memorizzazione ad accesso casuale mentre i dati che si desidera conservare, ma non ricercare, siano conservati mediante una soluzione alternativa e conveniente, come un dispositivo su nastro. Per istruzioni sull'impiego di questo approccio misto, consultare [“Using Sequential-Access Storage for Long Term Data Storage \(Utilizzo della memorizzazione ad accesso sequenziale per la memorizzazione dei dati a lungo termine\)”](#) nella *Guida all'amministrazione di Sentinel Log Manager 1.1*.

Per determinare la quantità di spazio di memorizzazione ad accesso casuale necessario per Sentinel Log Manager, valutare prima la quantità di giorni di dati sui quali è necessario effettuare ricerche o eseguire rapporti su base periodica. Per l'archiviazione dei dati, è necessario disporre di una quantità sufficiente di spazio su disco localmente sul computer in cui è installato Sentinel Log Manager oppure in modalità remota sul protocollo Server Message Block (SMB) o CIFS, nel Network File System (NFS) oppure in una SAN per Sentinel Log Manager.

Oltre ai requisiti minimi, è necessario disporre anche del seguente spazio aggiuntivo su disco rigido:

- ♦ Per rendere conto delle frequenze dati che sono più elevate del previsto.
- ♦ Per copiare i dati dal nastro e inviarli nuovamente a Sentinel Log Manager per l'elaborazione delle ricerche e la generazione dei rapporti sui dati presenti nella cronologia.

Utilizzare le seguenti formule per valutare la quantità di spazio necessario per la memorizzazione dei dati:

- ♦ **Dimensioni della memorizzazione dei dati evento:** {numero di giorni} x {eventi per secondo} x {dimensione media in byte dell'evento} x 0,000012 = GB di memorizzazione necessari

Generalmente, le dimensioni dell'evento variano dai 300 ai 1000 byte.

- ♦ **Dimensioni della memorizzazione dei dati non elaborati:** {numero di giorni} x {eventi per secondo} x {dimensione media in byte dei dati non elaborati} x 0,000012 = GB di memorizzazione necessari

Generalmente, la dimensione media dei dati non elaborati per i messaggi syslog è pari a 200 byte.

- ♦ **Dimensioni totali della memorizzazione:** ({dimensione media in byte dell'evento} + {dimensione media in byte dei dati non elaborati}) x {numero di giorni} x {eventi per secondo} x 0,000012 = totale GB di memorizzazione necessari

Nota: I numeri appena riportati rappresentano solo una stima. Essi dipendono dalle dimensioni dei dati evento e dalle dimensioni dei dati compressi.

Con le formule riportate sopra viene calcolato lo spazio minimo di memorizzazione necessario per memorizzare i dati completamente compressi nel sistema di memorizzazione esterno. Quando la memorizzazione locale viene colmata, Sentinel Log Manager comprime e sposta i dati da un sistema di memorizzazione locale (parzialmente compresso) a uno esterno (totalmente compresso). Per questo motivo, la stima dei requisiti di spazio per la memorizzazione esterna diventa ancora più difficile per la permanenza dei dati. Per migliorare la prestazione di ricerca e generazione dei rapporti rispetto ai dati più recenti, è possibile aumentare lo spazio locale di memorizzazione oltre i requisiti hardware di Sentinel Log Manager. Tuttavia, questa operazione non è necessaria.

È possibile utilizzare anche le formule riportate sopra per determinare la quantità di spazio di memorizzazione necessario per un sistema di memorizzazione dei dati a lungo termine come, ad esempio, un'unità nastro.

2.1.4 Ambiente virtuale

Sentinel Log Manager è stato ampiamente verificato ed è totalmente supportato in un server VMware ESX. I risultati di prestazione in un ambiente virtuale possono essere comparabili a quelli ottenuti nelle verifiche realizzate su un computer fisico, a patto che l'ambiente virtuale fornisca le stesse caratteristiche consigliate in quanto a memoria, CPU, spazio su disco e I/O del computer fisico.

2.2 Sistemi operativi supportati

In questa sezione sono contenute le informazioni relative ai sistemi operativi supportati per il server di Sentinel Log Manager e la Gestione servizi di raccolta remota:

- ♦ [Sezione 2.2.1, “Sentinel Log Manager”, a pagina 20](#)
- ♦ [Sezione 2.2.2, “Gestione servizi di raccolta”, a pagina 20](#)

2.2.1 Sentinel Log Manager

Le informazioni riportate in questa sezione sono applicabili solo nell'eventualità che si stia installando Sentinel Log Manager su un sistema operativo esistente.

- SUSE Linux Enterprise Server 11 a 64 bit.
- Un file system ad alta prestazione.

Nota: Tutte le verifiche Novell vengono realizzate con il file system ext3.

2.2.2 Gestione servizi di raccolta

È possibile installare ulteriori istanze di Gestione servizi di raccolta nei seguenti sistemi operativi:

- ♦ [“Linux” a pagina 21](#)
- ♦ [“Windows” a pagina 21](#)

Linux

- SUSE Linux Enterprise Server 10 SP2 (32 bit e 64 bit)
- SUSE Linux Enterprise Server 11 (32 bit e 64 bit)

Windows

- Windows Server 2003 (32 bit e 64 bit)
- Windows Server 2003 SP2 (32 bit e 64 bit)
- Windows Server 2008 (64 bit)

2.3 Browser supportati

L'interfaccia di Sentinel Log Manager è stata ottimizzata per la visualizzazione a una risoluzione pari a 1280 x 1024 o maggiore nei seguenti browser supportati:

- ♦ [Sezione 2.3.1, “Linux”, a pagina 21](#)
- ♦ [Sezione 2.3.2, “Windows”, a pagina 21](#)

2.3.1 Linux

- Mozilla Firefox 3.6

2.3.2 Windows

- Mozilla Firefox 3 (versione consigliata 3.6)
- Microsoft Internet Explorer 8 (versione consigliata 8.0)

Prerequisiti per Internet Explorer 8

- ♦ Se il Livello di protezione in Internet è impostato su Alta, una volta effettuato l'accesso a Novell Sentinel Log Manager verrà visualizzata solo una pagina vuota. Per risolvere questo problema, selezionare *Strumenti > Opzioni Internet > scheda Protezione > Siti attendibili*. Fare clic sul pulsante *Siti*, quindi aggiungere il sito Web di Sentinel Log Manager all'elenco dei siti attendibili.
- ♦ Assicurarsi che l'opzione *Strumenti > Visualizzazione Compatibilità* non sia selezionata.
- ♦ Se l'opzione *Richiesta di conferma automatica per download di file* non è attivata, la finestra popup del download dei file potrebbe essere bloccata dal browser. Per risolvere questo problema, selezionare *Strumenti > Opzioni Internet > scheda Protezione > Livello personalizzato*, quindi nella sezione Download dell'elenco a discesa selezionare *Attiva* per attivare l'opzione *Richiesta di conferma automatica per download di file*.

2.4 Ambiente virtuale supportato

- VMware ESX/ESXi 3.5/4.0 o successivo
- VMPlayer 3 (solo per versioni demo)
- Xen 3.1.1

2.5 Connettori supportati

Sentinel Log Manager supporta tutti i connettori supportati da Sentinel e Sentinel RD.

- Connettore di Audit
- Connettore di processi LEA per dispositivi Check Point
- Connettore di database
- Connettore di generazione dati
- Connettore di file
- Connettore di processi
- Connettore Syslog
- Connettore SNMP
- Connettore SDEE
- Connettore di collegamento Sentinel
- Connettore WMS
- Connettore mainframe
- Connettore SAP

Nota: I connettori mainframe e SAP richiedono una licenza separata.

2.6 Origini evento supportate

Sentinel Log Manager supporta diversi dispositivi e applicazioni come sistemi di rilevamento delle intrusioni, firewall, sistemi operativi, router, server Web, database, commutatori, mainframe e origini evento di antivirus. I dati provenienti da queste origini evento vengono analizzati sintatticamente e normalizzati per gradi variabili a seconda che i dati siano elaborati mediante un servizio di raccolta degli eventi generici che colloca l'intero payload dell'evento in un campo comune, oppure mediante l'utilizzo di un servizio di raccolta di un dispositivo specifico che analizza sintatticamente i dati all'interno di singoli campi.

Le seguenti origini evento sono supportate da Sentinel Log Manager:

- Cisco Firewall (6 e 7)
- Cisco Switch Catalyst serie 6500 (CatOS 8.7)
- Cisco Switch Catalyst serie 6500 (IOS 12.2SX)
- Cisco Switch Catalyst serie 5000 (CatOS 4.x)
- Cisco Switch Catalyst serie 4900 (IOS 12.2SG)
- Cisco Switch Catalyst serie 4500 (IOS 12.2SG)
- Cisco Switch Catalyst serie 4000 (CatOS 4.x)
- Cisco Switch Catalyst serie 3750 (IOS 12.2SE)
- Cisco Switch Catalyst serie 3650 (IOS 12.2SE)
- Cisco Switch Catalyst serie 3550 (IOS 12.2SE)
- Cisco Switch Catalyst serie 2970 (IOS 12.2SE)

