Sentinel Log Manager 1.2.2

Guida all'installazione

Luglio 2014



Note legali

NetIQ Sentinel è protetto dal brevetto nº 05829001 rilasciato negli Stati Uniti.

QUESTA DOCUMENTAZIONE E IL SOFTWARE IVI DESCRITTO SONO FORNITI SU LICENZA E SONO SOGGETTI AI TERMINI DI TALE CONTRATTO O DI UN'ESCLUSIONE DI GARANZIA. A ECCEZIONE DI QUANTO STABILITO ESPRESSAMENTE IN TALE CONTRATTO DI LICENZA O ESCLUSIONE DI GARANZIA, NETIQ CORPORATION FORNISCE LA PRESENTE DOCUMENTAZIONE E IL SOFTWARE CHE VI È DESCRITTO "COME È" SENZA GARANZIA DI ALCUN TIPO, ESPRESSA O IMPLICITA, INCLUSE, MA NON LIMITATE A, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ O IDONEITÀ A UN PARTICOLARE SCOPO. IN ALCUNI STATI NON È CONSENTITO STIPULARE ESCLUSIONI DI GARANZIA ESPRESSE O IMPLICITE RELATIVAMENTE A DETERMINATE TRANSAZIONI. LA PRESENTE ESCLUSIONE POTREBBE QUINDI NON ESSERE APPLICABILE.

Per maggiore chiarezza, qualsiasi modulo, adattatore o altro materiale simile ("Modulo") viene concesso su licenza in base ai termini e alle condizioni del contratto di licenza con l'utente finale relativo alla versione pertinente del prodotto o del software NetIQ cui è correlato o con il quale interagisce. Mediante l'accesso, la copia o l'utilizzo di un modulo l'utente conferma di accettare termini del contratto di licenza. Se l'utente non accetta i termini del contratto di licenza con l'utente finale, questi non è autorizzato a utilizzare, accedere o copiare un modulo ed è inoltre tenuto a distruggere tutte le copie del modulo e contattare NetIQ per ricevere ulteriori istruzioni.

La documentazione e il software che vi è descritto non possono essere noleggiati, venduti o donati senza disporre di previa autorizzazione scritta di NetIQ Corporation, eccetto nei casi consentiti dalla legge. Eccetto come stabilito espressamente nel contratto di licenza nell'esclusione di garanzia, nessuna parte di questa documentazione o del software che vi è descritto può essere riprodotta, memorizzata in un sistema di ripristino o trasmessa in qualsiasi forma o mezzo, sia esso elettronico o meccanico, senza disporre di previa autorizzazione scritta di NetIQ Corporation. Alcune aziende, nomi e dati presenti nella documentazione vengono utilizzati solo a scopo illustrativo e potrebbero non avere alcun riscontro reale.

La documentazione potrebbe includere alcune inesattezze tecniche o errori tipografici. Periodicamente vengono apportate delle modifiche alle informazioni contenute. Tali modifiche potrebbero essere introdotte nelle nuove edizioni della documentazione. NetIQ Corporation potrebbe apportare dei miglioramenti o delle modifiche al software descritto nella documentazione in qualsiasi momento.

Diritti limitati del governo degli Stati Uniti: se il software e la documentazione sono stati acquistati da o per conto del governo degli Stati Uniti o da un fornitore principale diretto o indiretto a qualsiasi livello del governo degli Stati Uniti, conformemente all'articolo 48 C.F.R. 227.7202-4 (per gli acquisti realizzati dal DOD, Department of Defens - Dipartimento della Difesa) e gli articoli 48 C.F.R. 2.101 e 12.212 (per gli acquisti non realizzati dal DOD), i diritti del governo relativi a software e documentazione, inclusi quelli relativi a utilizzo, modifica, riproduzione, rilascio, esecuzione, visualizzazione o divulgazione del software o della documentazione, saranno soggetti interamente ai diritti e ai limiti di licenza commerciale previsti nel contratto di licenza.

© 2014 NetIQ Corporation. Tutti i diritti riservati. Per informazioni sui marchi di fabbrica di NetIQ, vedere http://www.netiq.com/company/legal/.

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 Sistema di Gestione servizi di raccolta . . . 19
2.1.3 Stima dei requisiti per la memorizzazione dei dati . . . 19
2.1.4 Stima relativa all'utilizzo dell'operazione di I/O del disco . . . 20
2.1.5 Stima relativa all'utilizzo della larghezza di banda della rete . . . 21
2.1.6 Ambiente virtuale . . . 22
2.2 Sistemi operativi supportati . . . 22
2.2.1 Sentinel Log Manager . . . 22
2.2.2 Gestione servizi di raccolta . . . 22
2.3 Browser supportati . . . 23
2.3.1 Linux . . . 23
2.3.2 Windows . . . 23
2.4 Ambiente virtuale supportato . . . 23
2.5 Connettori supportati . . . 23
2.6 Origini evento supportate . . . 24
2.7 Limiti consigliati . . . 26
2.7.1 Limiti di Gestione servizi di raccolta . . . 26
2.7.2 Limiti dei rapporti . . . 27
2.7.3 Limiti EPS delle azioni . . . 27
2.7.4 Limiti dei file aperti in SLES . . . 28
2.8 Prestazione relativa all'esecuzione delle ricerche e alla generazione dei rapporti . . . 28
2.8.1 Risposta alle ricerche e velocità di completamento . . . 28
2.8.2 Velocità di generazione dei rapporti . . . 29

3 Installazione su un sistema SLES 11 SP1 esistente 31

3.1 Istruzioni preliminari . . . 31
3.2 Installazione standard . . . 32
3.3 Installazione personalizzata . . . 34
3.4 Installazione invisibile all'utente . . . 36
3.5 Installazione non root . . . 37

4 Installazione dell'applicazione 39

4.1 Istruzioni preliminari . . . 39
4.2 Porte utilizzate . . . 39
4.2.1 Porte aperte nel firewall . . . 40
4.2.2 Porte utilizzate localmente . . . 40
4.3 Installazione dell'applicazione VMware . . . 41
4.4 Installazione dell'applicazione Xen . . . 42
4.5 Installazione dell'applicazione sull'hardware . . . 44
4.6 Configurazione post-installazione per l'applicazione . . . 45
4.6.1 Installazione dei VMware Tools . . . 45
4.6.2 Esecuzione del login all'interfaccia Web dell'applicazione . . . 45
4.7 Configurazione di WebYaST . . . 45
4.8 Configurazione dell'applicazione con SMT . . . 47
4.8.1 Prerequisiti . . . 47
4.8.2 Configurazione dell'applicazione . . . 48
4.8.3 Esecuzione dell'upgrade dell'applicazione . . . 48
4.9 Interruzione e avvio dell'applicazione mediante l'interfaccia utente Web . . . 48
4.10 Registrazione degli aggiornamenti . . . 49

5 Esecuzione dell'upgrade di Sentinel Log Manager 51

5.1 Prerequisiti . . . 51
5.2 Esecuzione dell'upgrade del server di Sentinel Log Manager . . . 52
5.3 Esecuzione dell'upgrade della Gestione servizi di raccolta . . . 54
5.4 Esecuzione dell'upgrade dell'applicazione . . . 54
5.4.1 Esecuzione dell'upgrade dell'applicazione mediante WebYast . . . 54
5.4.2 Esecuzione dell'upgrade dell'applicazione mediante Zypper . . . 55
5.4.3 Esecuzione dell'upgrade dell'applicazione mediante SMT . . . 56
5.5 Esecuzione dell'upgrade dei plug-in di Sentinel . . . 56

6 Effettuare il login all'interfaccia Web 57

7 Installazione di Gestioni servizi di raccolta aggiuntive 59

7.1 Istruzioni preliminari . . . 59
7.2 Vantaggi apportati dalla presenza di più Gestioni servizi di raccolta . . . 60
7.3 Installazione di Gestioni servizi di raccolta aggiuntive . . . 60

8 Disinstallazione 63

8.1 Disinstallazione dell'applicazione . . . 63
8.2 Disinstallazione di Sentinel Log Manager . . . 63
8.3 Disinstallazione di Gestione servizi di raccolta . . . 64
8.3.1 Disinstallazione della Gestione servizi di raccolta su Linux . . . 64
8.3.2 Disinstallazione della Gestione servizi di raccolta su Windows . . . 64
8.3.3 Pulizia manuale delle directory . . . 65

A Risoluzione dei problemi relativi all'installazione 67

A.1 L'upgrade di Sentinel Log Manager ha esito negativo se la password dbauser non corrisponde
a quella memorizzata nel file .pgpass . . . 67
A.2 Installazione non riuscita a causa di una configurazione della rete non corretta . . . 68
A.3 Problema di configurazione della rete con VMware Player 3 in SLES 11 . . . 68

A.4 La Gestione servizi di raccolta remota genera un'eccezione in Windows 2008 quando è abilitato UAC 69
A.5 Esecuzione dell'upgrade di Gestione log installata come utente non root diverso dall'utente novell 70
A.6 UUID non dispone di Gestioni servizi di raccolta create mediante immagine 70

Terminologia di Sentinel **71**

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 SP1 esistente”, a pagina 31
- Capitolo 4, “Installazione dell'applicazione”, a pagina 39
- Capitolo 5, “Esecuzione dell'upgrade di Sentinel Log Manager”, a pagina 51
- Capitolo 6, “Effettuare il login all'interfaccia Web”, a pagina 57
- Capitolo 7, “Installazione di Gestioni servizi di raccolta aggiuntive”, a pagina 59
- Capitolo 8, “Disinstallazione”, a pagina 63
- Appendice A, “Risoluzione dei problemi relativi all'installazione”, a pagina 67
- “Terminologia di Sentinel” a pagina 71

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) 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). 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).

Per la documentazione aggiuntiva sulla configurazione di Sentinel Log Manager, consultare la *Sentinel Log Manager 1.2.2 Administration Guide (Guida all'amministrazione di Sentinel Log Manager 1.2).*.

