Guida all'installazione e alla configurazione

NetIQ Sentinel 7.0.1

March 2012

Note legali

Per ulteriori informazioni, contattare NetIQ all'indirizzo:

1233 West Loop South, Houston, Texas 77027

U.S.A

www.netiq.com

Sommario

Informazioni sulla Guida

In questa guida viene fornita un'introduzione a NetIQ Sentinel insieme alle istruzioni relative alle procedure di installazione, migrazione e configurazione.

Destinatari

La presente guida è rivolta agli amministratori e ai consulenti di Sentinel.

Feedback

È possibile inviare i propri commenti e suggerimenti relativi a questa guida e agli altri documenti forniti con questo prodotto. Per inserire i commenti, utilizzare l'apposita funzione disponibile in fondo a ogni pagina della documentazione online.

Aggiornamenti della documentazione

Per la versione più recente della *Guida all'installazione e alla configurazione di NetIQ Sentinel 7.0.1*, visitare il sito Web della documentazione di Sentinel (http://www.novell.com/documentation/sentinel70).

Documentazione aggiuntiva

La documentazione tecnica di Sentinel è suddivisa in diversi volumi, ovvero:

- Guida introduttiva di Sentinel (http://www.novell.com/documentation/sentinel70/s70_overview/data/bookinfo.html)
- Guida rapida di Sentinel (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Sentinel Administration Guide (Guida all'amministrazione di Sentinel) (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Guida dell'utente di Sentinel (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Guida introduttiva di Collegamento Sentinel (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Eventi di revisione interni a Sentinel (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  Nel sito SDK di Sentinel vengono fornite informazioni relative alla creazione di plug-in specifici dei clienti.

Contattare Novell e NetIQ

Benché Sentinel adesso sia un prodotto NetIQ, Novell continua a gestire diverse funzioni di supporto.

- Sito Web di Novell (http://www.novell.com)
- Sito Web di NetIQ (http://www.netiq.com)
- Assistenza tecnica (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Supporto in autonomia (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Sito per il download delle patch (http://download.novell.com/index.jsp)
- Forum di supporto della comunità di Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- TID di Sentinel (http://support.novell.com/products/sentinel)
- Sito Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **Elenco delle notifiche via e-mail:** iscrizione tramite il sito Web dei plug-in di Sentinel

Contattare l'assistenza alle vendite

Per informazioni relative ai prodotti, ai prezzi e alle funzionalità, rivolgersi al rivenditore locale. Nell'eventualità ciò non sia possibile, contattare il team di assistenza alle vendite.

Sedi globali: Uffici NetIQ (http://www.netiq.com/about_netiq/officelocations.asp)

Stati Uniti e Canada: 888-323-6768

E-mail: info@netiq.com

Sito Web: www.netiq.com

Installazione

Per installare Sentinel, fare riferimento alle istruzioni seguenti:

1 Requisiti di sistema

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

1.1 Requisiti di sistema e piattaforme supportate

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

1.1.1 Sistemi operativi e piattaforme supportate

Il server Sentinel, Gestione servizi di raccolta e il motore di correlazione sono supportati sui sistemi operativi e sulle piattaforme seguenti:

Categoria	Requisito
Sistema operativo	Sentinel è supportato sui sistemi operativi seguenti: ◆ SUSE Linux Enterprise Server (SLES) 11 SP1 a 64 bit * ◆ Red Hat Enterprise Linux for Servers (RHEL) 6 a 64 bit * Sentinel 7 non è supportato nelle installazioni Open Enterprise Server di SLES.
Piattaforma virtuale	NetIQ fornisce delle applicazioni che consentono l'installazione di un server SLES 11 SP1 a 64 bit e di Sentinel sulle piattaforme virtuali seguenti: ◆ VMWare ESX 4.0 ◆ Xen 4.0
ISO DVD	NetIQ fornisce un file ISO DVD che consente l'installazione di SLES 11 SP1 a 64 bit e di Sentinel su: ◆ Hyper-V Server 2008 R2 ◆ Hardware senza sistema operativo installato

1.1.2 Requisiti hardware

Le istruzioni relative alla configurazione hardware suggerite possono variare in base alla singola implementazione. Quindi, prima di finalizzare l'architettura Sentinel, consultare i NetIQ Consulting Services o qualsiasi partner NetIQ Sentinel.

- "Server Sentinel" a pagina 12
- "Gestione servizi di raccolta" a pagina 13
- "Motore di correlazione" a pagina 14

Server Sentinel

In questa sezione è elencato l'hardware suggerito per un sistema di produzione che conservi i dati online per 90 giorni. Tali indicazioni si basano su una dimensione media presunta degli eventi di 600 byte. Le indicazioni per la memorizzazione locale e in rete includono un buffer del 20% oltre le stime di memorizzazione attuali. NetIQ suggerisce di creare un buffer per eventuali imprecisioni nelle stime o incremento del carico dei server nel corso del tempo.