- Cisco Switch Catalyst serie 2960 (IOS 12.2SE)
- Cisco VPN 3000 (4.1.5, 4.1.7 e 4.7.2)
- Extreme Networks Summit X650 (con ExtremeXOS 12.2.2 e versioni precedenti)
- Extreme Networks Summit X450a (con ExtremeXOS 12.2.2 e versioni precedenti)
- Extreme Networks Summit X450e (con ExtremeXOS 12.2.2 e versioni precedenti)
- Extreme Networks Summit X350 (con ExtremeXOS 12.2.2 e versioni precedenti)
- Extreme Networks Summit X250e (con ExtremeXOS 12.2.2 e versioni precedenti)
- Extreme Networks Summit X150 (con ExtremeXOS 12.2.2 e versioni precedenti)
- Enterasys Dragon (7.1 e 7.2)
- Servizio di raccolta degli eventi generici
- HP HP-UX (11iv1 e 11iv2)
- IBM AIX (5.2, 5.3, e 6.1)
- Juniper Netscreen serie 5
- McAfee Firewall Enterprise
- McAfee Network Security Platform (2.1, 3.x e 4.1)
- McAfee VirusScan Enterprise (8.0i, 8.5i e 8.7i)
- McAfee ePolicy Orchestrator (3.6 e 4.0)
- McAfee AV Via ePolicy Orchestrator 8.5
- Microsoft Active Directory (2000, 2003 e 2008)
- Microsoft SQL Server (2005 e 2008)
- Nortel VPN (1750, 2700, 2750 e 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 con la patch di strumentazione eDirectory disponibile sul [sito Web di supporto di Novell \(http://download.novell.com/Download?buildid=RH_B5b3M6EQ~\)](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 e 2.8.4)
- Snare per Windows Intersect Alliance (3.1.4 e 1.1.1)
- Sun Microsystems Solaris 10
- Symantec AntiVirus Corporate Edition (9 e 10)
- TippingPoint Security Management System (2.1 e 3.0)

- Websense Web Security 7.0
- Websense Web Filter 7.0

Nota: Per abilitare la raccolta dei dati dalle origini evento Novell iManager e Novell Netware 6.5, aggiungere un'istanza di un servizio di raccolta e un connettore secondario, come il connettore Audit, all'interfaccia di Gestione origini eventi per ogni origine evento. Una volta completata questa operazione, queste origini evento vengono visualizzate nella console Web di Sentinel Log Manager nella scheda *Server Audit*.

I servizi di raccolta che supportano origini evento addizionali possono essere ottenuti dal [sito Web di contenuto di Sentinel 6.1](http://support.novell.com/products/sentinel/sentinel61.html) (<http://support.novell.com/products/sentinel/sentinel61.html>) o generati utilizzando i plug-in SDK disponibili nel [sito Web Sentinel Plug-in SDK](http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

Installazione su un sistema SLES 11 esistente

3

In questa sezione viene descritta la procedura di installazione di Sentinel Log Manager su un sistema SUSE Linux Enterprise Server (SLES) 11 mediante il programma di installazione dell'applicazione. Il server di Sentinel Log Manager può essere installato in diversi modi: mediante la procedura di installazione standard, la procedura personalizzata oppure mediante la procedura di installazione invisibile all'utente in cui l'intero processo di installazione viene eseguito senza richiedere alcun intervento dell'utente e utilizzando i valori di default. È possibile installare Sentinel Log Manager anche come un utente non root.

Se si utilizza il metodo di installazione personalizzato, è possibile installare il prodotto con una chiave di licenza e selezionare, inoltre, un'opzione di autenticazione. Infatti, oltre all'autenticazione del database, per Sentinel Log Manager è possibile configurare un'autenticazione LDAP. Quando Sentinel Log Manager viene configurato per l'autenticazione LDAP, gli utenti possono effettuare il login al server mediante le proprie credenziali Novell eDirectory o Microsoft Active Directory.

Se si desidera installare più server Sentinel Log Manager nella propria installazione, è possibile registrare le opzioni di installazione in un file di configurazione e, successivamente, utilizzare tale file per eseguire un'installazione automatica. Per ulteriori informazioni, consultare [Sezione 3.4, "Installazione invisibile all'utente"](#), a pagina 29.

Prima di procedere all'installazione, assicurarsi che i requisiti minimi specificati in [Capitolo 2, "Requisiti di sistema"](#), a pagina 17 siano soddisfatti.

- ♦ [Sezione 3.1, "Istruzioni preliminari"](#), a pagina 25
- ♦ [Sezione 3.2, "Installazione standard"](#), a pagina 26
- ♦ [Sezione 3.3, "Installazione personalizzata"](#), a pagina 27
- ♦ [Sezione 3.4, "Installazione invisibile all'utente"](#), a pagina 29
- ♦ [Sezione 3.5, "Installazione non root"](#), a pagina 30

3.1 Istruzioni preliminari

- Assicurarsi che l'hardware e il software soddisfino i requisiti minimi descritti in [Capitolo 2, "Requisiti di sistema"](#), a pagina 17.
- Configurare il sistema operativo in modo tale che il comando `hostname -f` restituisca un nome host valido.
- Per installare la versione concessa in licenza, richiedere la chiave di licenza al [Servizio clienti di Novell](#) (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22).
- Sincronizzare l'orario mediante il protocollo NTP (Network Time Protocol).
- Installare i seguenti comandi del sistema operativo:
 - ♦ `mount`
 - ♦ `umount`
 - ♦ `id`

- ◆ df
 - ◆ du
 - ◆ sudo
- ❑ Assicurarsi che le seguenti porte siano aperte nel firewall:
TCP 8080, TCP 8443, TCP 61616, TCP 10013, TCP 1289, TCP 1468, TCP 1443 e UDP 1514

3.2 Installazione standard

La procedura relativa all'installazione standard consente di installare Sentinel Log Manager completo di tutte le opzioni di default con una licenza di valutazione di 90 giorni.

- 1 Effettuare il download e copiare i file di installazione dal sito Web di download di Novell.
- 2 Effettuare il login come `root` al server in cui si desidera installare Sentinel Log Manager.
- 3 Specificare il seguente comando per estrarre i file di installazione dal file `.tar`:

```
tar xfz <install_filename>
```

Sostituire `<nomefile_installazione>` con il nome attuale del file di installazione.

- 4 Specificare il seguente comando per eseguire lo script `install-slm` necessario per l'installazione di Sentinel Log Manager:

```
./install-slm
```

Se si desidera installare Sentinel Log Manager su più sistemi, è possibile registrare le opzioni di installazione in un file. È possibile utilizzare questo file per installare automaticamente Sentinel Log Manager su altri sistemi. Per la registrazione delle opzioni di installazione, specificare il comando seguente:

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

- 5 Per procedere con una lingua determinata, selezionare il numero specificato situato accanto alla lingua.

Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.

- 6 Leggere la licenza con l'utente finale e immettere `si` o `s` per accettare la licenza e continuare con l'installazione.

L'installazione inizia a installare tutti i pacchetti RPM. Il completamento dell'installazione potrebbe richiedere alcuni secondi.

Se non sono già presenti, l'installazione crea un gruppo `novell` e un utente `novell`.

- 7 Quando richiesto, specificare l'opzione per procedere all'installazione standard.

L'installazione procede con la chiave di licenza di valutazione di 90 giorni inclusa nel programma di installazione. Questa chiave di licenza consente di attivare la serie completa di funzioni del prodotto per un periodo di prova di 90 giorni. In qualsiasi momento, durante o dopo il periodo di prova, è possibile sostituire la licenza di valutazione con una chiave di licenza acquistata.

- 8 Specificare la password per l'utente amministratore.
- 9 Confermare la password per l'utente amministratore.

Il programma di installazione seleziona il metodo *Autentica solo per database* e prosegue con l'installazione.

L'installazione di Sentinel Log Manager viene completata e il server si avvia. Prima che tutti i servizi vengano avviati potrebbero essere necessari 5-10 minuti in quanto, una volta terminata l'installazione, il sistema elabora un'inizializzazione unica. Prima di effettuare il login al server, attendere il completamento dell'inizializzazione.

- 10 Per effettuare il login al server di Sentinel Log Manager, utilizzare l'URL specificato nell'output dell'installazione. L'URL è simile a `https://10.0.0.1:8443/novelllogmanager`.

Per ulteriori informazioni sull'esecuzione del login al server, consultare [Capitolo 5, “Effettuare il login all'interfaccia Web”](#), a pagina 45.

- 11 Per configurare le origini evento per l'invio dei dati a Sentinel Log Manager, consultare “[Configuring Data Collection \(Configurazione della raccolta dei dati\)](#)” nella *Guida all'amministrazione di Sentinel Log Manager 1.1*.

3.3 Installazione personalizzata

Se si utilizza il metodo di installazione personalizzato, è possibile installare il prodotto con una chiave di licenza e selezionare, inoltre, un'opzione di autenticazione. Infatti, oltre all'autenticazione del database, per Sentinel Log Manager è possibile configurare un'autenticazione LDAP. Quando Sentinel Log Manager viene configurato per l'autenticazione LDAP, gli utenti possono effettuare il login al server mediante le credenziali della directory LDAP.

Se durante l'installazione di Sentinel Log Manager non viene configurata l'autenticazione LDAP, tale configurazione può essere eseguita una volta completata l'installazione, se necessario. Per configurare l'autenticazione LDAP dopo l'installazione, consultare “[Autenticazione LDAP](#)” nella *Guida all'amministrazione di Sentinel Log Manager 1.1*.

- 1 Effettuare il download e copiare i file di installazione dal sito Web di download di Novell.
- 2 Effettuare il login come `root` al server in cui si desidera installare Sentinel Log Manager.
- 3 Specificare il seguente comando per estrarre i file di installazione dal file `.tar`:

```
tar xzf <install_filename>
```

Sostituire `<nomefile_installazione>` con il nome attuale del file di installazione.

- 4 Specificare il seguente comando per eseguire lo script `install-slm` necessario per l'installazione di Sentinel Log Manager:

```
./install-slm
```

- 5 Per procedere con una lingua determinata, selezionare il numero specificato situato accanto alla lingua.

Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.

- 6 Leggere la licenza con l'utente finale e immettere `si o s` per accettare la licenza e continuare con l'installazione.

L'installazione inizia a installare tutti i pacchetti RPM. Il completamento dell'installazione potrebbe richiedere alcuni secondi.

Se non sono già presenti, l'installazione crea un gruppo `novell` e un utente `novell`.