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/)

1 Introduzione

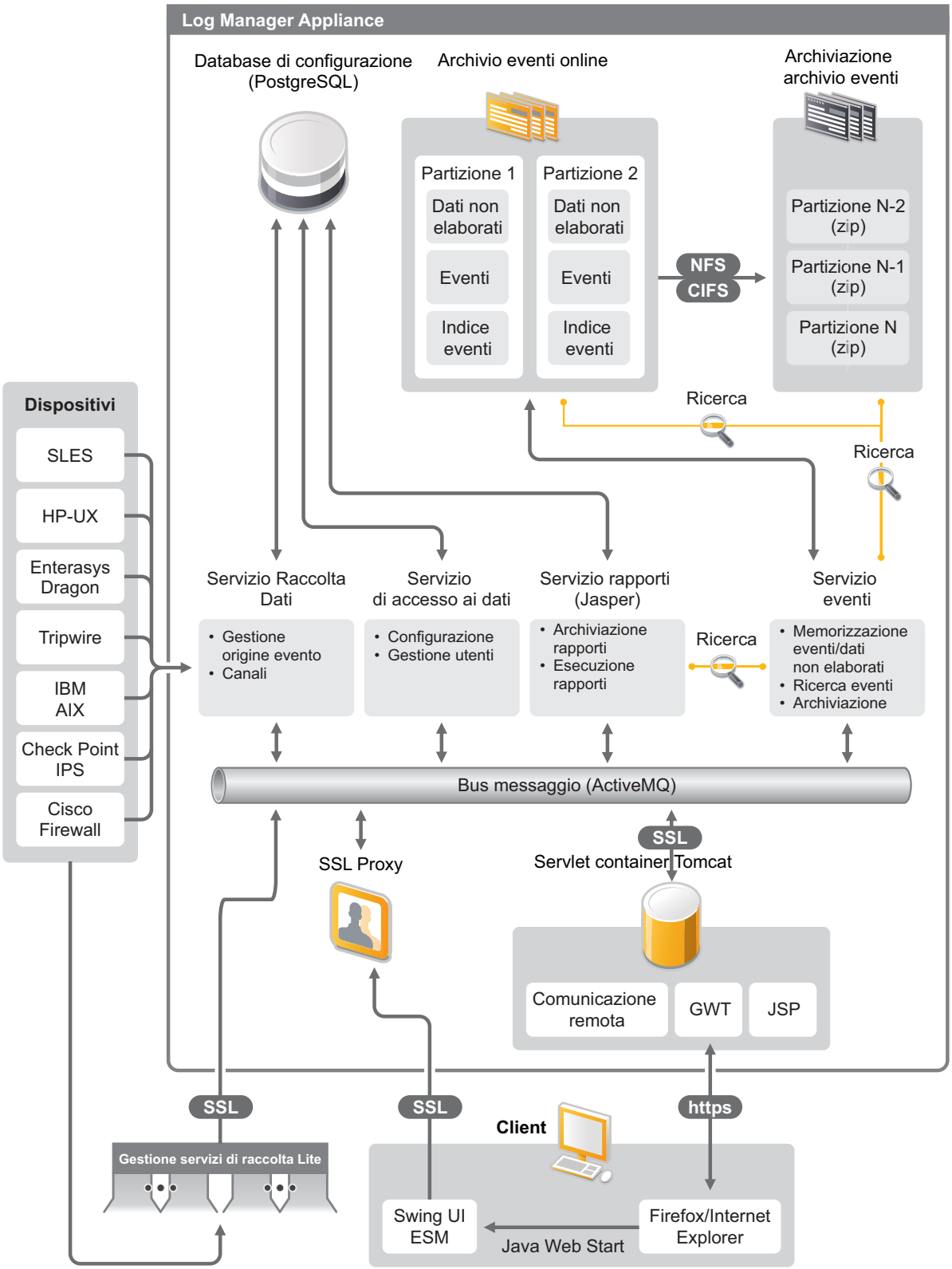
Novell Sentinel Log Manager consente di raccogliere e gestire dati da un'ampia gamma di dispositivi e applicazioni, compresi sistemi di rilevamento intrusioni, firewall, sistemi operativi, router, server Web, database, commutatori, mainframe e origini evento di antivirus. Novell Sentinel Log Manager 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 1.2 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 24.

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).

Per ulteriori informazioni sulla configurazione dei connettori, fare riferimento alla relativa documentazione nel sito Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Per ulteriori informazioni sulla configurazione della raccolta di dati, consultare "Configuring Data Collection (Configurazione della raccolta dei dati)" nella *Sentinel Log Manager 1.2.2 Administration Guide (Guida all'amministrazione di Sentinel Log Manager 1.2)*.

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 dei plug-in di Sentinel 6.1 (http://support.novell.com/products/sentinel/secure/sentinelplugins.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 60.

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 *Sentinel Log Manager 1.2.2 Administration Guide (Guida all'amministrazione di Sentinel Log Manager 1.2)*.

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 *Sentinel Log Manager 1.2.2 Administration Guide (Guida all'amministrazione di Sentinel Log Manager 1.2)*.

Per ulteriori informazioni sulla ricerca di eventi e sulla generazione di rapporti, consultare "Searching Events" (Ricerca di eventi) e "Reporting" (Generazione di rapporti) nella *Sentinel Log Manager 1.2.2 Administration Guide* (Guida all'amministrazione di Sentinel Log Manager 1.2.2).

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 un'applicazione oppure su un sistema operativo SUSE Linux Enterprise Server (SLES) 11 SP1 esistente. Quando Sentinel Log Manager viene installato come un'applicazione, il server di Log Manager viene installato su un sistema operativo SLES 11 SP1.

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 di generazione dei 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 59.

2 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 22
- Sezione 2.3, “Browser supportati”, a pagina 23
- Sezione 2.4, “Ambiente virtuale supportato”, a pagina 23
- Sezione 2.5, “Connettori supportati”, a pagina 23
- Sezione 2.6, “Origini evento supportate”, a pagina 24
- Sezione 2.7, “Limiti consigliati”, a pagina 26
- Sezione 2.8, “Prestazione relativa all'esecuzione delle ricerche e alla generazione dei rapporti”, a pagina 28

2.1 Requisiti hardware

- Sezione 2.1.1, “Server di Sentinel Log Manager”, a pagina 17
- Sezione 2.1.2, “Sistema di Gestione servizi di raccolta”, a pagina 19
- Sezione 2.1.3, “Stima dei requisiti per la memorizzazione dei dati”, a pagina 19
- Sezione 2.1.4, “Stima relativa all'utilizzo dell'operazione di I/O del disco”, a pagina 20
- Sezione 2.1.5, “Stima relativa all'utilizzo della larghezza di banda della rete”, a pagina 21
- Sezione 2.1.6, “Ambiente virtuale”, a pagina 22

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.

Nella tabella seguente sono elencati i requisiti hardware consigliati per un sistema di produzione che conservi i dati online per almeno 90 giorni. Questi requisiti sono consigliati per una dimensione eventi media di 300 byte.

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

Requisiti	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
Numero origini evento massimo	Fino a 1000	Fino a 1000	Fino a 2000
Numero frequenza evento massimo	500	2500	7500
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 locale (30 giorni)	2 unità 7,2k RPM da 500 GB (hardware RAID con 256 MB di cache, RAID 1)	4 unità 7,2k RPM da 1 TB (hardware RAID con 256 MB di cache, RAID 10)	16 unità, 15k RPM da 600 GB, (hardware RAID con 512 MB di cache, RAID 10) o una SAN (Storage Area Network) equivalente
Memorizzazione in rete (90 giorni)	600 GB	2 TB	5,8 TB

Per una prestazione ottimale del sistema, seguire le linee guida seguenti:

- La memorizzazione locale deve disporre di spazio a sufficienza per conservare i dati relativi ad almeno 5 giorni, inclusi i dati evento e i dati non elaborati. Per ulteriori informazioni sul calcolo dei requisiti per la memorizzazione dei dati, consultare Sezione 2.1.3, “Stima dei requisiti per la memorizzazione dei dati”, a pagina 19.
- La memorizzazione in rete contiene tutti i dati relativi ai 90 giorni, oltre a una copia compressa dei dati evento presenti nella memorizzazione locale. Una copia dei dati evento viene conservata nella memorizzazione locale allo scopo di migliorare le prestazioni relative all'esecuzione delle ricerche e alla generazione dei rapporti. Qualora la dimensione della memorizzazione locale non sia adeguata a esigenze specifiche, tale dimensione può essere ridotta. Tuttavia, a causa dell'overhead relativo alla decompressione, vi sarà una diminuzione stimata del 70% della prestazione relativa all'esecuzione delle ricerche e alla generazione dei rapporti sui dati che risiederebbero, altrimenti, nella memorizzazione locale.
- È necessario configurare l'ubicazione della memorizzazione in rete in una SAN (Storage Area Network) o NAS (Network Attached Storage) esterna dotata di più unità.
- 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..
- 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.
- 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 Sistema di Gestione servizi di raccolta

- ❒ Un Intel Xeon X5570 da 2,93 GHz (CPU a 4 core)
- ❒ 4 GB 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 le istruzioni relative all'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 *Sentinel Log Manager 1.2.2 Administration Guide (Guida all'amministrazione di Sentinel Log Manager 1.2)*.

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:

- **Memorizzazione eventi locale (parzialmente compressi):** {dimensione media in byte per evento} x {numero di giorni} x {eventi al secondo} x 0,00007 = totale GB di memorizzazione necessari

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

- **Memorizzazione eventi in rete (completamente compressi):** {dimensione media in byte per evento} x {numero di giorni} x {eventi al secondo} x 0,00002 = totale GB di memorizzazione necessari
- **Memorizzazione dati non elaborati (completamente compressi sia nella memorizzazione locale e che nella memorizzazione in rete):** {dimensione media in byte per record dei dati non elaborati} x {numero di giorni} x {eventi al secondo} x 0,000012 = totale GB di memorizzazione necessari

  Generalmente, la dimensione media dei dati non elaborati per i messaggi syslog è pari a 200 byte.
- **Dimensione totale della memorizzazione locale (con memorizzazione in rete abilitata):**

  {dimensioni memorizzazione eventi locale per il numero di giorni desiderato} + {dimensione memorizzazione dati non elaborati per un giorno) = totale GB di memorizzazione necessari

  Se la memorizzazione in rete è abilitata, quando la memorizzazione locale viene riempita i dati evento vengono spostati nella memorizzazione in rete. Tuttavia, i dati non elaborati vengono ubicati nella memorizzazione locale solo temporaneamente prima di essere spostati nella memorizzazione in rete. Generalmente, lo spostamento dei dati non elaborati dalla memorizzazione locale a quella in rete richiede meno di un giorno.
- **Dimensione totale della memorizzazione locale (con memorizzazione in rete disabilitata):**

  {dimensioni memorizzazione eventi locale per periodo di permanenza} + {dimensioni memorizzazione dati non elaborati per periodo di permanenza) = totale GB di memorizzazione necessari
- **Dimensione totale della memorizzazione in rete:** {dimensioni memorizzazione eventi in rete per periodo di permanenza} + {dimensioni memorizzazione dati non elaborati per periodo di permanenza) = totale GB di memorizzazione necessari

---

Nota:

- I coefficienti in ogni formula rappresentano ((secondi al giorno) x (GB per byte) x rapporto di compressione).
- I numeri rappresentano solo una stima. Essi dipendono dalle dimensioni dei dati evento e dalle dimensioni dei dati compressi.
- Parzialmente compressi significa che vengono compressi solo i dati, mentre il loro indice non viene compresso. Completamente compressi significa che vengono compressi sia i dati evento che i dati dell'indice. Generalmente, i rapporti di compressione dei dati evento sono 10:1. Generalmente, i rapporti di compressione dell'indice sono 5:1. L'indice viene utilizzato per ottimizzare l'esecuzione delle ricerche tra i dati.

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 Stima relativa all'utilizzo dell'operazione di I/O del disco

Utilizzare le formule seguenti per valutare la quantità di utilizzo del disco sul server in base a varie frequenze EPS.