Per eseguire il server Sentinel con tutti i componenti di Sentinel installati in un unico server, utilizzare il seguente hardware suggerito:

Categoria	100 EPS	2500 EPS	5000 EPS
CPU	Un Intel Xeon X5570 da 2,93 GHz (CPU a 4 core)	Due Intel Xeon X5470 3,33 GHz (CPU a 4 core, in totale: 8 core)	Due Intel Xeon X5470 3,33 GHz (CPU a 4 core, in totale: 8 core)
Memorizzazione locale (30 giorni)	2 unità da 256 GB a 7,2k RPM (hardware RAID 1 con 256 MB di cache)	8 unità da 1,2 TB a 7,2k RPM (hardware RAID 10 con 256 MB di cache)	16 unità da 1,2 TB a 15k RPM, (hardware RAID 10 con 512 MB di cache) o una SAN (Storage Area Network) equivalente
Memorizzazione in rete (90 giorni)	2x128 GB	4x1 TB	8x1 TB
Memoria	**Altre installazioni:** 4 GB **Installazione ISO DVD:** 4.5 GB	16 GB	24 GB

NOTE: Sentinel è supportato su processori Intel Xeon e AMD Opteron x86 a 64 bit ma non su processori a 64 bit puri come, ad esempio, Itanium.

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 1.1.5, “Stima relativa ai requisiti per la memorizzazione dei dati”, a pagina 16.
- 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 per l'esecuzione delle ricerche e la generazione dei rapporti. Qualora il costo della memorizzazione sia fattore di cui tenere specialmente considerazioni, è sempre possibile ridurre le dimensioni della memorizzazione locale. 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.
- 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, NetIQ consiglia di installare ulteriori istanze di Sentinel

Gestione servizi di raccolta

Per eseguire la Gestione servizi di raccolta su un sistema diverso da quello in cui è in esecuzione il server Sentinel in un ambiente di produzione, utilizzare i requisiti hardware seguenti:

Categoria	Minimo	Soluzione proposta
CPU	Intel Xeon L5240 da 3 GHz (2 core)	Un Intel Xeon X5570 da 2,93 GHz (CPU a 4 core)
Spazio su disco	10 GB (RAID 1)	20 GB (RAID 1)
Memoria	1.5 GB	4 GB
Frequenza stimata (EPS)	500	2000

Motore di correlazione

Per eseguire il motore di correlazione su un sistema diverso da quello in cui è in esecuzione il server Sentinel in un ambiente di produzione, utilizzare i requisiti di sistema seguenti:

Categoria	Minimo	Soluzione proposta
CPU	Intel Xeon L5240 da 3 GHz (2 core)	Un Intel Xeon X5570 da 2,93 GHz (CPU a 4 core)
Spazio su disco	10 GB (RAID non richiesto)	10 GB (RAID non richiesto)
Memoria	1.5 GB	4 GB
Frequenza stimata (EPS)	500	2500

1.1.3 Piattaforme database supportate

In Sentinel sono inclusi un sistema di memorizzazione basato su file incorporato e un database, che rappresentano tutto quanto è necessario per eseguire Sentinel. Tuttavia, se si desidera utilizzare la funzione di sincronizzazione dei dati facoltativa per copiare i dati in un archivio dati, Sentinel supporta l'utilizzo di Oracle versione 11g R2 o Microsoft SQL Server 2008 R2 come archivio dati.

1.1.4 Browser supportati

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

NOTE: Per caricare le applicazioni del client Sentinel nel modo più appropriato, è necessario che il plug-in Sun Java sia installato sul computer.

Piattaforma	Browser
Windows 7	◆ Firefox 5, 6, 7, 8, 9 e 10 ◆ Internet Explorer 8 e 9 * Per informazioni relative a Internet Explorer 8, vedere "Prerequisiti per Internet Explorer" a pagina 15.
SLES 11 SP1 e RHEL 6	◆ Firefox 5, 6, 7, 8, 9 e 10 Per ulteriori informazioni, vedere "Aggiornamento manuale della versione di Firefox" a pagina 15.

Prerequisiti per Internet Explorer

Se il livello di sicurezza per Internet è impostato su Alto, una volta effettuato il login a Sentinel viene visualizzata una pagina vuota e la finestra popup del download dei file potrebbe essere bloccata dal browser. Per risolvere questo problema, è necessario prima impostare il livello di sicurezza su Medio-alto, quindi modificare il livello Personalizzato nel modo seguente:

1. Andare a *Strumenti* > *Opzioni Internet* > *scheda Sicurezza* e impostare il livello di sicurezza su *Medio-alto*.
2. Assicurarsi che l'opzione *Strumenti* > *Visualizzazione Compatibilità* non sia selezionata.
3. Andare a *Strumenti* > *Opzioni Internet* > *scheda Sicurezza* > *Livello personalizzato...*, quindi scorrere fino alla sezione *Download* e selezionare *Attiva* nell'opzione *Richiesta di conferma automatica per il download di file*.