- 7 Quando richiesto, specificare l'opzione per procedere all'installazione personalizzata.

- 8 Quando viene richiesto di specificare l'opzione della chiave di licenza, immettere 2 per specificare la chiave di licenza per il prodotto acquistato.

- 9 Specificare la chiave di licenza, quindi premere Invio.

Per ulteriori informazioni sulle chiavi di licenza, consultare “[Gestione delle chiavi di licenza](#)” nella [Guida all'amministrazione di Sentinel Log Manager 1.1](#).

- 10 Specificare la password per l'utente amministratore.
 - 11 Confermare la password per l'utente amministratore.
 - 12 Specificare la password per l'amministratore del database (dbauser).
 - 13 Confermare la password per l'amministratore del database (dbauser).
 - 14 È possibile configurare qualsiasi numero di porta valido purché sia compreso nell'intervallo specificato per i seguenti servizi:
 - ♦ Server Web
 - ♦ Java Message Service
 - ♦ Client Proxy Service
 - ♦ Servizio database
 - ♦ Agent Internal Gateway
- Se si desidera proseguire con le porte di default, immettere l'opzione 6 e continuare con l'installazione personalizzata.
- 15 Specificare l'opzione per autenticare gli utenti mediante una directory LDAP esterna.
 - 16 Specificare l'indirizzo IP o il nome host del server LDAP.

Il valore di default è localhost. Tuttavia, è consigliato non installare il server LDAP sullo stesso computer in cui è installato il server di Sentinel Log Manager.
 - 17 Selezionare una delle seguenti tipologie di connessione LDAP:
 - ♦ **Connessione LDAP SSL/TSL:** consente di stabilire una connessione protetta tra il browser e il server per l'autenticazione. Immettere 1 per specificare questa opzione.
 - ♦ **Connessione LDAP non cifrata:** consente di stabilire una connessione non cifrata. Immettere 2 per specificare questa opzione.
 - 18 Specificare il numero della porta del server LDAP. La porta SSL di default è la 636 e la porta non SSL di default è la 389.
 - 19 (Condizionale) Se si seleziona la connessione LDAP SSL/TSL, specificare se il certificato del server LDAP è firmato da una CA nota.
 - 20 (Condizionale) Se è stato specificato `n`, specificare il nome file del certificato del server LDAP.
 - 21 Selezionare se si desidera eseguire ricerche nella directory LDAP in modalità anonima:
 - ♦ **Eseguire ricerche nella directory LDAP in modalità anonima:** Il server di Sentinel Log Manager consente di realizzare una *ricerca in modalità anonima* nella directory LDAP basata sul nome utente specificato, allo scopo di recuperare il corrispondente nome distinto (DN) dell'utente LDAP. Immettere 1 per specificare questo metodo.
 - ♦ **Non eseguire ricerche in modalità anonima nella directory LDAP:** Immettere 2 per specificare questa opzione.
 - 22 (Condizionale) Se è stata selezionata la ricerca in modalità anonima, specificare l'attributo di ricerca e passare a [Passo 25](#).
 - 23 (Condizionale) Se non è stata selezionata la ricerca in modalità autonoma in [Passo 21](#), specificare se si sta utilizzando Microsoft Active Directory.

Per Active Directory, l'attributo `userPrincipalName`, il cui valore è della forma `userName@domainName` può essere utilizzato, in via facoltativa, per autenticare l'utente prima di realizzare la ricerca dell'oggetto Utente LDAP, senza dover immettere il DN utente.

- 24** (Condizionale) Se si desidera utilizzare questo metodo per Active Directory, specificare il nome del dominio.
- 25** Specificare il DN di base.
- 26** Premere `s` per specificare che le opzioni fornite sono corrette, altrimenti `n` e modificare la configurazione.
- 27** Per effettuare il login al server di Sentinel Log Manager, utilizzare l'URL specificato nell'output dell'installazione. L'URL è simile a `https://10.0.0.1:8443/novelllogmanager`.
Per ulteriori informazioni sull'esecuzione del login al server, consultare [Capitolo 5, “Effettuare il login all'interfaccia Web”](#), a pagina 45.

3.4 Installazione invisibile all'utente

L'installazione invisibile all'utente o automatica di Sentinel Log Manager può risultare utile se si ha la necessità di installare più server Sentinel Log Manager nella propria installazione. In uno scenario di questo tipo è possibile registrare i parametri di installazione durante l'esecuzione della prima installazione e, successivamente, eseguire il file registrato in tutti gli altri server.

- 1** Effettuare il download e copiare i file di installazione dal sito Web di download di Novell.
- 2** Effettuare il login come `root` al server in cui si desidera installare Sentinel Log Manager.
- 3** Specificare il comando seguente per estrarre i file di installazione dal file `.tar`:

```
tar xfz <install_filename>
```

Sostituire `<nomefile_installazione>` con il nome attuale del file di installazione.

- 4** Specificare il comando seguente per eseguire lo script `install-slm` necessario per l'installazione invisibile all'utente di Sentinel Log Manager:

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

Per informazioni sulla creazione del file di risposta, fare riferimento a [Sezione 3.2, “Installazione standard”](#), a pagina 26. L'installazione prosegue con i valori memorizzati nel file di risposta.

- 5** Per effettuare il login al server di Sentinel Log Manager, utilizzare l'URL specificato nell'output dell'installazione. L'URL è simile a `https://10.0.0.1:8443/novelllogmanager`.
Per ulteriori informazioni sull'esecuzione del login al server, consultare [Capitolo 5, “Effettuare il login all'interfaccia Web”](#), a pagina 45.
- 6** Per configurare le origini evento per l'invio dei dati a Sentinel Log Manager, consultare [“Configuring Data Collection \(Configurazione della raccolta dei dati\)”](#) nella [“Guida all'amministrazione di Sentinel Log Manager 1.1”](#).

3.5 Installazione non root

Se per motivi di norme aziendali, non è possibile eseguire l'installazione completa di Sentinel Log Manager come utente `root`, molte delle fasi di installazione possono comunque essere realizzate come un utente di diverso tipo.

- 1** Effettuare il download e copiare i file di installazione dal sito Web di download di Novell.
- 2** Specificare il seguente comando per estrarre i file di installazione dal file `.tar`:

```
tar xfz <install_filename>
```

Sostituire `<nomefile_installazione>` con il nome attuale del file di installazione.
- 3** Effettuare il login come `root` al server in cui si desidera installare Sentinel Log Manager come utente `root`.
- 4** Immettere il comando seguente:

```
./bin/root_install_prepare
```

Viene visualizzato un elenco dei comandi da eseguire con i privilegi di utente `root`.
Se non sono già presenti, l'installazione crea un gruppo `novell` e un utente `novell`.
- 5** Accettare l'elenco dei comandi.
Vengono eseguiti i comandi visualizzati.
- 6** Specificare il comando seguente per modificare l'utente `novell` non root appena creato:

```
novell:  
su novell
```
- 7** Immettere il comando seguente:

```
./install-slm
```
- 8** Per procedere con una lingua determinata, selezionare il numero specificato situato accanto alla lingua.
Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.
- 9** Leggere la licenza con l'utente finale e immettere `si` o `s` per accettare la licenza e continuare con l'installazione.
L'installazione inizia a installare tutti i pacchetti RPM. Il completamento dell'installazione potrebbe richiedere alcuni secondi.
- 10** Viene richiesto di specificare la modalità di installazione.
 - ♦ Se si seleziona di procedere con la modalità di installazione standard, completare le operazioni come descritte dal [Passaggio 8](#) al [Passaggio 11](#) in [Sezione 3.2](#), “[Installazione standard](#)”, a pagina 26.
 - ♦ Se si sceglie di procedere con l'installazione personalizzata, completare le operazioni come descritte dal [Passaggio 8](#) al [Passaggio 23](#) in [Sezione 3.3](#), “[Installazione personalizzata](#)”, a pagina 27.Viene completata l'installazione di Sentinel Log Manager e il server viene avviato.
- 11** Specificare il comando seguente per modificare l'utente `root`:

```
su root
```
- 12** Specificare il comando seguente per terminare l'installazione:

```
./bin/root_install_finish
```

13 Per effettuare il login al server di Sentinel Log Manager, utilizzare l'URL specificato nell'output dell'installazione. L'URL è simile a `https://10.0.0.1:8443/novelllogmanager`.

Per ulteriori informazioni sull'esecuzione del login al server, consultare [Capitolo 5, “Effettuare il login all'interfaccia Web”](#), a pagina 45.

Installazione dell'applicazione

4

Novell Sentinel Log Manager Appliance è pronta per eseguire l'applicazione software creata su SUSE Studio, un servizio Web di facile utilizzo che unisce un sistema operativo SUSE Linux Enterprise Server (SLES) 11 di protezione avanzata con un servizio di aggiornamento del software Novell Sentinel Log Manager integrato per fornire un'esperienza dell'utente più semplice ed efficace volta a incrementare gli investimenti realizzati dai clienti. L'applicazione software può essere installata sia su hardware che in un ambiente virtuale.

- ♦ Sezione 4.1, “Istruzioni preliminari”, a pagina 33
- ♦ Sezione 4.2, “Porte utilizzate”, a pagina 33
- ♦ Sezione 4.3, “Installazione dell'applicazione VMware”, a pagina 35
- ♦ Sezione 4.4, “Installazione dell'applicazione Xen”, a pagina 36
- ♦ Sezione 4.5, “Installazione dell'applicazione sull'hardware”, a pagina 38
- ♦ Sezione 4.6, “Configurazione post-installazione per l'applicazione”, a pagina 39
- ♦ Sezione 4.7, “Configurazione di WebYaST”, a pagina 39
- ♦ Sezione 4.8, “Registrazione degli aggiornamenti”, a pagina 41

4.1 Istruzioni preliminari

- ♦ Assicurarsi che i requisiti hardware siano soddisfatti. Per ulteriori informazioni, consultare [Sezione 2.1, “Requisiti hardware”, a pagina 17](#).
- ♦ Per installare la versione concessa in licenza, richiedere la chiave di licenza al [Servizio clienti di Novell \(http://www.novell.com/center\)](http://www.novell.com/center).
- ♦ Per la registrazione degli aggiornamenti del software, richiedere il codice di registrazione al [Servizio clienti Novell \(http://www.novell.com/center\)](http://www.novell.com/center).
- ♦ Sincronizzare l'orario mediante il protocollo NTP (Network Time Protocol).
- ♦ (Condizionale) Se si intende utilizzare VMware, assicurarsi di disporre di VMware Converter per effettuare l'upload dell'immagine al server VMware ESX e contemporaneamente convertirla in un formato che possa essere eseguito sul server ESX.