- **Dati scritti sul disco (kilobyte al secondo):** (dimensione media degli eventi in byte + dimensione media dei dati non elaborati in byte) x (eventi al secondo) x coefficiente di compressione pari a .004 = dati scritti al secondo sul disco

Ad esempio, a 500 EPS, per una dimensione media degli eventi pari a 464 byte e una dimensione media dei dati non elaborati pari a 300 byte nel file di log, i dati scritti sul disco vengono determinati nel modo seguente:

(464 byte + 300 byte) x 500 EPS x .004 = 1558 KB

- **Numero di richieste I/O per il disco (trasferimenti al secondo):** (dimensione media degli eventi in byte + dimensione media dei dati non elaborati in byte) x (eventi al secondo) x coefficiente di compressione pari a .00007 = richieste I/O al secondo per il disco

  Ad esempio, a 500 EPS, per una dimensione media degli eventi pari a 464 byte e una dimensione media dei dati non elaborati pari a 300 byte nel file di log, il numero di richieste I/O al secondo per il disco viene determinato nel modo seguente:

  (464 byte + 300 byte) x 500 EPS x .00007 = 26 tps

- **Numero di blocchi scritti al secondo sul disco:** (dimensione media degli eventi in byte + dimensione media dei dati non elaborati in byte) x (eventi al secondo) x coefficiente di compressione pari a .008 = blocchi scritti al secondo sul disco

  Ad esempio, a 500 EPS, per una dimensione media degli eventi pari a 464 byte e una dimensione media dei dati non elaborati pari a 300 byte nel file di log, il numero di blocchi scritti al secondo sul disco viene determinato nel modo seguente:

  (464 byte + 300 byte) x 500 EPS x .008 = 3056

- **Dati letti al secondo dal disco durante l'esecuzione di una ricerca:** (dimensione media degli eventi in byte + dimensione media dei dati non elaborati in byte) x (numero di eventi corrispondenti all'interrogazione in milioni) x coefficiente di compressione pari a .013 = kilobyte letti al secondo dal disco

  Ad esempio, in caso di 3 milioni di eventi corrispondenti all'interrogazione della ricerca, per una dimensione media degli eventi pari a 464 byte e una dimensione media dei dati non elaborati pari a 300 byte nel file di log, il numero di dati letti al secondo dal disco viene determinato nel modo seguente:

  (464 byte + 300 byte) x 3 x .013 = 300 KB

2.1.5 Stima relativa all'utilizzo della larghezza di banda della rete

Utilizzare le seguenti formule per valutare l'utilizzo della banda larga di rete sul server a varie frequenze EPS:

{dimensione media degli eventi in byte + dimensione media dei dati non elaborati in byte} x {eventi al secondo} x coefficiente di compressione pari a .0003 = larghezza di banda della rete in Kbps (kilobit al secondo)

Ad esempio, a 500 EPS, per una dimensione media degli eventi pari a 464 byte e una dimensione media dei dati non elaborati pari a 300 byte nel file di log, l'utilizzo della larghezza di banda della rete viene determinato nel modo seguente:

(464 byte + 300 byte) x 500 EPS x .0003 = 115 Kbps

2.1.6 Ambiente virtuale

Sentinel Log Manager è stato ampiamente verificato ed è totalmente supportato in un server VMware ESX. Per ottenere in ESX o in qualsiasi altro ambiente virtuale prestazioni paragonabili ai risultati ottenuti nei test effettuati su computer fisici, memoria, CPU, spazio su disco e I/O dell'ambiente virtuale devono essere uguali a quelli consigliati per i computer fisici.

Per ulteriori informazioni sui consigli relativi al computer fisico, consultare Sezione 2.1, “Requisiti hardware”, a pagina 17.

2.2 Sistemi operativi supportati

Novell supporta Sentinel Log Manager sui sistemi operativi descritti in questa sezione. Novell supporta Sentinel Log Manager anche sui sistemi che dispongono di aggiornamenti secondari per tali sistemi operativi, come patch sulla sicurezza o correzioni HotFix. Tuttavia, l'esecuzione di Sentinel Log Manager sui sistemi che dispongono di aggiornamenti primari per tali sistemi operativi non sarà supportata fino a quando Novell non abbia eseguito le verifiche e le certificazioni necessarie per tali aggiornamenti.

- Sezione 2.2.1, “Sentinel Log Manager”, a pagina 22
- Sezione 2.2.2, “Gestione servizi di raccolta”, a pagina 22

2.2.1 Sentinel Log Manager

- ❒ SUSE Linux Enterprise Server 11 SP3 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 22
- “Windows” a pagina 22

Linux

- ❒ SUSE Linux Enterprise Server 11 SP3 (a 64 bit)

Windows

- ❒ Windows Server 2003 (32 bit e 64 bit)
- ❒ Windows Server 2003 SP2 (32 bit e 64 bit)
- ❒ Windows Server 2003 R2 (32 bit e 64 bit)
- ❒ Windows Server 2008 (64 bit)
- ❒ Windows Server 2008 R2 (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 23
- Sezione 2.3.2, “Windows”, a pagina 23

2.3.1 Linux

- ❒ Mozilla Firefox 5 e versioni successive

2.3.2 Windows

- ❒ Mozilla Firefox 5 e versioni successive
- ❒ Microsoft Internet Explorer 8 e 11*

* Vedere “Prerequisiti per Internet Explorer” a pagina 23.

Prerequisiti per Internet Explorer

- Se il Livello di protezione in Internet è impostato su Alta, una volta effettuato l'accesso a 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~)
- 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 eseguita questa operazione, queste origini evento vengono visualizzate nell'interfaccia Web di Sentinel Log Manager > *servizio di raccolta* > *Origini evento*.

I servizi di raccolta che supportano origini evento addizionali possono essere ottenuti dal sito Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.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).

2.7 Limiti consigliati

I limiti indicati nella sezione sono consigliati in base ai test sulle prestazioni effettuati presso Novell o le sedi dei clienti. Non si tratta di limiti rigidi. I consigli sono approssimativi. In sistemi estremamente dinamici, è opportuno creare buffer incorporati e lasciare spazio per l'eventuale aumento di volume.

- Sezione 2.7.1, “Limiti di Gestione servizi di raccolta”, a pagina 26
- Sezione 2.7.2, “Limiti dei rapporti”, a pagina 27
- Sezione 2.7.3, “Limiti EPS delle azioni”, a pagina 27
- Sezione 2.7.4, “Limiti dei file aperti in SLES”, a pagina 28

2.7.1 Limiti di Gestione servizi di raccolta

Salvo indicazioni diverse, i limiti di Gestione servizi di raccolta presuppongono 4 core CPU a 2,2 GHz ciascuno, 4 GB di RAM, quando è in esecuzione su SLES 11.

Tabella 2-2 *Numeri delle prestazioni di Gestione servizi di raccolta*

Attributo	Limiti dei	Commenti
Numero massimo di istanze di Gestione servizi di raccolta	20	Il limite specificato presuppone che ciascuna Gestione servizi di raccolta sia in esecuzione con una bassa frequenza EPS (ad esempio, meno di 100 EPS). Il limite diminuisce proporzionalmente all'aumento degli eventi al secondo.
Numero massimo di connettori (utilizzati appieno) in un'unica Gestione servizi di raccolta	1 per core CPU, con almeno un 1 core CPU riservato per il sistema operativo e altre elaborazioni	Un connettore utilizzato appieno, è un connettore che viene eseguito con una frequenza EPS massima per il suo genere.
Numero massimo di connettori (utilizzati appieno) in un'unica Gestione servizi di raccolta	1 per core CPU, con almeno un 1 core CPU riservato per il sistema operativo e altre elaborazioni	Un servizio di raccolta utilizzato appieno, è un servizio che viene eseguito con una frequenza EPS massima per il suo genere.

Attributo	Limiti dei	Commenti
Numero massimo di origini eventi in un'unica Gestione servizi di raccolta	2000	Il limite del server di Sentinel Log Manager è 1000 o 2000, a seconda delle caratteristiche hardware. Qualora su un'unica Gestione servizi di raccolta venga raggiunto il limite del server, ciò significa che con quella sola Gestione servizi di raccolta è stato raggiunto il limite delle origini evento per l'intero sistema di Sentinel.
Numero massimo di origini evento per l'istanza del server di Sentinel Log Manager	2000	

2.7.2 Limiti dei rapporti

Tabella 2-3 *Numeri di prestazioni dei rapporti*

Attributo	Limiti dei	Commenti
Numero massimo di rapporti salvati	200	
Numero massimo di rapporti contemporaneamente in esecuzione	3	Il limite presume che il server non venga già ampiamente utilizzato per l'elaborazione della raccolta dei dati o di altri task.

2.7.3 Limiti EPS delle azioni

Se non altrimenti specificato, i limiti EPS delle azioni presumono che venga configurata un'azione per regola.

Tabella 2-4 *Numeri relativi alla prestazione delle azioni*

Azione	EPS per azione
Collegamento Sentinel	300
Registra su file	30 - 50
Invia un e-mail	40
Registra su Syslog	5 - 10
Esegui script	5 - 10

2.7.4 Limiti dei file aperti in SLES

Nei sistemi che dispongono di un numero elevato di origini evento (ad esempio, più di 75), in cui la maggior parte utilizza il connettore di file e la differenza è impostata all'inizio del file, il limite di file aperti in SLES potrebbe non essere uguale al numero di file attualmente aperti nel sistema e ciò potrebbe provocare dei problemi relativi alla prestazione di Sentinel Log Manager.

Onde evitare questo problema, è possibile impostare i limiti flessibili e quelli rigidi per il numero massimo di file aperti in base al numero di file che sono aperti.

Per impostare i limiti dei file aperti eseguire i passaggi seguenti:

1. Eseguire il login al sistema come utente Novell.
2. Visualizzare il numero di file che sono aperti per l'utente (Novell) di Sentinel.

   ```
   lsof | wc -l
   ```

3. Visualizzare i limiti flessibili e rigidi:

   ```
   ulimit -Hn
   ```

   ```
   ulimit -Sn
   ```

   In base al numero di file aperti, possono essere impostati i limiti del descrittore di file nel file `/etc/security/limits.conf` file can be set. Ad esempio, se il numero di file aperti è 1000, i limiti possono essere impostati su 2000.

   Nota: Solo l'utente root può modificare il file `/etc/security/limits.conf`.

4. Assicurarsi che l'utente root imposti i limiti del descrittore di file come descritto di seguito:

   ```
   novell soft nofile 2000
   ```

   ```
   novell hard nofile 2000
   ```

   Nota: l'impostazione dei limiti flessibili è facoltativa mentre l'impostazione del limite rigido è obbligatoria.

5. Salvare le modifiche.

2.8 Prestazione relativa all'esecuzione delle ricerche e alla generazione dei rapporti

La prestazione di Sentinel Log Manager può variare in base all'ambiente, alla configurazione e alle caratteristiche hardware. Novell ha eseguito delle verifiche approfondite sulle prestazioni relative al sistema di Sentinel Log Manager per convalidare e verificare gli attributi qualitativi del sistema, quali la scalabilità, l'affidabilità e l'utilizzo delle risorse.