Aggiornamento manuale della versione di Firefox

Sentinel supporta Firefox dalla versione 5 alla 10; tuttavia il sistema SLES 11 SP1 viene fornito con Firefox versione 3.6*X*. Per aggiornare manualmente un'installazione di SLES 11 SP1 con una versione supportata di Firefox, eseguire la procedura seguente:

1. Aprire YaST.
2. Selezionare *Software* > *Software Repositories (Archivi software)* per visualizzare la finestra Configured Software Repositories (Archivi software configurati).
3. Fare clic su *Aggiungi* per aprire la finestra Tipo di supporto.
4. Selezionare l'opzione *Specify URL (Specifica URL)*, quindi fare clic su *Avanti*.

   Viene visualizzata la finestra Repository URL (URL archivio).
5. Immettere il collegamento Software Repository (Archivio software) (http://download.opensuse.org/repositories/mozilla/SLE_11/) nella casella di testo URL, quindi fare clic su *Avanti*.

   Il download dell'archivio software è stato completato.
6. Fare clic su *OK* per aggiornare l'archivio software.
7. Fare clic su *Software Management (Gestione software)* per aprire la finestra YaST2.
8. Immettere `Firefox` nella casella di testo *Cerca*.

   Vengono visualizzati i pacchetti di Firefox.
9. Selezionare i pacchetti necessari per la versione supportata di Firefox che si desidera installare.

Se si seleziona un pacchetto in conflitto con la versione esistente, viene visualizzata una finestra di avviso. Selezionare l'opzione appropriata, quindi fare clic sul pulsante *OK Try Again (Riprova)*.

10 Fare clic su *Accetta*.

1.1.5 Stima relativa ai requisiti per la memorizzazione dei dati

Sentinel 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 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 *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

Per determinare la quantità di spazio di memorizzazione ad accesso casuale necessario per Sentinel, 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 oppure in modalità remota sul protocollo Server Message Block (SMB) o CIFS, nel Network File System (NFS) oppure in una SAN per Sentinel

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 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 0.00008 = 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 0.00001 = 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 0.000003 = 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 è stata abilitata la memorizzazione in rete, generalmente i dati evento vi vengono copiati dopo due giorni. Per ulteriori informazioni, consultare "Configurazione della memorizzazione dei dati" nella *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

- **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

---

NOTE:

- 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.

1.1.6 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 .002 = dati scritti al secondo sul disco

  Ad esempio, a 500 EPS, per una dimensione media degli eventi pari a 758 byte e una dimensione media dei dati non elaborati pari a 490 byte nel file di log, i dati scritti sul disco vengono determinati nel modo seguente:

  (758 byte + 490 byte) x 500 EPS x .002 = ~1100 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 .00002 = richieste I/O al secondo per il disco

Ad esempio, a 500 EPS, per una dimensione media degli eventi pari a 758 byte e una dimensione media dei dati non elaborati pari a 490 byte nel file di log, il numero di richieste I/O al secondo per il disco viene determinato nel modo seguente:

(758 byte + 490 byte) x 500 EPS x .00002 = ~10 trasferimenti al secondo

- **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 .003 = blocchi scritti al secondo sul disco

  Ad esempio, a 500 EPS, per una dimensione media degli eventi pari a 758 byte e una dimensione media dei dati non elaborati pari a 490 byte nel file di log, il numero di blocchi scritti al secondo sul disco viene determinato nel modo seguente:

  (758 byte + 490 byte) x 500 EPS x .003 = ~1800 blocchi al secondo

- **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 .40 = kilobyte letti al secondo dal disco

  Ad esempio, a 5 milioni di eventi corrispondenti all'interrogazione della ricerca, per una dimensione media degli eventi pari a 758 byte e una dimensione media dei dati non elaborati pari a 490 byte nel file di log, il numero di dati letti al secondo sul disco viene determinato nel modo seguente:

  (758 byte + 490 byte) x 5 x .40 = ~500 KB

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

Utilizzare le seguenti formule per valutare l'utilizzo della larghezza di banda di rete tra il server Sentinel e la Gestione servizi di raccolta remota 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 758 byte e una dimensione media dei dati non elaborati pari a 490 byte nel file di log, l'utilizzo della larghezza di banda della rete viene determinato nel modo seguente:

(758 byte + 490 byte) x 500 EPS x .0003 = ~175 Kbps

1.1.8 Ambiente virtuale

Sentinel è stato ampiamente verificato ed è totalmente supportato in un server VMware ESX. Quando viene configurato un ambiente virtuale, le macchine virtuali devono disporre di almeno 2 CPU. Per ottenere prestazioni paragonabili ai risultati delle prove del computer fisico svolte su ESX o in qualsiasi altro ambiente virtuale, quest'ultimo deve disporre della stessa memoria, CPU, spazio su disco e I/O consigliati per il computer fisico.