4.2 Porte utilizzate

Si noti che Novell Sentinel Log Manager Appliance utilizza le porte seguenti per la comunicazione e che alcune di esse sono aperte nel firewall:

- ♦ [Sezione 4.2.1, “Porte aperte nel firewall”, a pagina 34](#)
- ♦ [Sezione 4.2.2, “Porte utilizzate localmente”, a pagina 34](#)

4.2.1 Porte aperte nel firewall

Tabella 4-1 Porte di rete utilizzate da Sentinel Log Manager

Porte	Descrizione
TCP 1289	Utilizzata per le connessioni di Novell Audit.
TCP 289	Inoltrata a 1289 per le connessioni Novell Audit.
TCP 22	Utilizzata per l'accesso shell sicuro a Sentinel Log Manager Appliance.
UDP 1514	Utilizzata per i messaggi syslog.
UDP 514	Inoltrata a 1514 per i messaggi.
TCP 8080	Utilizzata per la comunicazione HTTP. Utilizzata anche da Sentinel Log Manager Appliance per il servizio di aggiornamento.
TCP 80	Inoltrata a 8080 per il server Web di Sentinel Log Manager per la comunicazione HTTP. Utilizzata anche da Sentinel Log Manager Appliance per il servizio di aggiornamento.
TCP 8443	Utilizzata per la comunicazione HTTPS. Utilizzata anche da Sentinel Log Manager Appliance per il servizio di aggiornamento.
TCP 1443	Utilizzata per i messaggi syslog cifrati mediante il protocollo SSL.
TCP 443	Inoltrata a 8443 per il server Web di Sentinel Log Manager per la comunicazione HTTPS. Utilizzata anche da Sentinel Log Manager Appliance per il servizio di aggiornamento.
TCP 61616	Utilizzata per la comunicazione tra le Gestioni servizi di raccolta e il server.
TCP 10013	Utilizzata dal Proxy SSL dell'interfaccia utente Gestione origini eventi.
TCP 54984	Utilizzata dalla console di gestione di Sentinel Log Manager Appliance (WebYaST).
TCP 1468	Utilizzata per i messaggi syslog.

4.2.2 Porte utilizzate localmente

Tabella 4-2 Porte utilizzate localmente per la comunicazione

Porte	Descrizione
TCP 61617	Utilizzata per la comunicazione interna tra il server Web e il server.
TCP 5556	Utilizzata nell'interfaccia di loop-back per la comunicazione interna, con <code>internal_gateway_server</code> e <code>internal_gateway</code> . Viene utilizzata per la comunicazione tra il motore agente e la Gestione servizi di raccolta.

Porte	Descrizione
TCP 5432	Utilizzata per il database PostgreSQL. Non è necessario aprire questa porta di default. Tuttavia, se si stanno sviluppando dei rapporti mediante Sentinel SDK è necessario aprire questa porta. Per ulteriori informazioni, fare riferimento al sito Web Sentinel Plug-in SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) .
Altre due porte TCP selezionate in modo casuale	Utilizzate per la comunicazione interna tra il motore agente e la Gestione servizi di raccolta.
TCP 8005	Utilizzata per la comunicazione interna con i processi Tomcat.
TCP 32000	Utilizzata per la comunicazione interna tra il motore agente e la Gestione servizi di raccolta.

4.3 Installazione dell'applicazione VMware

Per eseguire l'immagine dell'applicazione dal server VMware ESX, importare e installare l'immagine dell'applicazione nel server.

- 1 Effettuare il download del file di installazione dell'applicazione VMware.

Il file corretto per l'applicazione VMware contiene `vmx` nel nome file. Ad esempio, `Sentinel_Log_Manager_1.1.0.0_64_VMX.x86_64-0.777.0.vmx.tar.gz`

- 2 Stabilire un archivio dati ESX sul quale possa essere installata l'immagine dell'applicazione.
- 3 Eseguire il login come amministratore al server in cui si desidera installare l'applicazione.
- 4 Specificare il comando seguente per estrarre l'immagine compressa dell'applicazione dal computer in cui VM Converter è installato:

```
tar zxvf <file_installazione>
```

Sostituire `<file_installazione>` con il nome del file attuale.

- 5 Per importare l'immagine di VMware al server ESX, utilizzare VMware Converter e seguire le istruzioni visualizzate sullo schermo durante l'installazione guidata.
- 6 Eseguire il login nel computer del server ESX.
- 7 Selezionare l'immagine VMware importata dell'applicazione e fare clic sull'icona *Power On (Accensione)*.
- 8 Selezionare la lingua che si desidera, quindi fare clic su *Avanti*.
- 9 Selezionare il layout della tastiera, quindi fare clic su *Avanti*.
- 10 Leggere e accettare il contratto di licenza di Novell SUSE Enterprise Server Software.
- 11 Leggere e accettare il contratto di licenza con l'utente finale di Novell Sentinel Log Manager.
- 12 Nella schermata Nome host e nome dominio, specificare il nome host e il nome del dominio. Assicurarsi che l'opzione *Write hostname to /etc/hosts (Scrivi nome host in /etc/hosts)* sia selezionata.
- 13 Selezionare *Avanti*. La configurazione del nome host è salvata.

- 14 Effettuare una delle seguenti operazioni:
 - ♦ Per utilizzare le impostazioni di connessione alla rete attuali, selezionare *Use the following configuration (Utilizza la configurazione seguente)* nella schermata *Network Configuration II (Configurazione di rete II)*.
 - ♦ Per modificare le impostazioni di connessione alla rete, selezionare *Modifica*.
- 15 Impostare l'ora e la data, fare clic su *Avanti*, quindi su *Fine*.

Nota: Per modificare la configurazione NTP una volta completata l'installazione, utilizzare YaST dalla riga di comando dell'applicazione. WebYast può essere utilizzato per modificare l'ora e la data, ma non la configurazione NTP.

Se immediatamente dopo aver completato l'installazione, l'ora visualizzata non è sincronizzata, eseguire il comando seguente e riavviare NTP:

```
rcntp restart
```

- 16 Impostare la password `root` di Novell SUSE Enterprise Server nativo, quindi fare clic su *Avanti*.
- 17 Impostare la password `root`, quindi fare clic su *Avanti*.
- 18 Impostare la password `admin` e la password `dbauser` di Sentinel Log Manager, quindi fare clic su *Avanti*.
- 19 Selezionare *Avanti*. Le impostazioni della connessione di rete sono salvate.
L'installazione prosegue e viene completata. Annotare l'indirizzo IP dell'applicazione mostrato nella console.
- 20 Procedere con [Sezione 4.6, "Configurazione post-installazione per l'applicazione"](#), a pagina 39.

4.4 Installazione dell'applicazione Xen

- 1 Effettuare il download e copiare il file di installazione dell'applicazione virtuale Xen in `/var/lib/xen/images`.

Il nome file corretto dell'applicazione virtuale Xen contiene `xen`. Ad esempio, `Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.xen.tar.gz`

- 2 Per decomprimere il file, specificare il seguente comando:

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

Sostituire `<file_installazione>` con il nome del file di installazione attuale.

- 3 Modificare la nuova directory di installazione. In questa directory sono contenuti i seguenti file:

- ♦ file di immagine `<nome_file>.raw`
- ♦ file `<nome_file>.xenconfig`

- 4 Aprire il file `<nome_file>.xenconfig` mediante un editor di testo.

- 5 Modificare il file nel seguente modo:

Specificare il percorso completo per il file `.raw` nelle impostazioni del disco.

Specificare le impostazioni del bridge per la configurazione di rete. Ad esempio, `"bridge=br0"` oppure `"bridge=xenbr0"`.

Specificare i valori per le impostazioni relative al `nome` e alla `memoria`.