- Sezione 2.8.1, “Risposta alle ricerche e velocità di completamento”, a pagina 28
- Sezione 2.8.2, “Velocità di generazione dei rapporti”, a pagina 29

2.8.1 Risposta alle ricerche e velocità di completamento

Diverse verifiche sono state condotte con la configurazione seguente per determinare il tempo necessario a una ricerca per restituire i dati iniziali:

- **Hardware:** CPU a 4 core con 2.93 GHz ciascuna, 4 GB di RAM, in esecuzione su SLES 11

- **Frequenza EPS:** la frequenza EPS in entrata durante l'elaborazione di una ricerca è pari a 2000
- **Memorizzazione dei dati:** tutti i dati evento nell'intervallo di tempo risiedono nella memorizzazione locale

A seguire, i dati osservati grazie a tali verifiche:

Tabella 2-5 *Risultati relativi all'elaborazione ricerche*

Eventi totali	Numero di eventi corrispondenti all'interrogazione della ricerca	Tempo per i risultati della ricerca iniziale
10.000.000	1.000 - 10.000.000	5 - 10 secondi
100.000.000	20.000.000 - 100.000.000	10 – 30 secondi
200.000.000	110.000.000 - 200.000.000	1 – 5 minuti

2.8.2 Velocità di generazione dei rapporti

Diverse verifiche sono state condotte con la configurazione seguente per determinare il tempo necessario alla generazione dei rapporti.

- **Hardware:** CPU a 4 core con 2.93 GHz ciascuna, 4 GB di RAM, in esecuzione su SLES 11
- **Frequenza EPS:** la frequenza EPS in entrata durante l'elaborazione di una ricerca è pari a 2000
- **Ubicazione dei dati:** tutti i dati evento nell'intervallo di tempo risiedono nella memorizzazione locale

A seguire, i dati osservati grazie a tali verifiche:

Tabella 2-6 *Risultati relativi alla generazione dei rapporti*

Eventi totali	Numero di eventi corrispondenti all'interrogazione della ricerca	Tempo necessario alla generazione del rapporto
10.000.000	1.000 - 10.000.000	1 - 2 minuti
100.000.000	20.000.000 - 100.000.000	10 – 50 minuti
200.000.000	110.000.000 - 200.000.000	1 – 3 ore

Nota: per i rapporti con un numero superiore di eventi e di campi, come ad esempio il rapporto relativo ai dettagli evento, la generazione potrebbe richiedere molto tempo e il sistema potrebbe esaurire la memoria. Per migliorare le prestazioni di generazione dei rapporti è possibile aumentare la RAM del sistema.

3 Installazione su un sistema SLES 11 SP1 esistente

Questa sezione descrive la procedura di installazione di Sentinel Log Manager su un sistema SUSE Linux Enterprise Server (SLES) 11 SP1 esistente utilizzando 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 36.

- Sezione 3.1, “Istruzioni preliminari”, a pagina 31
- Sezione 3.2, “Installazione standard”, a pagina 32
- Sezione 3.3, “Installazione personalizzata”, a pagina 34
- Sezione 3.4, “Installazione invisibile all'utente”, a pagina 36
- Sezione 3.5, “Installazione non root”, a pagina 37

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.
- Assicurarsi che l'rpm libstdc++33-32-bit sia installato. È possibile installare questo RPM utilizzando YaST oppure il comando Zypper:

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

- Per il funzionamento ottimale di Sentinel Log Manager 1.2 e versioni successive su SLES 11 SP1, devono essere installate le versioni seguenti o successive di Redhat Package Manager (RPM):
  - **Patch kernel:**
    - `kernel-default-2.6.32.29-0.3.1.x86_64.rpm`
    - `kernel-default-base-2.6.32.29-0.3.1.x86_64.rpm`

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

  Sentinel Log Manager 1.1.0.x utilizza la versione 3.4-35.1 di Squashfs, mentre SLES 11 SP1 supporta Squashfs 4.0 e versioni successive, che non sono compatibili con le versioni precedenti e non consentono di aprire un file system compresso creato utilizzando tali versioni. Grazie all'installazione di questi RPM, viene risolto il problema relativo all'incompatibilità tra le versioni squashfs di Sentinel Log Manager 1.1.0.x e quelle di SLES 11 SP1.

  Questi RPM sono disponibili nel canale di aggiornamento online di SLES 11. Per ulteriori informazioni sull'aggiornamento del sistema SLES, vedere "YaST Online Update (Aggiornamento online di YaST)" (http://www.novell.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html) nella *SLES 11 SP1 Administration Guide (Guida all'amministrazione di SLES 11 SP1) (http://www.novell.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html)*.

  Nota: la procedura di installazione si blocca fino a quando non vengono installati gli RPM e le patch kernel e Linux sopra specificate.

- 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

  Per ulteriori informazioni sull'utilizzo di queste porte, consultare Sezione 4.2, "Porte utilizzate", a pagina 39.

3.2 Installazione standard

La procedura di installazione standard consente di installare Sentinel Log Manager con una licenza di valutazione di 60 giorni, completa di tutte le funzioni eccetto Ripristino dati.

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 Modificare la directory in cui è stato estratto il file di installazione.

5 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
```

6 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.

7 Leggere la licenza con l'utente finale e immettere `yes` o `y` 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`.

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

L'installazione continua utilizzando la chiave di licenza di valutazione di 60 giorni inclusa nel programma di installazione. Questa chiave di licenza consente di attivare le serie completa delle funzioni del prodotto, eccetto la funzione per il Ripristino dati, per un periodo di prova di 60 giorni. In qualsiasi momento, durante o dopo il periodo di prova, è possibile sostituire la licenza di valutazione con una chiave di licenza acquistata.

9 Specificare la password per l'utente amministratore.

10 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.

11 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 6, “Effettuare il login all'interfaccia Web”, a pagina 57.

12 Per configurare le origini evento per l'invio dei dati a Sentinel Log Manager, consultare “Configuring Data Collection (Configurazione della raccolta dei dati)” nella *Sentinel Log Manager 1.2.2 Administration Guide (Guida all'amministrazione di Sentinel Log Manager 1.2)*.

Nota: Dopo avere eseguito l'installazione, la prima volta in cui viene avviato il sistema potrebbero essere necessari cinque minuti circa per la sua inizializzazione prima di poterlo utilizzare. Tale ritardo si verifica solo la prima volta in cui il sistema viene avviato dopo aver eseguito l'installazione o un aggiornamento.

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 1.2.2*.

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. Modificare la directory in cui è stato estratto il file di installazione.
5. Specificare il seguente comando per eseguire lo script `install-slm` necessario per l'installazione di Sentinel Log Manager:

   ```
   ./install-slm
   ```
6. 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.
7. Leggere la licenza con l'utente finale e immettere `yes` o `y` 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`.
8. Quando richiesto, specificare l'opzione per procedere all'installazione personalizzata.
9. Quando viene richiesto di specificare l'opzione della chiave di licenza, immettere `2` per specificare la chiave di licenza per il prodotto acquistato.
10. Specificare la chiave di licenza, quindi premere Invio.

    Per ulteriori informazioni sulle chiavi di licenza, consultare "License Information (Informazioni sulla licenza)" nella *Guida all'amministrazione di Sentinel Log Manager 1.2.2*.
11. Specificare la password per l'utente amministratore.
12. Confermare la password per l'utente amministratore.
13. Specificare la password per l'amministratore del database (dbauser).
14. Confermare la password per l'amministratore del database (dbauser).

15 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.

16 Specificare l'opzione per autenticare gli utenti mediante una directory LDAP esterna.

17 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.

18 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.

19 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.

20 (Condizionale) Se si seleziona la connessione LDAP SSL/TSL, specificare se il certificato del server LDAP è firmato da una CA nota.

21 (Condizionale) Se è stato specificato `n`, specificare il nome file del certificato del server LDAP.

22 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.

23 (Condizionale) Se è stata selezionata la ricerca in modalità anonima, specificare l'attributo di ricerca e passare a Passo 26.

24 (Condizionale) Se non è stata selezionata la ricerca in modalità autonoma in Passo 22, 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.

25 (Condizionale) Se si desidera utilizzare questo metodo per Active Directory, specificare il nome del dominio.

26 Specificare il DN di base.

27 Premere s per specificare che le opzioni fornite sono corrette, altrimenti n e modificare la configurazione.

28 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 6, “Effettuare il login all'interfaccia Web”, a pagina 57.

29 Per configurare le origini evento per l'invio dei dati a Sentinel Log Manager, consultare “Configuring Data Collection (Configurazione della raccolta dei dati)” nella *Sentinel Log Manager 1.2.2 Administration Guide (Guida all'amministrazione di Sentinel Log Manager 1.2)*.

Nota: Dopo avere eseguito l'installazione, la prima volta in cui viene avviato il sistema potrebbero essere necessari cinque minuti circa per la sua inizializzazione prima di poterlo utilizzare. Tale ritardo si verifica solo la prima volta in cui il sistema viene avviato dopo aver eseguito l'installazione o un aggiornamento.

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 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 Modificare la directory in cui è stato estratto il file di installazione.

5 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 32. L'installazione prosegue con i valori memorizzati nel file di risposta.

6 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 6, “Effettuare il login all'interfaccia Web”, a pagina 57.

7 Per configurare le origini evento per l'invio dei dati a Sentinel Log Manager, consultare “Configuring Data Collection (Configurazione della raccolta dei dati)” nella “Sentinel Log Manager 1.2.2 Administration Guide (Guida all'amministrazione di Sentinel Log Manager 1.2)”.

Nota: Dopo avere eseguito l'installazione, la prima volta in cui viene avviato il sistema potrebbero essere necessari cinque minuti circa per la sua inizializzazione prima di poterlo utilizzare. Tale ritardo si verifica solo la prima volta in cui il sistema viene avviato dopo aver eseguito l'installazione o un aggiornamento.

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 utente (`novell`) di tipo non root.

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. Modificare la directory in cui è stato estratto il file di installazione.
5. 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`.
6. Accettare l'elenco dei comandi.

   Vengono eseguiti i comandi visualizzati.
7. Specificare il comando seguente per passare all'utente (`novell`) non root appena creato:

   ```
   su novell
   ```
8. Immettere il comando seguente:

   ```
   ./install-slm
   ```
9. 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.
10. Leggere la licenza con l'utente finale e immettere `yes` o `y` 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.
11. Viene richiesto di specificare la modalità di installazione.
    - Se si sceglie di procedere con l'installazione standard, continuare con il passaggio 8 in Sezione 3.2, “Installazione standard”, a pagina 32.
    - Se si sceglie di procedere con l'installazione personalizzata, continuare con Fase 8 in Sezione 3.3, “Installazione personalizzata”, a pagina 34.

    Viene completata l'installazione di Sentinel Log Manager e il server viene avviato.
12. Specificare il comando seguente per modificare l'utente `root`:

    ```
    su root
    ```
13. Specificare il comando seguente per terminare l'installazione:

    ```
    ./bin/root_install_finish
    ```
14. 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 6, “Effettuare il login all'interfaccia Web”, a pagina 57.

Nota: Dopo avere eseguito l'installazione, la prima volta in cui viene avviato il sistema potrebbero essere necessari cinque minuti circa per la sua inizializzazione prima di poterlo utilizzare. Tale ritardo si verifica solo la prima volta in cui il sistema viene avviato dopo aver eseguito l'installazione o un aggiornamento.

---

4 Installazione dell'applicazione

Sentinel Log Manager Appliance è pronta per eseguire l'applicazione software creata su SUSE Studio che unisce un sistema SUSE Linux Enterprise Server (SLES) 11 SP1 di protezione avanzata con un servizio di aggiornamento del software Novell Sentinel Log Manager integrato, allo scopo di fornire un'esperienza utente più semplice ed efficace, volta a incrementare gli investimenti realizzati dal cliente. L'applicazione software può essere installata sia su hardware che in un ambiente virtuale.

- Sezione 4.1, “Istruzioni preliminari”, a pagina 39
- Sezione 4.2, “Porte utilizzate”, a pagina 39
- Sezione 4.3, “Installazione dell'applicazione VMware”, a pagina 41
- Sezione 4.4, “Installazione dell'applicazione Xen”, a pagina 42
- Sezione 4.5, “Installazione dell'applicazione sull'hardware”, a pagina 44
- Sezione 4.6, “Configurazione post-installazione per l'applicazione”, a pagina 45
- Sezione 4.7, “Configurazione di WebYaST”, a pagina 45
- Sezione 4.8, “Configurazione dell'applicazione con SMT”, a pagina 47
- Sezione 4.9, “Interruzione e avvio dell'applicazione mediante l'interfaccia utente Web”, a pagina 48
- Sezione 4.10, “Registrazione degli aggiornamenti”, a pagina 49

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).
- Per la registrazione degli aggiornamenti del software, richiedere il codice di registrazione al Servizio clienti Novell (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 40
- Sezione 4.2.2, “Porte utilizzate localmente”, a pagina 40

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.
TCP 80	Inoltrata a 8080 per il server Web di Sentinel Log Manager per la comunicazione HTTP.
TCP 8443	Utilizzata per la comunicazione HTTPS.
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 internal_gateway_server e internal_gateway. 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 per 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_vmx.tar.gz>*

2. Specificare il comando seguente per estrarre l'immagine compressa dell'applicazione dal computer in cui è installato VM Converter:

   ```
   tar zxvf <install_file>
   ```

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

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

12 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 (Configurazione di rete).
- Per modificare le impostazioni di connessione alla rete, selezionare *Modifica*.

13 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. È possibile utilizzare WebYaST per modificare la data e l'ora 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
```