Per ulteriori informazioni sui consigli relativi al computer fisico, consultare Sezione 1.1, “Requisiti di sistema e piattaforme supportate”, a pagina 11.

1.2 Requisiti di sistema relativi al connettore e al servizio di raccolta

Ogni connettore e servizio di raccolta dispone di un set specifico di requisiti di sistema e piattaforme supportate. Consultare la documentazione relativa ai connettori e ai servizi di raccolta sulla pagina Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

1.3 Porte utilizzate

1.3.1 Server Sentinel

Porte locali

Per la comunicazione interna con il database e altri processi interni, Sentinel utilizza le porte seguenti:

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, vedere il sito Web Sentinel dei plug-in SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).
TCP 27017	Utilizzata per il database di configurazione di Security Intelligence.
TCP 28017	Utilizzata per l'interfaccia Web del database Security Intelligence.
TCP 32000	Utilizzata per la comunicazione interna tra il processo del wrapper e quello del server.

Porte di rete

Per la comunicazione esterna con altri componenti, Sentinel utilizza porte diverse. Per consentire l'installazione delle applicazioni, le porte vengono aperte sul firewall per default. Tuttavia, in un'installazione di tipo standard, per aprire le porte sul firewall è necessario configurare il sistema operativo sul quale si sta eseguendo l'installazione di Sentinel.

Per un funzionamento ottimale di Sentinel, assicurarsi che le porte seguenti siano aperte sul firewall:

Porte	Descrizione
TCP 1099 e 2000	Vengono utilizzate congiuntamente dagli strumenti di monitoraggio per connettersi al processo del server Sentinel mediante Java Management Extensions (JMX).
TCP 1289	Utilizzata per le connessioni di Audit.
UDP 1514	Utilizzata per i messaggi syslog.
TCP 8443	Utilizzata per la comunicazione HTTPS.
TCP 1443	Utilizzata per i messaggi syslog cifrati mediante il protocollo SSL.
TCP 61616	Utilizzata per la comunicazione tra le Gestioni servizi di raccolta e il server.
TCP 10013	Utilizzata da Sentinel Control Center e Solution Designer.
TCP 1468	Utilizzata per i messaggi syslog.
TCP 10014	Utilizzata dalle Gestioni servizi di raccolta remote per connettersi al server mediante il proxy SSL. Tale procedura, tuttavia, non è comune. Infatti, per connettersi al server le Gestioni servizi di raccolta remote utilizzano la porta SSL 61616 per default.

Porte specifiche per l'applicazione server Sentinel

In aggiunta a quelle riportate sopra, nell'applicazione server Sentinel vengono aperte anche le porte seguenti.

Porte	Descrizione
TCP 22	Utilizzata per l'accesso shell sicuro a Sentinel Appliance.
TCP 54984	Utilizzata dalla console di gestione dell'applicazione Sentinel (WebYaST). Utilizzata anche dall'applicazione Sentinel per il servizio di aggiornamento.
TCP 289	Inoltrata a 1289 per le connessioni Audit.
UDP 443	Inoltrata alla 8443 per la comunicazione HTTPS.
UDP 514	Inoltrata a 1514 per i messaggi.
TCP 1290	È la porta di Collegamento Sentinel cui è consentito connettersi attraverso il firewall SuSE.
UDP e TCP 40000 - 41000	Sono le porte che possono essere utilizzate durante la configurazione dei server per i servizi di raccolta dei dati, come syslog. Per default, Sentinel non è in ascolto su queste porte.

1.3.2 Gestione servizi di raccolta

Porte di rete

Per il funzionamento ottimale di Gestione servizi di raccolta di Sentinel, assicurarsi che le porte seguenti siano aperte sul firewall:

Porte	Descrizione
TCP 1289	Utilizzata per le connessioni di Audit.
UDP 1514	Utilizzata per i messaggi syslog.
TCP 1443	Utilizzata per i messaggi syslog cifrati mediante il protocollo SSL.
TCP 1468	Utilizzata per i messaggi syslog.
TCP 1099 e 2000	Vengono utilizzate congiuntamente dagli strumenti di monitoraggio per connettersi al processo del server Sentinel mediante Java Management Extensions (JMX).

Porte specifiche per l'applicazione Gestione servizi di raccolta

In aggiunta a quelle riportate sopra, nell'applicazione Gestione servizi di raccolta di Sentinel vengono aperte anche le porte seguenti.