Ad esempio:

```
# -*- 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** Una volta modificato il file `<nomefile>.xenconfig`, specificare il seguente comando per creare la memoria virtuale:

```
xm create <nome_file>.xenconfig
```

- 7** (Facoltativo) Per verificare se la memoria virtuale è stata creata, specificare il comando seguente:

```
xm list
```

La memoria virtuale viene visualizzata nell'elenco.

Ad esempio, se è stato configurato `name="Sentinel_Log_Manager_1.1.0.0_64"` nel file `.xenconfig`, la memoria virtuale viene visualizzata con quel nome.

- 8** Per avviare l'installazione, specificare il comando seguente:

```
xm console <nome vm>
```

Sostituire `<nome vm>` con il nome specificato nelle impostazioni relative al nome del file `.xenconfig`, che rappresenta anche il valore restituito nel [Passaggio 7](#). Ad esempio:

```
xm console Sentinel_Log_Manager_1.1.0.0_64
```

- 9** Selezionare la lingua che si desidera, quindi fare clic su *Avanti*.
- 10** Selezionare il layout della tastiera, quindi fare clic su *Avanti*.
- 11** Leggere e accettare il contratto di licenza di Novell SUSE Enterprise Server Software.
- 12** Leggere e accettare il contratto di licenza con l'utente finale di Novell Sentinel Log Manager.
- 13** Nella schermata Nome host e nome dominio, specificare il nome host e il nome del dominio. Assicurarsi che l'opzione *Write hostname to /etc/hosts* sia selezionata.
- 14** Selezionare *Avanti*. La configurazione del nome host è salvata.
- 15** Effettuare una delle seguenti operazioni:
- ♦ Per utilizzare le impostazioni di connessione alla rete attuali, selezionare *Use the following configuration (Utilizza la configurazione seguente)* nella schermata *Network Configuration II (Configurazione di rete II)*.
 - ♦ Per modificare le impostazioni di connessione alla rete, selezionare *Modifica*.
- 16** Impostare l'ora e la data, fare clic su *Avanti*, quindi su *Fine*

Nota: Per modificare la configurazione NTP una volta completata l'installazione, utilizzare YaST dalla riga di comando dell'applicazione. WebYast può essere utilizzato per modificare l'ora e la data, ma non la configurazione NTP.

Se immediatamente dopo aver completato l'installazione, l'ora visualizzata non è sincronizzata, eseguire il comando seguente e riavviare NTP:

```
rcntp restart
```

- 17** Impostare la password `root` di Novell SUSE Enterprise Server nativo, quindi fare clic su *Avanti*.

- 18 Impostare la password admin e la password dbauser di Sentinel Log Manager, quindi fare clic su *Avanti*.
L'installazione prosegue e viene completata. Annotare l'indirizzo IP dell'applicazione mostrato nella console.
- 19 Procedere con [Sezione 4.6, “Configurazione post-installazione per l'applicazione”](#), a pagina 39.

4.5 Installazione dell'applicazione sull'hardware

Prima di installare l'applicazione sull'hardware, assicurarsi che sia stato effettuato il download dell'immagine del disco ISO dell'applicazione dal sito di supporto, quindi che sia stata decompressa e sia disponibile su DVD.

- 1 Inserire il DVD e avviare il computer fisico dall'unità DVD.
- 2 Utilizzare le istruzioni visualizzate sullo schermo durante l'installazione guidata.
- 3 Eseguire l'immagine dell'applicazione Live DVD selezionando la voce collocata nella parte superiore del menu di avvio.
- 4 Leggere e accettare il contratto di licenza di Novell SUSE Enterprise Server Software.
- 5 Leggere e accettare il contratto di licenza con l'utente finale di Novell Sentinel Log Manager.
- 6 Selezionare *Avanti*.
- 7 Nella schermata Nome host e nome dominio, specificare il nome host e il nome del dominio.
Assicurarsi che l'opzione *Write hostname to /etc/hosts (Scrivi nome host in /etc/hosts)* sia selezionata.
- 8 Selezionare *Avanti*. La configurazione del nome host è salvata.
- 9 Effettuare una delle seguenti operazioni:
 - ♦ Per utilizzare le impostazioni della connessione di rete attuali, selezionare *Use the following configuration (Utilizzare la configurazione seguente)* nella schermata Network Configuration II (Configurazione di rete II).
 - ♦ Per modificare le impostazioni di connessione alla rete, selezionare *Modifica*.
- 10 Selezionare *Avanti*. Le impostazioni della connessione di rete sono salvate.
- 11 Impostare l'ora e la data, quindi fare clic su *Avanti*.

Nota: Per modificare la configurazione NTP una volta completata l'installazione, utilizzare YaST dalla riga di comando dell'applicazione. WebYast può essere utilizzato per modificare l'ora e la data, ma non la configurazione NTP.

Se immediatamente dopo aver completato l'installazione, l'ora visualizzata non è sincronizzata, eseguire il comando seguente e riavviare NTP:

```
rcntp restart
```

-
- 12 Impostare la password `root`, quindi fare clic su *Avanti*.
 - 13 Impostare la password admin e la password dbauser di Sentinel Log Manager, quindi fare clic su *Avanti*.
 - 14 Per effettuare il login all'applicazione, immettere il nome utente e la password nella console.
Il valore di default del nome utente è `root` e la password è `password`.
 - 15 Per installare l'applicazione nel server fisico, eseguire il comando seguente:

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

L'installazione prosegue e viene completata. Annotare l'indirizzo IP dell'applicazione mostrato nella console.

- 16 Procedere con [Sezione 4.6, “Configurazione post-installazione per l'applicazione”](#), a pagina 39.

4.6 Configurazione post-installazione per l'applicazione

Per effettuare il login alla console Web dell'applicazione e inizializzare il software:

- 1 Aprire un browser Web ed effettuare il login a `https://<indirizzo IP>:8443`. Viene visualizzata la pagina Web di Sentinel Log Manager.

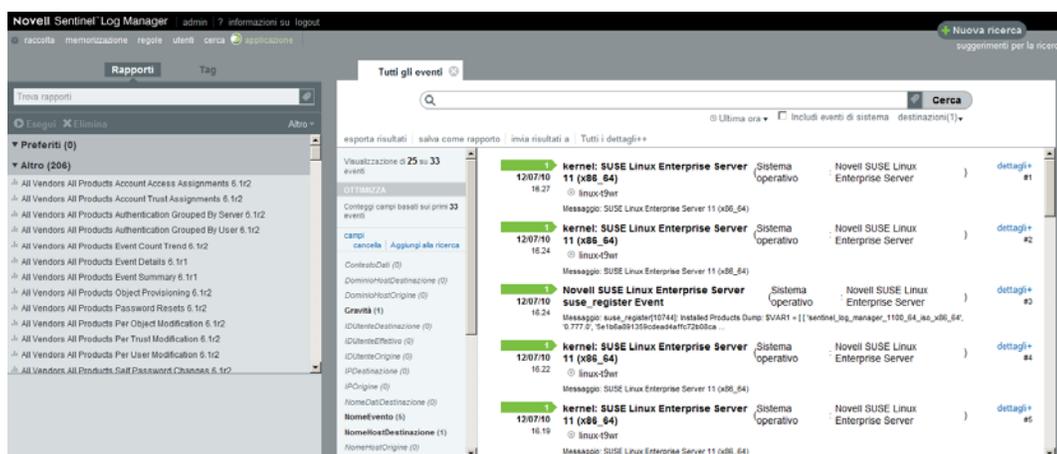
L'indirizzo IP dell'applicazione viene visualizzato nella console dell'applicazione una volta completata l'installazione e riavviato il server.

- 2 È possibile configurare Sentinel Log Manager Appliance per la memorizzazione e la raccolta dei dati. Per ulteriori informazioni sulla configurazione dell'applicazione, consultare la [Guida all'amministrazione di Sentinel Log Manager 1.1](#).
- 3 Per effettuare la registrazione per gli aggiornamenti, consultare [Sezione 4.8, “Registrazione degli aggiornamenti”](#), a pagina 41.

4.7 Configurazione di WebYaST

L'interfaccia utente di Novell Sentinel Log Manager Appliance include WebYaST. WebYaST è una console remota basata sul Web per il controllo delle applicazioni che si basano su SUSE Linux Enterprise. Mediante WebYaST è possibile accedere, configurare e controllare le applicazioni di Sentinel Log Manager. Nella procedura seguente sono descritti brevemente i passaggi da eseguire per la configurazione di WebYaST. Per ulteriori informazioni sulla configurazione dettagliata, consultare la [Guida dell'utente WebYaST \(http://www.novell.com/documentation/webyast/\)](http://www.novell.com/documentation/webyast/).

- 1 Effettuare il login a Sentinel Log Manager Appliance.



- 2 Fare clic su *Applicazione*.

Login

Inserisci le credenziali di login per l'host localhost.

Nome utente:

Password:

Login

- 3 Specificare le credenziali di login per il sistema, quindi fare clic su *Login*.

Language

webYaST language

Next

- 4 Selezionare una lingua desiderata, quindi fare clic su *Avanti*.



Mail Settings

Outgoing mail server
(SMTP)

Transport Layer Security
(TLS)

User name

Password

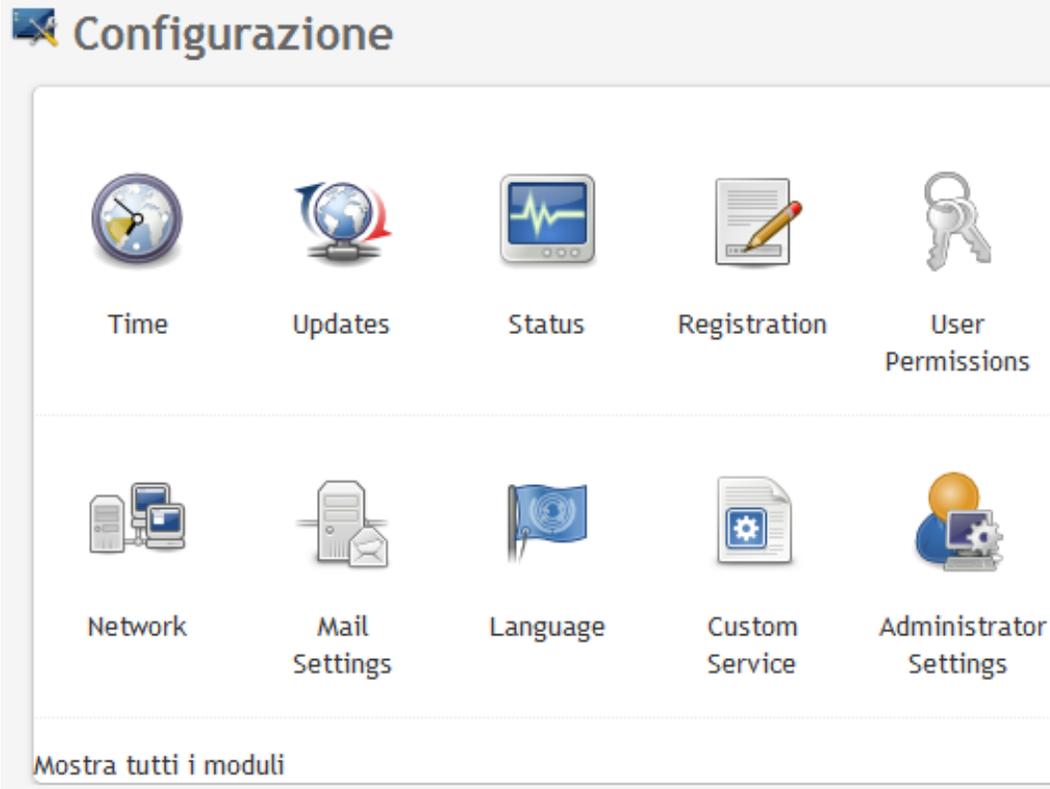
Confirm password

[Annulla](#) oppure

- 5 Specificare i dettagli per la configurazione del server di posta, quindi fare clic su *Salva*.
Viene visualizzata la pagina di registrazione.
- 6 Configurare il server di Sentinel Log Manager per ricevere gli aggiornamenti come descritto in [Sezione 4.8, “Registrazione degli aggiornamenti”](#), a pagina 41.
- 7 Fare clic su *Avanti* per completare la configurazione iniziale.

4.8 Registrazione degli aggiornamenti

- 1 Effettuare il login a Sentinel Log Manager Appliance.
Viene visualizzata l'interfaccia utente Web di Sentinel Log Manager.
- 2 Fare clic su *Applicazione* per avviare WebYaST.



3 Fare clic su *Registrazione*.



Registration

Mandatory Information

Email

System name

regcode-slm

[Show Details](#)

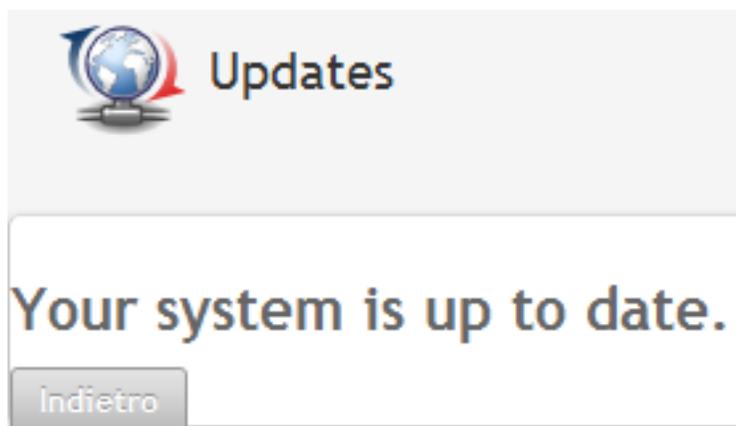
[Annulla](#) oppure

4 Specificare il codice di registrazione dell'applicazione.

5 Fare clic su *Salva*.

6 Per verificare se vi sono aggiornamenti disponibili, fare clic su *Aggiorna*.

Nella pagina visualizzata vengono indicati gli aggiornamenti disponibili, se presenti.



Effettuare il login all'interfaccia Web

5

L'utente amministratore creato durante l'installazione può effettuare l'accesso all'interfaccia Web per configurare e utilizzare Sentinel Log Manager:

- 1** Aprire un browser Web supportato. Per ulteriori informazioni, vedere la [Sezione 2.3, “Browser supportati”](#), a pagina 21.
- 2** Specificare l'URL della pagina Novell Sentinel Log Manager (ad esempio, `https://10.0.0.1:8443/novelllogmanager`), quindi premere Invio.
- 3** (Condizionale) La prima volta che si effettua l'accesso a Sentinel Log Manager, viene richiesto di accettare un certificato. La pagina di login di Sentinel Log Manager viene visualizzata al momento dell'accettazione del certificato.

Novell.

Novell.
Sentinel™ Log Manager

Versione 1.1

© Novell, Inc. Tutti i diritti riservati.

Nome utente:

Password:

Lingua:

Accesso

Novell Sentinel Log Manager supporta Firefox 3 (versione consigliata: 3.6) e Internet Explorer 8 (versione consigliata: 8.0)

4 Specificare il nome utente e la password dell'amministratore di Sentinel Log Manager.

5 Selezionare la lingua dell'interfaccia di Sentinel Log Manager.

L'interfaccia utente di Sentinel Log Manager è disponibile in Inglese, Portoghese, Francese, Italiano, Tedesco, Spagnolo, Giapponese, Cinese tradizionale o semplificato.

6 Fare clic su *Accesso*.

Viene visualizzata l'interfaccia utente Web di Novell Sentinel Log Manager.

The screenshot displays the Novell Sentinel Log Manager web interface. The top navigation bar includes the application name, user information, and search options. The main content area is titled "Tutti gli eventi" and shows a list of system events. The left sidebar contains a "Rapporti" section with a search bar and a list of report categories. The event list includes columns for time, source, system, and destination, with expandable details for each entry.

Time	Source	System	Destination	Details
12/07/10 16:27	kernel: SUSE Linux Enterprise Server 11 (x86_64)	Sistema operativo	Novell SUSE Linux Enterprise Server	dettagli+ #1
12/07/10 16:24	kernel: SUSE Linux Enterprise Server 11 (x86_64)	Sistema operativo	Novell SUSE Linux Enterprise Server	dettagli+ #2
12/07/10 16:24	Novell SUSE Linux Enterprise Server suse_register Event	Sistema operativo	Novell SUSE Linux Enterprise Server	dettagli+ #3
12/07/10 16:22	kernel: SUSE Linux Enterprise Server 11 (x86_64)	Sistema operativo	Novell SUSE Linux Enterprise Server	dettagli+ #4
12/07/10 16:19	kernel: SUSE Linux Enterprise Server 11 (x86_64)	Sistema operativo	Novell SUSE Linux Enterprise Server	dettagli+ #5

Esecuzione dell'upgrade di Sentinel Log Manager

6

Mediante lo script di upgrade, è possibile eseguire l'upgrade di Novell Sentinel Log Manager dalla versione 1.0.0.4, o successiva, a Sentinel Log Manager 1.1.

- ♦ [Sezione 6.1, “Esecuzione dell'upgrade dalla versione 1.0 alla versione 1.1”](#), a pagina 49
- ♦ [Sezione 6.2, “Esecuzione dell'upgrade della Gestione dei servizi di raccolta”](#), a pagina 50
- ♦ [Sezione 6.3, “Esecuzione della migrazione dall'applicazione 1.0 a 1.1”](#), a pagina 51

6.1 Esecuzione dell'upgrade dalla versione 1.0 alla versione 1.1

1 Se la versione del server di Sentinel Log Manager è precedente a quella 1.0.0.4., è necessario eseguire prima l'upgrade alla versione 1.0.0.4 o successiva.

2 Effettuare il download e copiare i file di installazione dal sito Web di download di Novell.

3 Effettuare il login come `root` al server in cui si desidera installare Sentinel Log Manager.

4 Specificare il comando seguente per arrestare il server di Sentinel Log Manager:

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

Ad esempio, `/opt/novell/sentinel_log_mgr_1.0_x86-64/bin/server.sh stop`

5 Specificare il seguente comando per estrarre i file di installazione dal file `.tar`:

```
tar xfz <install_filename>
```

Sostituire `<nomefile_installazione>` con il nome attuale del file di installazione.

6 Specificare il comando seguente per eseguire lo script `install-slm` per effettuare l'upgrade a Sentinel Log Manager:

```
./install-slm
```

7 Per procedere con una lingua determinata, selezionare il numero specificato situato accanto alla lingua.

Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.

8 Leggere la licenza dell'utente finale e immettere `si o s` per accettare la licenza e continuare l'installazione.

9 Lo script di installazione individua una versione precedente al prodotto già esistente nel sistema e richiede all'utente di specificare se si desidera eseguire l'upgrade del prodotto. Se viene premuto `n`, la procedura di installazione viene terminata. Per continuare con l'upgrade, premere `s`.

L'installazione inizia a installare tutti i pacchetti RPM. Il completamento dell'installazione potrebbe richiedere alcuni secondi.

L'installazione esistente di Sentinel Log Manager 1.0 viene lasciata intatta, con le seguenti eccezioni:

- ♦ Se la directory dei dati della versione 1.0 (ad esempio, `/opt/novell/sentinel_log_manager_1.0_x86-64/data`) e la directory dei dati della versione 1.1 (ad esempio, `/var/opt/novell/sentinel_log_mgr/data`) risiedono nello stesso file system, le sottodirectory `<1.0>/data/eventuate` e `<1.0>/data/rawdata` vengono spostate nella posizione della versione 1.1 in quanto le dimensioni delle directory `eventdata` e `rawdata` sono, di solito, molto grandi. Se le directory dei dati 1.0 e 1.1 risiedono in file system diversi, le sottodirectory `eventdata` e `rawdata` vengono copiate nella posizione della versione 1.1 e i file della versione 1.0 sono lasciati intatti.
 - ♦ Se la directory dei dati esistente della versione 1.0 (ad esempio, `/opt/novell/sentinel_log_mgr_1.0_x86-64`) risiede in un file system montato separatamente e lo spazio sul file system contenente la directory dei dati della versione 1.1 non è sufficiente (`/var/opt/novell/sentinel_log_mgr/data`), è possibile fare in modo che il programma di installazione monti nuovamente il file system dalla posizione 1.0 a quella 1.1. Vengono aggiornate anche tutte le voci presenti in `/etc/fstab`. Se si decide di non consentire che il programma di installazione monti nuovamente il file system esistente, la procedura di upgrade viene chiusa. In tal caso, è possibile creare spazio sul file system sufficiente per la directory dei dati 1.1.
- 10** Completata l'installazione di Sentinel Log Manager 1.1 e con il server già in funzione, è necessario specificare il comando seguente per rimuovere manualmente la directory di Sentinel Log Manager 1.0:

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

Ad esempio:

```
rm -rf /opt/novell/sentinel_log_mgr_1.0_x86-64
```

La rimozione in modo permanente della directory di installazione provoca l'eliminazione dell'installazione di Sentinel Log Manager 1.0

6.2 Esecuzione dell'upgrade della Gestione dei servizi di raccolta

- 1** Eseguire il login a Sentinel Log Manager come amministratore.
- 2** Selezionare *raccolta > Avanzato*.
- 3** Fare clic sul collegamento *Download del programma di installazione*, presente nella sezione Programma di installazione dell'upgrade di Gestione servizi di raccolta.
Viene visualizzata una finestra contenente le opzioni per aprire o salvare il file `scm_upgrade_installer.zip` nel computer locale. Salvare il file.
- 4** Copiare il file in un'ubicazione temporanea.
- 5** Estrarre i contenuti del file `.zip`.
- 6** Come proprietario dell'installazione di Gestione servizi di raccolta, eseguire uno dei seguenti file di upgrade in base al software operativo in uso:
 - ♦ Per eseguire l'upgrade di Gestione servizi di raccolta Windows, eseguire `service_pack.bat`.
 - ♦ Per eseguire l'upgrade di Gestione servizi di raccolta Linux, eseguire `service_pack.sh`.

- 7 Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo.
- 8 Riavviare il computer.

6.3 Esecuzione della migrazione dall'applicazione 1.0 a 1.1

Se si ha installato Sentinel Log Manager 1.0 e si desidera eseguire la migrazione a Sentinel Log Manager Appliance 1.1, seguire le procedure fornite di seguito per la migrazione dei dati e della configurazione

- 1 (Condizionale) Se la versione di Sentinel Log Manager installata è inferiore a 1.0 correzione HotFix 4, eseguirne l'upgrade alla versione Sentinel Log Manager 1.0 correzione HotFix 5, che rappresenta la correzione HotFix disponibile. Eseguire il download della correzione HotFix dal sito [Novell di download delle patch \(http://download.novell.com/protected/Summary.jsp?buildid=VgZ3aerzjYc~\)](http://download.novell.com/protected/Summary.jsp?buildid=VgZ3aerzjYc~).

Nota: Per eseguire il download delle patch è necessario essere registrati. Se non si ha effettuato la registrazione, fare clic su Register (Registra) per creare un account utente nel sito di download delle patch.

- 2 Esecuzione dell'upgrade a Sentinel Log Manager 1.1. Per ulteriori informazioni, consultare [Sezione 6.1, “Esecuzione dell'upgrade dalla versione 1.0 alla versione 1.1”, a pagina 49](#).
- 3 Specificare il comando seguente per modificare l'utente `novell`:

```
su -novell
```
- 4 Specificare il comando seguente per modificare la directory `/bin`:

```
cd /opt/novell/sentinel_log_mgr/bin
```
- 5 Specificare il comando seguente per eseguire un backup completo dei dati e della configurazione di Sentinel Log Manager 1.1.

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

Sostituire *<nomefilebackup>* con un nome del file per memorizzare i dati di backup.

Per ulteriori informazioni sui dati di backup, consultare [“Backing Up and Restoring Data \(Backup e ripristino dei dati\)”](#).
- 6 Installare Sentinel Log Manager Appliance 1.1 in un computer separato. Per ulteriori informazioni, consultare [Capitolo 4, “Installazione dell'applicazione”, a pagina 33](#).
- 7 Copiare il file contenente i dati di cui è stato eseguito il backup in un'applicazione Sentinel Log Manager 1.1 nuova.
- 8 Immettere il comando seguente:

```
chown novell:novell <backfupfilename>
```
- 9 Specificare il comando seguente per modificare la directory `/bin`:

```
cd /opt/novell/sentinel_log_mgr/bin
```
- 10 Specificare il comando seguente per ripristinare completamente i dati di cui è stato eseguito il backup dall'applicazione Sentinel Log Manager 1.1:

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

Per ulteriori informazioni, consultare [“Backing Up and Restoring Data \(Backup e ripristino dei dati\)”](#).

Installazione di Gestioni servizi di raccolta aggiuntive

7

La Gestione servizi di raccolta consente di gestire tutte le raccolte e le analisi sintattiche dei dati per Novell Sentinel Log Manager. Questo processo di installazione di Sentinel Log Manager installa una Gestione servizi di raccolta di default sul server di Sentinel Log Manager. Tuttavia, in una configurazione distribuita è possibile installare più Gestioni servizi di raccolta.

- ♦ [Sezione 7.1, “Istruzioni preliminari”, a pagina 53](#)
- ♦ [Sezione 7.2, “Vantaggi apportati dalla presenza di più Gestioni servizi di raccolta”, a pagina 53](#)
- ♦ [Sezione 7.3, “Installazione di Gestioni servizi di raccolta aggiuntive”, a pagina 54](#)

7.1 Istruzioni preliminari

- ♦ Assicurarsi che l'hardware e il software soddisfino i requisiti minimi descritti in [Capitolo 2, “Requisiti di sistema”, a pagina 17](#).
- ♦ Sincronizzare l'orario mediante il protocollo NTP (Network Time Protocol).
- ♦ Per una Gestione servizi di raccolta è necessaria la connettività di rete alla porta bus messaggi (61616) nel server di Sentinel Log Manager. Prima di iniziare l'installazione di Gestione servizi di raccolta, assicurarsi che a tutti i firewall e altre impostazioni di rete sia permesso comunicare su questa porta.

7.2 Vantaggi apportati dalla presenza di più Gestioni servizi di raccolta

L'installazione di più istanze di Gestione servizi di raccolta apporta diversi vantaggi a una rete distribuita:

- ♦ **Miglioramento della prestazione del sistema:** Le Gestioni servizi di raccolta aggiuntive consentono di analizzare sintatticamente ed elaborare i dati evento in un ambiente distribuito, accrescendo le potenzialità di prestazione del sistema.
- ♦ **Una maggiore protezione dei dati e la richiesta di una larghezza di banda di rete più ridotta:** Se le Gestioni servizi di raccolta vengono posizionate insieme alle origini evento, i processi di filtraggio, cifratura e compressione dei dati possono essere elaborati su lato origine.
- ♦ **Possibilità di raccogliere i dati da sistemi operativi aggiuntivi:** Ad esempio, è possibile installare una Gestione servizi di raccolta su Microsoft Windows per abilitare la raccolta dei dati mediante il protocollo WMI.
- ♦ **Memorizzazione dei file nella cache:** Quando viene abilitata la memorizzazione dei file nella cache, la Gestione servizi di raccolta può memorizzare una grande quantità di dati nella cache mentre il server è temporaneamente occupato dall'archiviazione degli eventi o dall'elaborazione di un picco negli eventi. Questa funzione rappresenta un vantaggio importante soprattutto per quei protocolli, come syslog, che non supportano la memorizzazione nella cache.

7.3 Installazione di Gestioni servizi di raccolta aggiuntive

- 1 Eseguire il login a Sentinel Log Manager come amministratore.
- 2 Selezionare *raccolta > Avanzato*.
- 3 Fare clic sul collegamento *Download del programma di installazione*. nella sezione del programma di installazione di Gestione servizi di raccolta.
Viene visualizzata una finestra contenente le opzioni per aprire o salvare il file `scm_installer.zip` nel computer locale. Salvare il file.
- 4 Copiare ed estrarre il file nell'ubicazione in cui si desidera installare la Gestione servizi di raccolta.
- 5 Eseguire uno dei seguenti file di installazione in base al software operativo in uso:
 - ♦ Per installare Gestione servizi di raccolta in un sistema Windows, eseguire `setup.bat`.
 - ♦ Per installare Gestione servizi di raccolta in un sistema Linux, eseguire `setup.sh`.
- 6 Selezionare una lingua, quindi fare clic su *OK*.
Viene visualizzata la schermata di installazione.
- 7 Fare clic su *OK*.
- 8 Leggere e accettare il contratto di licenza, quindi fare clic su *Avanti*.
- 9 È possibile procedere con la directory di installazione di default oppure cercare e selezionare una directory specifica, quindi fare clic su *Avanti*.
- 10 Non modificare la porta bus messaggi (61616) di default e specificare il nome host del server di comunicazione, quindi fare clic su *Avanti*.
- 11 Fare clic su *Avanti* per procedere con la Configurazione memoria automatica di default (256 megabyte).
Viene visualizzato un riepilogo dell'installazione.
- 12 Fare clic su *Installa*.
- 13 Specificare il nome utente e la password della Gestione servizi di raccolta.

Nota: Il nome utente e la password sono memorizzati nel file `/etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties` che risiede nel server di Sentinel Log Manager.

- 14 Quando richiesto, accettare il certificato in modo permanente.
- 15 Per terminare l'installazione, premere *Fine*.
- 16 Riavviare il computer.

Disinstallazione di Sentinel Log Manager

8

In questa sezione vengono descritte le procedure per la disinstallazione del server di Novell Sentinel Log Manager e della Gestione servizi di raccolta.

- ♦ [Sezione 8.1, “Disinstallazione dell'applicazione”](#), a pagina 55
- ♦ [Sezione 8.2, “Disinstallazione da un sistema SLES 11 esistente”](#), a pagina 55
- ♦ [Sezione 8.3, “Disinstallazione di Gestione servizi di raccolta”](#), a pagina 56

8.1 Disinstallazione dell'applicazione

Se si desidera conservare i dati di Gestione log di Sentinel, eseguire il backup dei dati prima di procedere alla disinstallazione dell'applicazione, in modo che sia possibile ripristinarli in un secondo momento. Per ulteriori informazioni, consultare [“Backing Up and Restoring Data \(Backup e ripristino dati\)”](#) nella *Guida all'amministrazione di Sentinel Log Manager 1.1*.

Al contrario, se non è necessario conservare i dati, utilizzare le procedure seguenti per disinstallare l'applicazione:

- ♦ **Applicazione VMware ESX:** Se la macchina virtuale è dedicata a Novell Sentinel Log Manager e non è necessario conservare alcun dato, eliminarla per disinstallare l'applicazione virtuale della Gestione log di Sentinel.
- ♦ **Applicazione Xen:** Se la macchina virtuale Xen è dedicata a Novell Sentinel Log Manager e non è necessario conservare alcun dato, eliminarla per disinstallare l'applicazione virtuale della Gestione log di Sentinel.
- ♦ **Applicazione hardware:** Se il sistema è dedicato a Novell Sentinel Log Manager e non è necessario conservare alcun dato, formattare nuovamente il disco rigido per disinstallare la Gestione log di Sentinel su un computer fisico.

8.2 Disinstallazione da un sistema SLES 11 esistente

- 1 Eseguire il login al server di Sentinel Log Manager come utente `root`.
- 2 Per eseguire lo script di disinstallazione, eseguire il comando seguente:

```
/opt/novell/sentinel_log_mgr/setup/uninstall-slm
```
- 3 Quando viene richiesto di confermare nuovamente se si desidera procedere alla disinstallazione, premere `s`.

Il server di Sentinel Log Manager viene prima arrestato e, successivamente, disinstallato.

8.3 Disinstallazione di Gestione servizi di raccolta

In questa sezione vengono descritte le procedure per disinstallare la Gestione servizi di raccolta di Sentinel installata su computer che eseguono il sistema operativo Windows o Linux.

- ♦ [Sezione 8.3.1, “Disinstallazione della Gestione servizi di raccolta su Linux”](#), a pagina 56
- ♦ [Sezione 8.3.2, “Disinstallazione della Gestione servizi di raccolta su Windows”](#), a pagina 56
- ♦ [Sezione 8.3.3, “Pulizia manuale delle directory”](#), a pagina 57

8.3.1 Disinstallazione della Gestione servizi di raccolta su Linux

- 1 Eseguire il login come utente `root`.
- 2 Nel computer in cui è installata la Gestione servizi di raccolta, spostarsi nell'ubicazione seguente:

```
$ESEC_HOME/_unist
```
- 3 Eseguire il comando seguente:

```
./uninstall.bin
```
- 4 Selezionare una lingua, quindi fare clic su *OK*.
- 5 Fare clic su *Avanti* nella schermata di installazione guidata.
- 6 Selezionare le funzioni che si desidera disinstallare, quindi fare clic su *Avanti*.
- 7 Interrompere tutte le applicazioni di Sentinel Log Manager in esecuzione, quindi fare clic su *Avanti*.
- 8 Fare clic su *Disinstalla*.
- 9 Fare clic su *Fine*.
- 10 Selezionare *Riavvia il sistema* e fare clic su *Fine*.

8.3.2 Disinstallazione della Gestione servizi di raccolta su Windows

- 1 Eseguire il login come amministratore.
- 2 Arrestare il server di Sentinel Log Manager.
- 3 Selezionare *Avvia > Esegui*.
- 4 Specificare quanto segue:

```
%Esec_home%\_unist
```
- 5 Fare doppio clic su `uninstall.exe` per eseguirlo.
- 6 Selezionare una lingua e fare clic su *OK*.
Viene visualizzata la schermata dell'installazione guidata.
- 7 Fare clic su *Avanti*.
- 8 Selezionare le funzioni che si desidera disinstallare, quindi fare clic su *Avanti*.

- 9 Interrompere tutte le applicazioni di Sentinel Log Manager in esecuzione, quindi fare clic su *Avanti*.
- 10 Fare clic su *Disinstalla*.
- 11 Fare clic su *Fine*.
- 12 Selezionare *Riavvia il sistema* e fare clic su *Fine*.

8.3.3 Pulizia manuale delle directory

- ♦ [“Linux” a pagina 57](#)
- ♦ [“Windows” a pagina 57](#)

Linux

- 1 Eseguire il login al computer in cui la Gestione servizi di raccolta è stata disinstallata come utente `root`.
- 2 Interrompere tutti i processi di Sentinel Log Manager.
- 3 Rimuovere i contenuti di `/opt/novell/sentinel6`

Windows

- 1 Eseguire il login al computer in cui la Gestione servizi di raccolta è stata disinstallata come amministratore.
- 2 Eliminare la cartella `%CommonProgramFiles%\InstallShield\Universal` e tutti i suoi contenuti.
- 3 Eliminare la cartella `%ESEC_HOME%` . Di default, è `C:\Programmi\Novell\Sentinel6`.

Risoluzione dei problemi relativi all'installazione

A

In questa sezione vengono descritti alcuni dei problemi che potrebbero verificarsi durante l'installazione nonché la procedura corretta per poterli affrontare.

- ♦ [Sezione A.1, “Installazione non riuscita a causa di una configurazione della rete non corretta”, a pagina 59](#)
- ♦ [Sezione A.2, “Problema di configurazione della rete con VMware Player 3 in SLES 11”, a pagina 59](#)
- ♦ [Sezione A.3, “Esecuzione dell'upgrade di Gestione log installata come utente non root diverso dall'utente novell”, a pagina 60](#)

A.1 Installazione non riuscita a causa di una configurazione della rete non corretta

Durante il primo avvio, se il programma di installazione rileva che le impostazioni di rete non sono corrette, viene visualizzato un messaggio di errore. Se la rete non è disponibile, non è possibile completare l'installazione di Sentinel Log Manager.

Per risolvere questo problema, configurare le impostazioni di rete nel modo appropriato. Durante la verifica della configurazione, il comando `ifconfig` deve restituire l'indirizzo IP valido e il comando `hostname -f` deve restituire il nome host valido.

A.2 Problema di configurazione della rete con VMware Player 3 in SLES 11

L'errore seguente potrebbe essere visualizzato durante la configurazione della rete con VMware Player 3 in SLES 11:

```
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| --
```

Questo errore indica che il file VMX potrebbe essere stato aperto da un'altra memoria virtuale. Per risolvere questo problema, aggiornare l'indirizzo MAC nel file VMX come mostrato di seguito:

- 1 Aprire il file VMX in un editor di testo.
- 2 Copiare l'indirizzo MAC dal campo `ethernet0.generatedAddress`.
- 3 Aprire il file `/etc/udev/rules.d/70-persistent-net.rules` dal sistema operativo guest.

- 4 Impostare come commento la riga originale, quindi digitare una riga SUBSYSTEM come mostrato di seguito:

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

- 5 Sostituire *<indirizzo MAC>* con l'indirizzo copiato durante il Passaggio [2Passo 2](#).
- 6 Salvare e chiudere il file.
- 7 Aprire la memoria virtuale in VMware Player.

A.3 Esecuzione dell'upgrade di Gestione log installata come utente non root diverso dall'utente novell

Se si tenta di eseguire l'upgrade del server di Novell Sentinel Log Manager 1.0 installato come utente root diverso dall'utente `novell`, la procedura di upgrade non può essere completata. Questo problema si verifica a causa del tipo di autorizzazioni del file impostate durante l'installazione di Sentinel Log Manager 1.0.

Per eseguire l'upgrade del server di Sentinel Log Manager 1.0 installato come un utente non root diverso dall'utente `novell`, realizzare le seguenti operazioni:

- 1 Creare un utente `novell`.
- 2 Modificare la proprietà di installazione di Sentinel Log Manager 1.0 in `novell:novell`.

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

Modificare *<directory_installazione>* con il nome della directory di installazione. Ad esempio,

```
chown -R novell:novell /opt/novell/sentinel_log_mgr_1.0_x86-64
```
- 3 modificare la voce `ESEC_USER` presente in `config/eseccuser.properties` in `novell`.
- 4 Eseguire il login come utente `root`, quindi effettuare l'upgrade a Sentinel Log Manager 1.1. Per ulteriori informazioni sull'esecuzione dell'upgrade, consultare [Sezione 6.1, "Esecuzione dell'upgrade dalla versione 1.0 alla versione 1.1"](#), a pagina 49.

Terminologia di Sentinel

Questa sezione descrive la terminologia utilizzata in questo documento.

Servizi di raccolta

Un'utility che analizza sintatticamente i dati e fornisce un flusso di eventi più dettagliato mediante l'introduzione di tassonomia, il rilevamento degli exploit e la rilevanza aziendale nel flusso di dati prima che gli eventi siano correlati, analizzati e inviati al database.

Connettori

Un'utility che utilizza metodi standard del settore per connettersi all'origine dati e ottenere dati non elaborati.

Permanenza dati

Una norma che definisce la durata in base alla quale gli eventi vengono conservati prima di essere eliminati dal server di Sentinel Log Manager.

Origine evento

L'applicatore o il sistema che registra gli eventi.

Gestione origini eventi

ESM. L'interfaccia che consente di gestire e controllare le connessioni tra Sentinel e le sue origini evento mediante l'utilizzo dei connettori e i servizi di raccolta di Sentinel.

Eventi al secondo

EPS. Un valore che consente la misurazione della velocità con la quale una rete genera i dati dai propri dispositivi e applicazioni di sicurezza. Rappresenta anche una frequenza sulla quale Sentinel Log Manager può raccogliere e memorizzare i dati dai dispositivi di sicurezza.

Integratore

Plug-in che consentono ai sistemi Sentinel di stabilire la connessione ad altri sistemi esterni. Le azioni JavaScript possono utilizzare gli integratori per interagire con altri sistemi.

Dati non elaborati

Gli eventi non elaborati che vengono ricevuti dal connettore e inviati direttamente al bus dei messaggi di Sentinel Log Manager e, successivamente, scritti sul disco nel server di Sentinel Log Manager. I dati non elaborati variano da connettore a connettore a causa del formato dei dati memorizzati nel dispositivo.