---

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

15 Impostare la password `root`, quindi fare clic su *Avanti*.

16 Impostare la password admin e la password dbauser di Sentinel Log Manager, quindi fare clic su *Avanti*.

17 Selezionare *Avanti*.

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

18 Procedere con Sezione 4.6, “Configurazione post-installazione per l'applicazione”, a pagina 45.

Nota: Dopo avere eseguito l'installazione, la prima volta in cui viene avviato il sistema potrebbero essere necessari cinque minuti circa per la sua inizializzazione prima di poterlo utilizzare. Tale ritardo si verifica solo la prima volta in cui il sistema viene avviato dopo aver eseguito l'installazione o un aggiornamento.

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_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 `disk`.

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_1.2.0.0_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.2.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.2.0.0_64_Xen.x86_64-0.777.0.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```

6 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_1.2.0.0_64"` nel file `.xenconfig`, la macchina virtuale viene visualizzata con tale 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_1.2.0.0_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 di dominio. Assicurarsi che l'opzione *Assegnare il nome host all'IP di loopback* sia selezionata.

14 Selezionare *Avanti*. La configurazione del nome host è salvata.

15 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(Configurazione di rete).
- 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 45.

Nota: Dopo avere eseguito l'installazione, la prima volta in cui viene avviato il sistema potrebbero essere necessari cinque minuti circa per la sua inizializzazione prima di poterlo utilizzare. Tale ritardo si verifica solo la prima volta in cui il sistema viene avviato dopo aver eseguito l'installazione o un aggiornamento.

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 schemata Nome host e nome dominio, specificare il nome host e il nome del dominio.

Assicurarsi che l'opzione *Assegnare il nome host all'IP di loopback* 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 (Configurazione di rete).
- 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 Reimpostare le configurazioni del terminale:

```
reset
```

16 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.

17 Procedere con Sezione 4.6, “Configurazione post-installazione per l'applicazione”, a pagina 45.

Nota: Dopo avere eseguito l'installazione, la prima volta in cui viene avviato il sistema potrebbero essere necessari cinque minuti circa per la sua inizializzazione prima di poterlo utilizzare. Tale ritardo si verifica solo la prima volta in cui il sistema viene avviato dopo aver eseguito l'installazione o un aggiornamento.

4.6 Configurazione post-installazione per l'applicazione

- Sezione 4.6.1, “Installazione dei VMware Tools”, a pagina 45
- Sezione 4.6.2, “Esecuzione del login all'interfaccia Web dell'applicazione”, a pagina 45

4.6.1 Installazione dei VMware Tools

Per un funzionamento ottimale di Sentinel Log Manager sul server VMware, è necessario installare VMware Tools. VMware Tools è una suite di utility che migliora la prestazione del sistema operativo della macchina virtuale, oltre a rendere più efficace la gestione della macchina virtuale. Per ulteriori informazioni sull'installazione di VMware Tools, vedere VMware Tools for Linux Guests (https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177) (VMware Tools per i guest Linux).

Per ulteriori informazioni sulla documentazione relativa VMware, vedere Workstation User's Manual (http://www.vmware.com/pdf/ws71_manual.pdf) (Manuale dell'utente della workstation).

4.6.2 Esecuzione del login all'interfaccia Web dell'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, consultare la *Sentinel Log Manager 1.2.2 Administration Guide* (Guida all'amministrazione di Sentinel Log Manager 1.2.2).

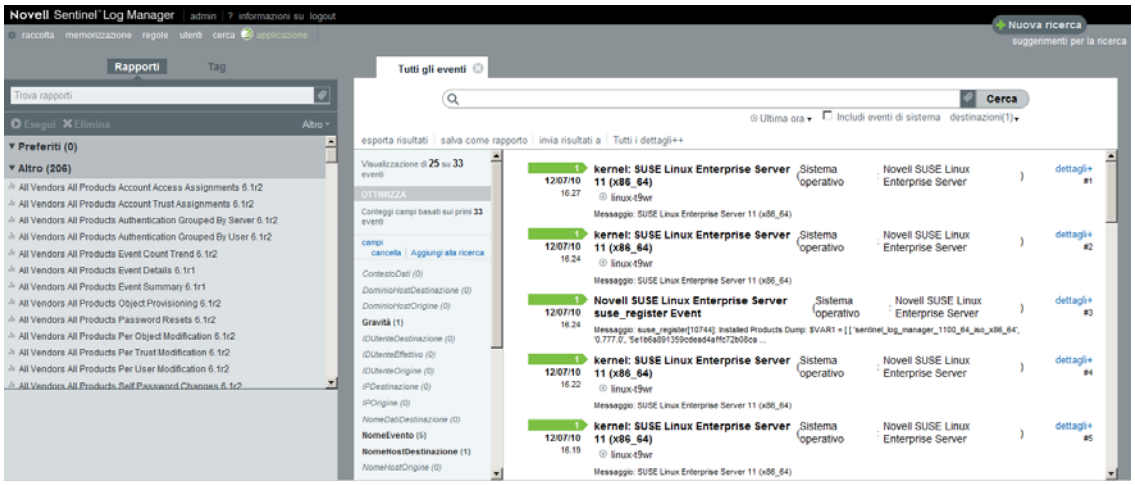
3 Per effettuare la registrazione per gli aggiornamenti, consultare Sezione 4.10, “Registrazione degli aggiornamenti”, a pagina 49.

4.7 Configurazione di WebYaST

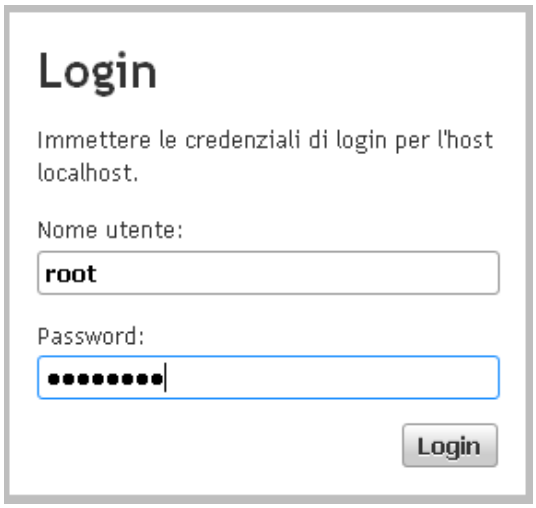
L'interfaccia utente di Novell Sentinel Log Manager Appliance include WebYaST. WebYaST è una console remota basata sul Web per il controllo delle applicazioni che si basano su SUSE Linux Enterprise. Mediante WebYaST è possibile accedere, configurare e controllare le applicazioni di

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/).

1 Effettuare il login a Sentinel Log Manager Appliance.



2 Fare clic su *Applicazione*.



3 Configurare il server di Sentinel Log Manager per ricevere gli aggiornamenti come descritto in Sezione 4.10, “Registrazione degli aggiornamenti”, a pagina 49.

4 Fare clic su *Avanti* per completare la configurazione iniziale.

4.8 Configurazione dell'applicazione con SMT

Negli ambienti protetti in cui l'applicazione deve essere eseguita senza un accesso diretto a Internet, è necessario configurare l'applicazione con Subscription Management Tool (SMT), mediante il quale è possibile eseguire l'upgrade dell'applicazione alle versioni più recenti disponibili. SMT è un sistema proxy a pacchetti integrato in Novell Customer Center completo di importanti funzionalità.

- Sezione 4.8.1, “Prerequisiti”, a pagina 47
- Sezione 4.8.2, “Configurazione dell'applicazione”, a pagina 48
- Sezione 4.8.3, “Esecuzione dell'upgrade dell'applicazione”, a pagina 48

4.8.1 Prerequisiti

- Disporre delle credenziali di Novell Customer Center per Sentinel Log Manager in modo da poter usufruire degli aggiornamenti concessi da Novell. Per ulteriori informazioni su come disporre delle credenziali, contattare l'assistenza Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup).
- Assicurarsi che SLES 11 SP1 sia installato con i pacchetti seguenti sul computer in cui si desidera installare SMT:
  - htmldoc
  - smt
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - pertl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - smt-support
  - yast2-smt
  - yum-metadata-parser
  - createrepo
  - sle-smt-release-cd
  - sle-smt_en
  - perl-DBI
  - apache2-prefork
  - libapr1
  - perl-Data-ShowTable
  - perl-Net-Daemon
  - perl-Tie-IxHash
  - fltk
  - libapr-util1
  - perl-PIRPC
  - apache2-mod_perl
  - apache2-utils

- apache2
- perl-DBD-mysql

- Installare SMT e configurare il server SMT. Per ulteriori informazioni, consultare le sezioni seguenti presenti nella documentazione di SMT (http://www.novell.com/documentation/smt11/):
  - SMT Installation (Installazione di SMT)
  - SMT Server Configuration (Configurazione del server SMT)
  - Mirroring Installation and Update Repositories with SMT (Esecuzione della copia speculare dell'installazione e aggiornamento degli archivi con SMT)
- Installare l'utility `wget` sul computer in cui risiede l'applicazione.