Porte	Descrizione
TCP 22	Utilizzata per l'accesso shell sicuro a Sentinel Appliance.
TCP 54984	Utilizzata dalla console di gestione dell'applicazione Sentinel (WebYaST). Utilizzata anche dall'applicazione Sentinel per il servizio di aggiornamento.
TCP 289	Inoltrata a 1289 per le connessioni Audit.
UDP 514	Inoltrata a 1514 per i messaggi.
TCP 1290	È la porta di Collegamento Sentinel cui è consentito connettersi attraverso il firewall SuSE.
UDP e TCP 40000 - 41000	Sono le porte che possono essere utilizzate durante la configurazione dei server per i servizi di raccolta dei dati, come syslog. Per default, Sentinel non è in ascolto su queste porte.

1.3.3 Motore di correlazione

Porte di rete

Per un funzionamento ottimale del motore di correlazione di Sentinel, assicurarsi che le porte seguenti siano aperte sul firewall:

Porte	Descrizione
TCP 1099 e 2000	Vengono utilizzate congiuntamente dagli strumenti di monitoraggio per connettersi al processo del server Sentinel mediante Java Management Extensions (JMX).

Porte specifiche per l'applicazione Motore di correlazione

In aggiunta a quelle riportate sopra, nell'applicazione Motore di correlazione di Sentinel vengono aperte anche le porte seguenti.

Porte	Descrizione
TCP 22	Utilizzata per l'accesso shell sicuro a Sentinel Appliance.
TCP 54984	Utilizzata dalla console di gestione dell'applicazione Sentinel (WebYaST). Utilizzata anche dall'applicazione Sentinel per il servizio di aggiornamento.

2 Installazione di Sentinel

Sentinel può essere installato in modalità autonoma oppure come applicazione. Il programma di installazione per la modalità autonoma installa Sentinel su un sistema operativo SUSE Linux Enterprise Server (SLES) 11 SP1 o Red Hat Enterprise Linux (RHEL) 6 esistente. Il programma di installazione per la modalità applicazione, invece, installa sia il sistema operativo SLES 11 SP1 a 64 bit che Sentinel.

Questa sezione descrive la procedura per eseguire un'installazione in modalità autonoma del server Sentinel su un sistema SLES 11 SP1 o RHEL 6 esistente. Per la procedura di installazione in modalità applicazione, vedere Capitolo 5, “Installazione dell'applicazione”, a pagina 41.

2.1 Metodi di installazione

Per l'installazione in modalità autonoma, sono disponibili i metodi seguenti:

- **Interattivo:** l'installazione procede mediante gli input dell'utente. Durante l'installazione è possibile registrare le opzioni di installazione (input utente o valori di default) in un file che, in un secondo momento, potrà essere utilizzato per un'installazione in modalità automatica.
- **Modalità automatica:** è possibile utilizzare questa opzione nell'eventualità che le opzioni di installazione siano preregistrate. L'installazione in modalità automatica fa riferimento al file in cui risiedono gli input di installazione registrati ed elabora l'installazione utilizzando i valori catturati in tale file. L'installazione in modalità automatica è particolarmente efficace quando si desidera installare diverse repliche della stessa configurazione nell'ambiente. Per ulteriori informazioni, consultare il Sezione 2.5, “Installazione invisibile all'utente”, a pagina 29.

L'installazione interattiva e quella in modalità automatica di Sentinel possono essere eseguite come utente `root` o non root.

2.1.1 Installazione standard e personalizzata

Durante l'installazione di Sentinel, sono disponibili le modalità di configurazione seguenti:

- **Standard:** in questa modalità, per impostare la configurazione il processo di installazione utilizza i valori di default. L'input dell'utente è richiesto solo per la password. Per ulteriori informazioni sull'installazione di Sentinel mediante la configurazione standard, vedere Sezione 2.4.1, “Configurazione standard”, a pagina 26.
- **Personalizzato:** in questa modalità, la procedura di installazione richiede all'utente di specificare i valori desiderati per la configurazione. È possibile selezionare i valori di default oppure specificare quelli necessari. Per ulteriori informazioni sull'installazione di Sentinel mediante la configurazione personalizzata, vedere Sezione 2.4.2, “Configurazione personalizzata”, a pagina 28.

Configurazione standard	Configurazione personalizzata
L'installazione viene eseguita con una chiave di valutazione di 90 giorni di default.	Consente di eseguire l'installazione utilizzando la chiave di licenza di 90 giorni o una chiave di licenza valida.
Consente di specificare la password admin e utilizza la password di default sia per dbauser che per appuser.	Consente di specificare la password admin. Per dbauser e appuser, è possibile specificare una password nuova oppure utilizzare quella password.
Vengono installate le porte di default per tutti i componenti.	Consente di specificare le porte per i vari componenti.
Autentica utenti con il database interno.	Fornisce l'opzione per autenticare gli utenti con il database interno o mediante autenticazione LDAP.