4.8.2 Configurazione dell'applicazione

Per ulteriori informazioni sulla configurazione dell'applicazione con SMT, consultare "Configuring Clients to Use SMT (Configurazione dei client per l'utilizzo di SMT)" (http://www.novell.com/documentation/smt11/smt_sle_11_guide/?page=/documentation/smt11/smt_sle_11_guide/data/smt_client.html) nella documentazione di *Subscription Management Tool* .

Per abilitare gli archivi dell'applicazione, eseguire il comando seguente:

- **Immagine dell'applicazione VMWare:**

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

- **Immagine dell'applicazione Xen:**

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

- **ISO:**

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

4.8.3 Esecuzione dell'upgrade dell'applicazione

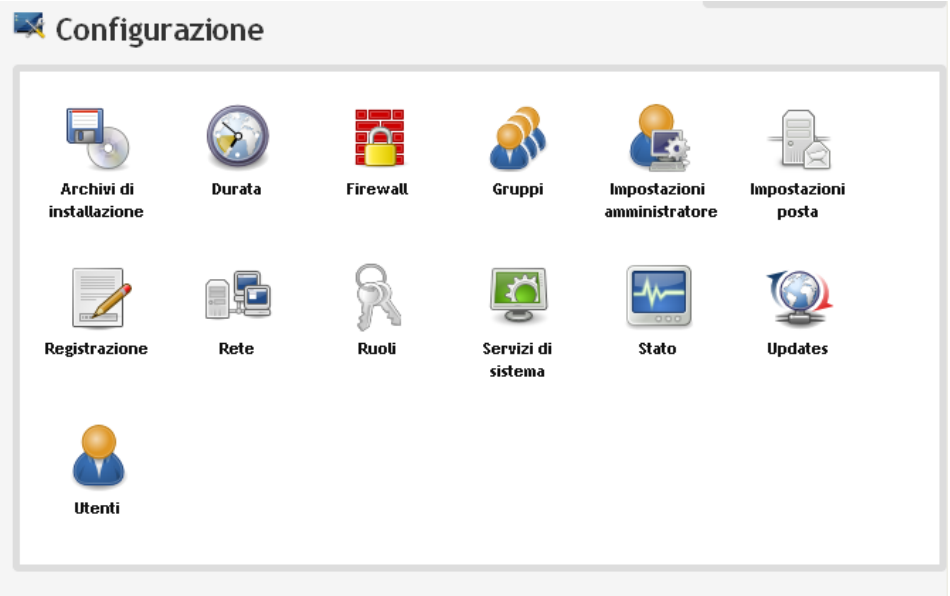
Per ulteriori informazioni relative all'upgrade dell'applicazione, vedere Sezione 5.4.3, "Esecuzione dell'upgrade dell'applicazione mediante SMT", a pagina 56.

4.9 Interruzione e avvio dell'applicazione mediante l'interfaccia utente Web

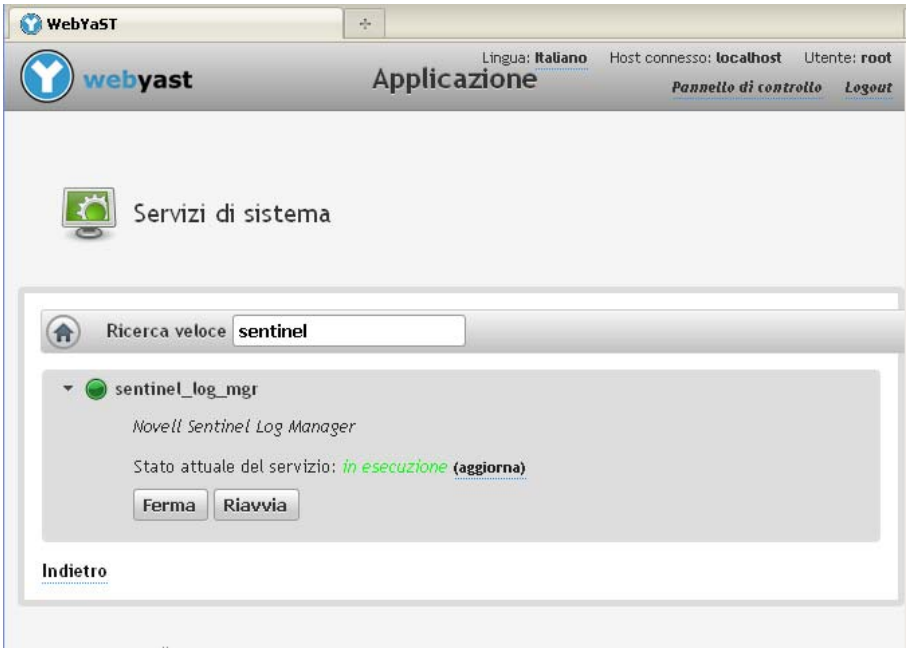
È possibile avviare e interrompere il server di Sentinel Log Manager mediante l'interfaccia utente Web nel modo seguente:

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 *Servizi di sistema*.



4 Per interrompere il server Sentinel Log Manager, fare clic su *Interrompi*.

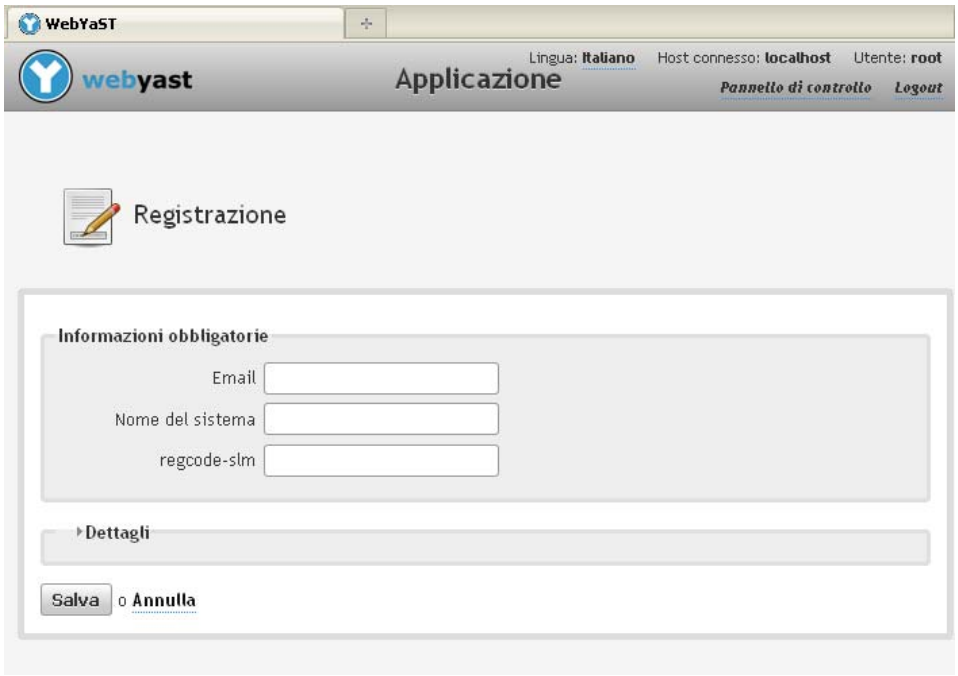
5 Per avviare il server Sentinel Log Manager, fare clic su *Avvia*.

4.10 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*.



4 Specificare l'ID dell'e-mail dove si desidera ricevere gli aggiornamenti, il nome del sistema e il codice di registrazione dell'applicazione.

5 Fare clic su *Salva*.

Per ulteriori informazioni sull'esecuzione dell'upgrade dell'applicazione, consultare Sezione 5.4, “Esecuzione dell'upgrade dell'applicazione”, a pagina 54.

5 Esecuzione dell'upgrade di Sentinel Log Manager

È possibile installare Sentinel Log Manager 1.2.0.2 su Sentinel Log Manager 1.2 e versioni successive. Se si desidera eseguire l'upgrade di Sentinel Log Manager versioni 1.1.*x*, è necessario prima di tutto eseguire l'upgrade a Sentinel Log Manager 1.2.0.1 e quindi installare Sentinel Log Manager 1.2.0.2.

Nota: Una volta eseguito l'upgrade, vengono conservate tutte le personalizzazioni dei servizi di raccolta elaborate utilizzando la modalità Esecuzione personalizzata e il metodo del file ausiliario, come consigliato nella documentazione di SDK.

- Sezione 5.1, “Prerequisiti”, a pagina 51
- Sezione 5.2, “Esecuzione dell'upgrade del server di Sentinel Log Manager”, a pagina 52
- Sezione 5.3, “Esecuzione dell'upgrade della Gestione servizi di raccolta”, a pagina 54
- Sezione 5.4, “Esecuzione dell'upgrade dell'applicazione”, a pagina 54
- Sezione 5.5, “Esecuzione dell'upgrade dei plug-in di Sentinel”, a pagina 56

5.1 Prerequisiti

- Sentinel Log Manager 1.2 e versioni successive richiedono la piattaforma SUSE Linux Enterprise Server (SLES) 11 SP1. Se si sta eseguendo l'upgrade a Sentinel Log Manager 1.2 o a una versione successiva, assicurarsi che la versione del sistema operativo sia SLES 11 SP1.
- Per il funzionamento ottimale di Sentinel Log Manager 1.2 e versioni successive su SLES 11 SP1, devono essere installate le versioni seguenti o successive di Redhat Package Manager (RPM):
  - **Patch kernel:**
    - `kernel-default-2.6.32.29-0.3.1.x86_64.rpm`
    - `kernel-default-base-2.6.32.29-0.3.1.x86_64.rpm`
  - **RPM per util-linux:**
    - `libblkid1-2.16-6.11.1.x86_64.rpm`
    - `libuuid1-2.16-6.11.1.x86_64.rpm`
    - `util-linux-2.16-6.11.1.x86_64.rpm`
    - `util-linux-lang-2.16-6.11.1.x86_64.rpm`
    - `uuid-runtime-2.16-6.11.1.x86_64.rpm`

  Sentinel Log Manager 1.1.0.*x* utilizza la versione 3.4-35.1 di Squashfs, mentre SLES 11 SP1 supporta Squashfs 4.0 e versioni successive, che non sono compatibili con le versioni precedenti e non consentono di aprire un file system compresso creato utilizzando tali versioni. Grazie all'installazione di questi RPM, viene risolto il problema relativo all'incompatibilità tra le versioni Squashfs di Sentinel Log Manager 1.1.0.*x* e quelle di SLES 11 SP1.

Questi RPM sono disponibili nel canale di aggiornamento online di SLES 11. Per ulteriori informazioni sull'aggiornamento del sistema SLES, vedere "YaST Online Update (Aggiornamento online di YaST)" (http://www.novell.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html) nella *SLES 11 SP1 Administration Guide (Guida all'amministrazione di SLES 11 SP1) (http://www.novell.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html)*.

Nota: la procedura di installazione si blocca fino a quando non vengono installati gli RPM e le patch kernel e Linux sopra specificate.

- Se si desidera eseguire l'upgrade di Sentinel Log Manager versioni 1.1.*x*, è necessario prima di tutto eseguire l'upgrade a Sentinel Log Manager 1.2.0.1 e quindi installare Sentinel Log Manager 1.2.0.2.
- Assicurarsi che non siano utilizzati collegamenti simbolici per le cartelle e sottocartelle seguenti:
  - `opt/novell` (cartella di base)
  - `etc/opt/novell` (cartella di configurazione)
  - `var/opt/novell` (cartella di dati)

  Nell'eventualità siano stati utilizzati, rimuovere i collegamenti simbolici. ovvero, riportare queste directory alle directory di installazione standard.

5.2 Esecuzione dell'upgrade del server di Sentinel Log Manager

1. Eseguire un backup della configurazione, quindi creare un'esportazione ESM.

   Per ulteriori informazioni sull'esecuzione del backup dei dati, vedere "Backup e ripristino dati."
2. Effettuare il download della patch più recente dal sito dei download di Novell (http://download.novell.com).
3. (Condizionale) Se si desidera eseguire l'upgrade alla correzione Hotfix 1 di Sentinel Log Manager, effettuare il download della patch dal sito di ricerca delle patch di Novell (http://download.novell.com/patch/finder/).
4. Effettuare il login come `root` al server in cui si desidera installare Sentinel Log Manager.
5. 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/bin # ./server.sh stop`.
6. 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.
7. Passare alla directory in cui è stato estratto il file d'installazione.
8. Specificare il comando seguente per eseguire lo script `install-slm` ed effettuare l'upgrade a Sentinel Log Manager:

   ```
   ./install-slm
   ```
9. Per continuare impostando una lingua desiderata, selezionare il numero visualizzato accanto alla lingua.

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

10 Leggere il contratto di licenza con l'utente finale, immettere `sì` o `s` per accettarlo, quindi continuare con il processo di installazione.

11 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.

Se si sta eseguendo l'upgrade di un sistema Sentinel Log Manager 1.1 sul quale è stato eseguito un upgrade da Sentinel Log Manager 1.0, l'installazione esistente di Sentinel Log Manager 1.0 viene lasciata intatta, con le eccezioni seguenti:

- Se la directory dati (ad esempio, `/opt/novell/sentinel_log_manager_1.0_x86-64/data`) e quella 1.1 (ad esempio, `/var/opt/novell/sentinel_log_mgr/data`) risiedono nello stesso file system, le sottodirectory `<1.0>/data/eventdata` e `<1.0>/data/rawdata` vengono spostate nell'ubicazione 1.1 in quanto, generalmente, le directory eventdata e rawdata sono 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 mentre i file della versione 1.0 vengono lasciati intatti.
- Se la directory dati 1.0 esistente, come `/opt/novell/sentinel_log_mgr_1.0_x86-64`, risiede su un file system montato separatamente e sul file system contenente la directory dati 1.1 (`/var/opt/novell/sentinel_log_mgr/data`) non vi è sufficiente spazio libero, è possibile fare in modo che il programma di installazione monti nuovamente il file system dall'ubicazione 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.

Una volta completata l'installazione di Sentinel Log Manager 1.2.0.2 e con il server già in funzione, 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_x86-64
```

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

12 Specificare il comando seguente per avviare il server di Sentinel Log Manager:

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

13 Assicurarsi che sia stato eseguito l'upgrade di tutte le Gestioni servizi di raccolta a una versione compatibile con il server di Sentinel Log Manager su cui è stato eseguito l'upgrade.

Per ulteriori informazioni sull'esecuzione dell'upgrade delle Gestioni servizi di raccolta, vedereSezione 5.3, “Esecuzione dell'upgrade della Gestione servizi di raccolta”, a pagina 54.

Nota: Dopo aver eseguito l'upgrade, la prima volta in cui viene avviato il sistema potrebbero essere necessari cinque minuti circa per la sua inizializzazione prima di poterlo utilizzare. Tale ritardo si verifica solo la prima volta in cui il sistema viene avviato dopo aver eseguito l'installazione o un upgrade.

5.3 Esecuzione dell'upgrade della Gestione servizi di raccolta

1. Eseguire un backup della configurazione e creare un'esportazione ESM.

   Per ulteriori informazioni, consultare "Backup e ripristino dati" nella *Guida all'amministrazione di Sentinel Log Manager 1.2.2)*.
2. Effettuare il login a Sentinel Log Manager come amministratore.
3. Selezionare *Servizio di raccolta* > *Avanzato*.

   Da questa pagina, è possibile scaricare il programma di installazione per l'upgrade più recente per la Gestione servizi di raccolta compatibile con Sentinel Log Manager.
4. Fare clic sul collegamento *Download del programma di installazione* nella sezione Programma di installazione 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.
5. Salvare il file.
6. Copiare il file in un'ubicazione temporanea.
7. Estrarre i contenuti del file `.zip`.
8. Eseguire uno degli script seguenti:
   - 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`.
9. Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo.

5.4 Esecuzione dell'upgrade dell'applicazione

È possibile eseguire l'upgrade dell'applicazione Sentinel Log Manager utilizzando WebYaST o SMT.

- Sezione 5.4.1, "Esecuzione dell'upgrade dell'applicazione mediante WebYast", a pagina 54
- Sezione 5.4.2, "Esecuzione dell'upgrade dell'applicazione mediante Zypper", a pagina 55
- Sezione 5.4.3, "Esecuzione dell'upgrade dell'applicazione mediante SMT", a pagina 56

5.4.1 Esecuzione dell'upgrade dell'applicazione mediante WebYast

---

Nota: se si esegue l'upgrade dell'applicazione Sentinel Log Manager installata in un sistema operativo precedente a SLES 11 SP3, è necessario effettuare questa operazione utilizzando l'utility da riga di comando Zypper, poiché la procedura di upgrade richiede l'interazione con l'utente. WebYaST non consente tale interazione con l'utente. Per informazioni sull'uso di Zypper per eseguire l'upgrade dell'applicazione, consultare Sezione 5.4.2, "Esecuzione dell'upgrade dell'applicazione mediante Zypper", a pagina 55.

---

1. Specificare l'URL di Sentinel Log Manager utilizzando la porta 4984 per avviare WebYaST.
2. Eseguire il login a WebYaST utilizzando le credenziali dell'applicazione.
3. Eseguire un backup della configurazione, quindi creare un'esportazione ESM.

   Per ulteriori informazioni sull'esecuzione del backup dei dati, vedere "Backup e ripristino dati."
4. (Condizionale) Se non è già stato fatto, registrare l'applicazione per l'esecuzione automatica degli aggiornamenti.

Per ulteriori informazioni, vedere Sezione 4.10, “Registrazione degli aggiornamenti”, a pagina 49.

Se l'applicazione non è registrata, in WebYaST viene visualizzato un avviso di colore giallo che segnala tale situazione.

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

Gli aggiornamenti disponibili vengono visualizzati.

6 Selezionare e applicare gli aggiornamenti.

Il completamento degli aggiornamenti potrebbe richiedere alcuni minuti. Una volta completato l'aggiornamento, viene visualizzata la pagina di login di WebYaST.

Prima di eseguire l'upgrade dell'applicazione, WebYaST interrompe automaticamente il servizio Sentinel Log Manager. Una volta completato l'upgrade, questo servizio deve essere riavviato manualmente.

7 Riavviare il server di Sentinel Log Manager mediante l'interfaccia utente Web.

Per ulteriori informazioni, vedere Sezione 4.9, “Interruzione e avvio dell'applicazione mediante l'interfaccia utente Web”, a pagina 48.

5.4.2 Esecuzione dell'upgrade dell'applicazione mediante Zypper

Per eseguire l'upgrade dell'applicazione mediante la patch Zypper:

1 Eseguire un backup della configurazione, quindi creare un'esportazione ESM.

Per ulteriori informazioni sull'esecuzione del backup dei dati, vedere “Backup e ripristino dati.”

2 (Condizionale) Se non è già stato fatto, registrare l'applicazione per l'esecuzione automatica degli aggiornamenti.

Per ulteriori informazioni, vedere Sezione 4.10, “Registrazione degli aggiornamenti”, a pagina 49.

Se l'applicazione non è registrata, in WebYaST viene visualizzato un avviso di colore giallo che segnala tale situazione.

3 Eseguire il login alla console dell'applicazione come utente `root`.

4 Eseguire il comando seguente:

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

5 (Condizionale) Se si esegue l'upgrade di una versione di Sentinel Log Manager precedente alla 1.2, viene visualizzato un messaggio che segnala un conflitto fra le versioni di Squashfs. Immettere `1` per eseguire l'upgrade a squashfs versione 4.0-1.2.10, quindi accettare la modifica apportata dal fornitore.

Sentinel Log Manager 1.1 utilizza la versione 3.4 di Squashfs, mentre Sentinel Log Manager 1.2 e le versioni successive utilizzano Squashfs versione 4.0. Inoltre, il fornitore di Squashfs yast2-live-installer è passato da OpenSUSE a SLES. Per continuare con l'upgrade, eseguire prima l'upgrade di squashfs, quindi accettare la modifica realizzata dal fornitore.

6 Immettere `Y` per continuare.

7 (Condizionale) Se si esegue l'upgrade di una versione di Sentinel Log Manager precedente alla 1.2, viene visualizzato il contratto di licenza con l'utente finale di Sentinel Log Manager. Per accettare la licenza, immettere `sì`.

Il contratto di licenza di Sentinel Log Manager 1.2 e versioni successive è diverso da quello di Sentinel Log Manager 1.1. Per eseguire l'upgrade da Sentinel Log Manager 1.1 e versioni successive alle versioni 1.2 e successive è necessario accettare il nuovo contratto di licenza.

8 (Condizionale) Se si esegue l'upgrade dell'applicazione Sentinel Log Manager installata in un sistema operativo precedente a SLES 11 SP3, viene visualizzato il contratto di licenza con l'utente finale. Per accettare la licenza, immettere `sì`.

   L'upgrade dell'applicazione Sentinel Log Manager viene eseguito correttamente.

9 (Condizionale) Se si esegue l'upgrade di una versione di Sentinel Log Manager precedente alla 1.2, al termine della procedura viene visualizzato un avviso di elemento obsoleto.

   Ciò avviene in quanto Sentinel Log Manager 1.2.0.1 utilizza WebYaST 1.1 ma le versioni di Sentinel Log Manager 1.1 utilizzano WebYaST 1.0. Durante l'esecuzione dell'upgrade, in WebYaST 1.1 il modulo della lingua di WebYaST 1.0 viene dichiarato obsoleto. In ogni caso, tale avviso non ha alcuna influenza sull'upgrade.

10 Riavviare l'applicazione Sentinel Log Manager.

5.4.3 Esecuzione dell'upgrade dell'applicazione mediante SMT

Negli ambienti protetti in cui l'applicazione deve essere eseguita senza un accesso diretto a Internet, è necessario configurare l'applicazione con Subscription Management Tool (SMT), mediante il quale è possibile eseguire l'upgrade dell'applicazione alle versioni più recenti disponibili.

1 Assicurarsi che l'applicazione sia configurata con SMT.

   Per ulteriori informazioni, vedere il Sezione 4.8, “Configurazione dell'applicazione con SMT”, a pagina 47.

2 Eseguire il login alla console dell'applicazione come utente `root`.

3 Aggiornare l'archivio per l'upgrade:

```
zypper ref -s
```

4 Verificare che l'applicazione sia abilitata per l'esecuzione degli upgrade:

```
zypper lr
```

5 (Facoltativo) Verificare se vi sono aggiornamenti disponibili per l'applicazione:

```
zypper lu
```

6 (Facoltativo) Controllare i pacchetti in cui sono inclusi gli aggiornamenti disponibili per l'applicazione:

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

7 Aggiornare l'applicazione:

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

8 Riavviare l'applicazione.