2.1.2 Componenti installati

Sentinel è dotato di diversi componenti. Tutti i componenti seguenti sono installati per default:

- Server Sentinel
- Motore di correlazione
- Gestione servizi di raccolta

Su sistemi diversi, è possibile installare ulteriori motori di correlazione e Gestioni servizi di raccolta.

2.2 Istruzioni preliminari

Prima di avviare l'installazione, verificare di aver completato i task seguenti:

- Verificare che hardware e software soddisfino i requisiti di sistema elencati in Sezione 1.1, “Requisiti di sistema e piattaforme supportate”, a pagina 11.
- Se era presente un'installazione precedente di Sentinel, assicurarsi che non siano rimasti file o impostazioni di sistema di tale versione. Per ulteriori informazioni, vedere Parte V, “Disinstallazione,” a pagina 101.

- Per prestazioni, stabilità e affidabilità ottimali del server Sentinel, utilizzare il file system ext3 su SLES e quello ext4 su RHEL. Per ulteriori informazioni sui file system, vedere Overview of File Systems in Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) in *Storage Administration Guide* (in lingua inglese).
- Configurare le impostazioni di rete per verificare che il sistema disponga di un indirizzo IP e un nome host validi.
- Se si intende 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).
- Assicurarsi che le porte elencate in Sezione 1.3, “Porte utilizzate”, a pagina 19 siano aperte sul firewall.
- Per prestazioni ottimali, le impostazioni di memoria devono essere quelle appropriate per il database PostgreSQL:

  Il parametro SHMMAX deve essere maggiore o uguale a 1073741824. Per impostare il valore appropriato, aggiungere le informazioni seguenti al file `/etc/sysctl.conf`:

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```

- Per un'installazione minima o di tipo headless, il sistema operativo del server Sentinel deve includere almeno il server di base e i componenti del server SLES o del server RHEL 6. Per Sentinel sono necessarie le versioni a 64 bit dei seguenti RPM:
  - bash
  - bc
  - coreutils
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof
  - net-tools
  - openssl
  - python-libs
  - sed
  - zlib

2.3 Opzioni di installazione

`./install-sentinel --help` consente di visualizzare le opzioni seguenti:

Opzioni	Valore	Descrizione
--location	Directory	Specifica una directory diversa da quella radice (/) per installare Sentinel.
-m, --manifest	Nome file	Specifica un file manifesto del prodotto da utilizzare al posto del file manifesto di default.
--no-configure		Specifica di non eseguire la configurazione del prodotto una volta eseguita l'installazione.
-n, --no-start		Specifica di non avviare o riavviare Sentinel dopo l'installazione o la configurazione.
-r, --recordunattended	Nome file	Specifica un file per registrare i parametri che possono essere utilizzati per l'installazione in modalità automatica.
-u, --unattended	Nome file	Utilizza i parametri presenti nel file specificato per eseguire l'installazione su sistemi automatici.
-h, --help		Visualizza le opzioni che possono essere utilizzate durante l'installazione di Sentinel.
-l, --log-file	Nome file	Registra i messaggi del log in un file.
--no-banner		Sopprime la visualizzazione dei messaggi di intestazione.
-q, --quiet		Visualizza un numero inferiore di messaggi.
-v, --verbose		Visualizza tutti i messaggi durante l'installazione.

2.4 Installazione interattiva

- Sezione 2.4.1, “Configurazione standard”, a pagina 26
- Sezione 2.4.2, “Configurazione personalizzata”, a pagina 28

2.4.1 Configurazione standard

1. Scaricare il file di installazione di Sentinel dalla pagina Web dei download di Novell (http://download.novell.com/index.jsp).
   - **1a** Nel campo *Product or Technology* (Prodotto o tecnologia) sfogliare e selezionare *SIEM-Sentinel*.
   - **1b** Fare clic su *Cerca*.
   - **1c** Fare clic sul pulsante nella colonna *Download* in corrispondenza di *Sentinel 7.0 Evaluation*.
   - **1d** Fare clic su *proceed to download* (procedi con il download), quindi specificare il nome e la password cliente.
   - **1e** Fare clic su *download* per la versione di installazione compatibile con la piattaforma in uso.
2. Per estrarre il file di installazione, specificare il comando seguente nella riga di comando.

   ```
   tar zxvf <install_filename>
   ```

   Sostituire *<nomefile_installazione>* con il nome attuale del file di installazione.
3. Passare alla directory in cui è stato estratto il programma di installazione:

```
cd sentinel_server-7.0.0.0.x86_64
```

4. Per installare Sentinel, specificare il comando seguente:

   ```
   ./install-sentinel
   ```

   oppure

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

   ```
   ./install-sentinel -r <response_filename>
   ```

5. Specificare il numero corrispondente alla lingua che si desidera utilizzare per l'installazione, quindi premere Invio.