```
rcsentinel_log_mgr restart
```

5.5 Esecuzione dell'upgrade dei plug-in di Sentinel

Spesso, sul sito Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) viene effettuato l'upload dei plug-in di Sentinel più recenti e aggiornati. Per disporre delle correzioni relative ai bug, degli aggiornamenti della documentazione e dei miglioramenti più recenti, effettuare il download della nuova versione del plug-in. Per ulteriori informazioni sull'installazione o esecuzione dell'upgrade di un plug-in, vedere la relativa documentazione.

6 Effettuare il login all'interfaccia Web

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 23.
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.

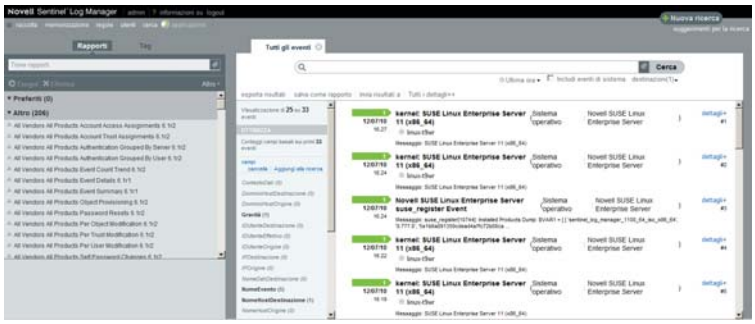


4. Specificare il nome utente e la password dell'amministratore di Sentinel Log Manager.
5. Selezionare la lingua dell'interfaccia di Sentinel Log Manager.

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.



7 Installazione di Gestioni servizi di raccolta aggiuntive

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 59
- Sezione 7.2, “Vantaggi apportati dalla presenza di più Gestioni servizi di raccolta”, a pagina 60
- Sezione 7.3, “Installazione di Gestioni servizi di raccolta aggiuntive”, a pagina 60

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.
- Per installare la Gestione servizi di raccolta su RHEL 6, installare lo script e i pacchetti seguenti:
  - Installare lo script ksh:

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

  - Per eseguire il programma di installazione nella modalità Console, installare i pacchetti seguenti:
    - glibc-2.12-1.7.el6.i686
    - nss-softokn-freebl-3.12.7-1.1.el6.i686
  - Per eseguire il programma di installazione nella modalità GUI, installare i pacchetti seguenti:
    - glibc-2.12-1.7.el6.i686
    - libX11-1.3-2.el6.i686
    - libXau-1.0.5-1.el6.i686
    - libxcb-1.5-1.el6.i686
    - libXext-1.1-3.el6.i686
    - libXi-1.3-3.el6.i686
    - libXtst-1.0.99.2-3.el6.i686
    - nss-softokn-freebl-3.12.7-1.1.el6.i686

7.2 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:** 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/indirizzo IP del server di Sentinel Log Manager.
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.

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.

Vedere la linea seguente nel file `activemqusers.properties` :

```
collectormanager=<password>
```

dove `collectormanager` è il nome utente e il valore corrispondente è la password.

14 Quando richiesto, accettare il certificato in modo permanente.

15 Per terminare l'installazione, premere *Fine*.

16 Riavviare il computer.

Se la Gestione servizi di raccolta è in esecuzione su Windows 2008 e dopo il riavvio vi sono delle eccezioni registrate nel file `collector_manager0.0.log`, consultare Sezione A.4, “La Gestione servizi di raccolta remota genera un'eccezione in Windows 2008 quando è abilitato UAC”, a pagina 69 per risolvere questo problema.

8 Disinstallazione

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 63
- Sezione 8.2, “Disinstallazione di Sentinel Log Manager”, a pagina 63
- Sezione 8.3, “Disinstallazione di Gestione servizi di raccolta”, a pagina 64

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 “Backup e ripristino dati” nella *Guida all'amministrazione di Sentinel Log Manager 1.2.2)*.

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 di Sentinel Log Manager

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 64
- Sezione 8.3.2, “Disinstallazione della Gestione servizi di raccolta su Windows”, a pagina 64
- Sezione 8.3.3, “Pulizia manuale delle directory”, a pagina 65

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/_uninst
   ```
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%\_uninst
   ```
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 65
- "Windows" a pagina 65

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`.

A Risoluzione dei problemi relativi all'installazione

In questa sezione vengono descritti alcuni dei problemi che potrebbero verificarsi durante l'installazione insieme alle relative procedure di risoluzione.

- Sezione A.1, “L'upgrade di Sentinel Log Manager ha esito negativo se la password dbauser non corrisponde a quella memorizzata nel file .pgpass”, a pagina 67
- Sezione A.2, “Installazione non riuscita a causa di una configurazione della rete non corretta”, a pagina 68
- Sezione A.3, “Problema di configurazione della rete con VMware Player 3 in SLES 11”, a pagina 68
- Sezione A.4, “La Gestione servizi di raccolta remota genera un'eccezione in Windows 2008 quando è abilitato UAC”, a pagina 69
- Sezione A.5, “Esecuzione dell'upgrade di Gestione log installata come utente non root diverso dall'utente novell”, a pagina 70
- Sezione A.6, “UUID non dispone di Gestioni servizi di raccolta create mediante immagine”, a pagina 70

A.1 L'upgrade di Sentinel Log Manager ha esito negativo se la password dbauser non corrisponde a quella memorizzata nel file .pgpass

Problema:

Quando si esegue l'upgrade di Sentinel Log Manager, l'upgrade del database ha esito negativo se la password dbauser non corrisponde a quella memorizzata nel file `.pgpass`.

Il comportamento differisce a seconda del metodo di installazione utilizzato:

Programma di installazione standard: la procedura di upgrade si blocca e viene visualizzato un messaggio che indica la causa dell'errore e la soluzione.

Console dell'applicazione: viene visualizzato il messaggio di errore seguente:

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

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

WebYaST: WebYaST continua a indicare che è disponibile un aggiornamento. Per individuare la causa effettiva di questo errore è possibile controllare il file `/var/opt/novell/sentinel_log_mgr/log/install.log`.

Soluzione:

Aggiornare la password nel file `.pgpass` utilizzando la password dbauser attuale e continuare la procedura di upgrade. Per informazioni sul file `.pgpass`, vedere la documentazione di PostgreSQL.

Se si esegue l'upgrade mediante la console dell'applicazione, eseguire una delle operazioni seguenti:

- Immettere `a` per interrompere l'installazione, aggiornare la password nel file `/home/novell/.pgpass` ed eseguire la `patch Zypper` per continuare l'upgrade.
- Aprire un'altra console e aggiornare la password nel file `/home/novell/.pgpass`. Nella console dell'upgrade immettere `r` per continuare la procedura di upgrade.
- Immettere `i` per ignorare il messaggio di errore e continuare l'installazione. Al termine dell'upgrade, aggiornare la password nel file `/home/novell/.pgpass` ed eseguire la `patch Zypper` nella console per completare la procedura di upgrade.

Se si esegue l'upgrade mediante WebYaST:

1. Eseguire il login alla console dell'applicazione.
2. Aggiornare la password dbauser nel file `/home/novell/.pgpass`.
3. In WebYaST, fare clic su *Aggiorna tutto* per continuare la procedura di upgrade.

   Al termine dell'upgrade, in WebYaST viene visualizzato il messaggio `Il sistema è aggiornato`.

A.2 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 è necessario configurare correttamente le impostazioni di rete in modo che il sistema disponga di indirizzo IP e nome host validi.

A.3 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 MAC copiato in Passo 2.
6. Salvare e chiudere il file.
7. Aprire la memoria virtuale in VMware Player.

A.4 La Gestione servizi di raccolta remota genera un'eccezione in Windows 2008 quando è abilitato UAC

Problema: Eseguire il login come un qualsiasi utente appartenente al gruppo di amministratori. Eseguire il comando `setup.bat` in un prompt del terminale per installare Gestione servizi di raccolta. Riavviare il sistema o avviare manualmente i servizi di Gestione servizi di raccolta, quindi eseguire il login con le stesse credenziali utente. Le eccezioni sono registrate nel file `collector_manager0.0.log` che incide sulle seguenti funzionalità di Gestione servizi di raccolta:

- Le mappature non vengono inizializzate.
- Non è possibile scegliere file di origine eventi nel file system del computer di Gestione servizi di raccolta (Win2008) mediante il connettore file.

Possibile causa: Gestione servizi di raccolta è stato installato in un sistema Windows 2008 SP1 standard edition a 64 bit. Di default, la funzione UAC (User Access Control, controllo accesso utente) presente nel computer è impostata su Abilitato.

Soluzione: Cambiare il proprietario dell'Accesso per i servizi di Sentinel 6.1 Rapid Deployment sostituendolo con l'utente corrente. Per default, come proprietario dell'Accesso è impostato l'Account di sistema locale. Per cambiare l'opzione di default:

1. Eseguire `services.msc` per aprire la finestra Servizi.
2. Fare clic con il pulsante destro del mouse su *Sentinel*, quindi selezionare *Proprietà*.
3. Nella finestra delle proprietà di Sentinel selezionate la scheda *Accesso*.
4. Selezionare *Account* e fornire le credenziali per l'utente corrente, utilizzato per installare Gestione servizi di raccolta.

   Nota: L'utente deve risiedere nel gruppo degli amministratori.

A.5 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 in `/etc/opt/novell/sentinel_log_mgr/config/esecuser.properties` in `novell`.

A.6 UUID non dispone di Gestioni servizi di raccolta create mediante immagine

Se viene creata un'immagine del server della Gestione servizi di raccolta (ad esempio, utilizzando ZenWorks Imaging) e le immagini vengono successivamente ripristinate su computer diversi, Sentinel Log Manager non identifica in modo univoco le nuove istanze della Gestione servizi di raccolta. Ciò si verifica a causa degli UUID duplicati.

È necessario generare l'UUID sui sistemi di Gestione servizi di raccolta che sono stati recentemente installati eseguendo le operazioni seguenti:

1. Eliminare il file `host.id` oppure `sentinel.id` che risiede nella cartella `/var/opt/novell/sentinel_log_mgr/data`.
2. Riavviare Gestione servizi di raccolta.

   La Gestione servizi di raccolta genera automaticamente l'UUID.

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.