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

6. Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.

7. Immettere `yes` o `y` per accettare la licenza e continuare con l'installazione.

   Il processo di installazione potrebbe richiedere alcuni secondi per effettuare l'upload dei pacchetti di installazione e richiedere il tipo di configurazione che si desidera utilizzare.

8. Quando richiesto, specificare `1` per continuare con la configurazione di tipo standard.

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

9. Specificare la password per l'utente amministratore `admin`.

10. Confermare nuovamente la password.

    Questa password viene utilizzata da `admin`, `dbauser` e `appuser`.

    Viene completata l'installazione di Sentinel e il server viene avviato. Una volta eseguita l'installazione, l'avvio di tutti i servizi potrebbe richiedere alcuni minuti in quanto il sistema esegue una sola inizializzazione. Prima di effettuare il login al server, attendere il completamento dell'installazione.

Per accedere all'interfaccia Web di Sentinel, specificare l'URL seguente nel browser Web:

`https://<IP_Address_Sentinel_server>:8443.`

<*Indirizzo_IP_server_Sentinel*> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

2.4.2 Configurazione personalizzata

Se si sta installando Sentinel con una configurazione personalizzata, è possibile specificare la chiave di licenza, modificare la password per utenti diversi e specificare i valori relativi alle differenti porte che devono essere utilizzate per interagire con i componenti interni.

1. Scaricare il file di installazione di Sentinel dalla pagina Web dei download di Novell (http://download.novell.com/index.jsp).
   - **1a** Nel campo *Product or Technology* (Prodotto o tecnologia) sfogliare e selezionare *SIEM-Sentinel*.
   - **1b** Fare clic su *Cerca*.
   - **1c** Fare clic sul pulsante nella colonna *Download* in corrispondenza di *Sentinel 7.0 Evaluation*.
   - **1d** Fare clic su *proceed to download* (procedi con il download), quindi specificare il nome e la password cliente.
   - **1e** Fare clic su *download* per la versione di installazione compatibile con la piattaforma in uso.
2. Per estrarre il file di installazione, specificare il comando seguente nella riga di comando.

   ```
   tar zxvf <install_filename>
   ```

   Sostituire <*nomefile_installazione*> con il nome attuale del file di installazione.
3. Per installare Sentinel, specificare il comando seguente nella radice della directory estratta:

   ```
   ./install-sentinel
   ```

   oppure

   Se si desidera utilizzare questa configurazione personalizzata per installare Sentinel su più sistemi, è possibile registrare le opzioni specifiche su un file. È possibile utilizzare questo file per eseguire un'installazione automatica di Sentinel su altri sistemi. Per la registrazione delle opzioni di installazione, specificare il comando seguente:

   ```
   ./install-sentinel -r <response_filename>
   ```
4. Specificare il numero corrispondente alla lingua che si desidera utilizzare per l'installazione, quindi premere Invio.

   Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.
5. Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.
6. Immettere `yes` o `y` per accettare il contratto di licenza e continuare l'installazione.

   Il processo di installazione potrebbe richiedere alcuni secondi per effettuare l'upload dei pacchetti di installazione e richiedere il tipo di configurazione che si desidera utilizzare.
7. Specificare `2` per elaborare una configurazione personalizzata di Sentinel.
8. Immettere `1` per utilizzare la chiave di licenza di valutazione di 90 giorni di default.

   oppure

   Immettere `2` per inserire una chiave di licenza di Sentinel acquistata.
9. Specificare la password dell'utente amministratore `admin` e confermarla nuovamente.
10. Specificare la password per l'utente del database `dbauser` e confermarla nuovamente.

    L'account `dbauser` rappresenta l'identità che Sentinel utilizza per interagire con il database. La password immessa in questa posizione può essere utilizzata per elaborare i task di manutenzione del database, incluso il ripristino della password admin qualora sia stata dimenticata o persa.

11 Specificare la password per l'utente dell'applicazione `appuser` e confermarla nuovamente.

12 Modificare le assegnazioni delle porte per i servizi di Sentinel immettendo il numero desiderato della porta e, successivamente, specificando quello nuovo.

13 Una volta modificate le porte, specificare 7 per confermare il completamento.

14 Immettere `1` per autenticare gli utenti utilizzando solo il database interno.

oppure

Se nel dominio è stata configurata una directory LDAP, immettere `2` per autenticare gli utenti utilizzando l'autenticazione di tale directory.

Il valore di default è `1`.

Viene completata l'installazione di Sentinel e il server viene avviato. Una volta eseguita l'installazione, l'avvio di tutti i servizi potrebbe richiedere alcuni minuti in quanto il sistema esegue una sola inizializzazione. Prima di effettuare il login al server, attendere il completamento dell'installazione.

Per accedere all'interfaccia Web di Sentinel, specificare l'URL seguente nel browser Web:

`https://<IP_Address_Sentinel_server>:8443.`

<*Indirizzo_IP_server_Sentinel*> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

2.5 Installazione invisibile all'utente

L'installazione automatica di Sentinel può risultare particolarmente utile se è necessario installare più server Sentinel nella propria installazione. In uno scenario di questo tipo è possibile registrare i parametri di installazione durante l'esecuzione dell'installazione interattiva e, successivamente, eseguire il file registrato su tutti gli altri server. In una configurazione standard o personalizzata, i parametri di installazione possono essere registrati durante l'elaborazione dell'installazione di Sentinel.

Per eseguire un'installazione in modalità automatica, assicurarsi di aver registrato i parametri di installazione in un file. Per ulteriori informazioni sulla creazione del file di risposta, fare riferimento a Sezione 2.4.1, “Configurazione standard”, a pagina 26 o Sezione 2.4.2, “Configurazione personalizzata”, a pagina 28.

1 Effettuare il download dei file di installazione dalla pagina Web dei download di Novell (http://download.novell.com/index.jsp).

2 Effettuare il login come utente `root` al server in cui si desidera installare Sentinel.

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

```
tar -zxvf <install_filename>
```

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

4 Per installare Sentinel in modalità automatica, specificare il comando seguente:

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

L'installazione continua con i valori memorizzati nel file di risposta.

Viene completata l'installazione di Sentinel e il server viene avviato. Una volta eseguita l'installazione, l'avvio di tutti i servizi potrebbe richiedere alcuni minuti in quanto il sistema esegue una sola inizializzazione. Prima di effettuare il login al server, attendere il completamento dell'installazione.

Per accedere all'interfaccia Web di Sentinel, specificare l'URL seguente nel browser Web:

`https://<IP_Address_Sentinel_server>:8443.`

<*Indirizzo_IP_server_Sentinel*> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

2.6 Installazione di Sentinel come utente non root

Se per motivi di norme aziendali non è possibile eseguire l'installazione completa di Sentinel come utente `root`, l'installazione può essere realizzata come un utente di diverso tipo. In questo tipo di installazione, alcuni passaggi vengono elaborati come utente `root` ma, successivamente, l'installazione di Sentinel viene proseguita come un altro tipo di utente creato dall'utente `root`. L'utente `root`, alla fine, completa l'installazione.

1. Effettuare il download dei file di installazione dalla pagina Web dei download di Novell (http://download.novell.com/index.jsp)
2. Nella riga di comando, specificare il comando seguente per estrarre i file di installazione dal file tar:

   `tar -zxvf <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 come utente `root`.
4. Immettere il comando seguente:

   `./bin/root_install_prepare`

   Viene visualizzato un elenco dei comandi da eseguire con i privilegi di utente root. Se si desidera che un utente non root esegua l'installazione di Sentinel in un'ubicazione diversa da quella di default, specificare l'opzione --location insieme al comando. Ad esempio:

   `./bin/root_install_prepare --location=/foo`

   Il valore impostato per l'opzione `--location foo` è posto all'inizio dei percorsi delle directory.

   Se non sono già presenti, l'installazione crea un gruppo `novell` e un utente `novell`.
5. Accettare l'elenco dei comandi.

   Vengono eseguiti i comandi visualizzati.
6. Specificare il comando seguente per modificare l'utente `novell` non root appena creato: `novell`:

   `su novell`
7. (Condizionale) Per eseguire un'installazione interattiva:

   7a Immettere il comando seguente:

   `./install-sentinel`

   Per installare Sentinel in un'ubicazione diversa da quella di default, specificare l'opzione --location insieme al comando. Ad esempio:.

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

   7b Continuare con la Passo 9.
8. (Condizionale) Per eseguire un'installazione in modalità automatica:

   8a Immettere il comando seguente:

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

L'installazione continua con i valori memorizzati nel file di risposta.

8b Continuare con la Passo 12.

9 Immettere il numero relativo alla lingua che si desidera utilizzare per l'installazione.

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 la configurazione standard, continuare con Passo 8 mediante Passo 10 in Sezione 2.4.1, “Configurazione standard”, a pagina 26.
- Se si sceglie di procedere con la configurazione personalizzata, continuare con Passo 7 mediante Passo 14 in Sezione 2.4.2, “Configurazione personalizzata”, a pagina 28.

12 Effettuare il login come utente `root` e immettere il comando seguente per completare il processo di installazione:

```
./bin/root_install_finish
```

Viene completata l'installazione di Sentinel e il server viene avviato. Una volta eseguita l'installazione, l'avvio di tutti i servizi potrebbe richiedere alcuni minuti in quanto il sistema esegue una sola inizializzazione. Prima di effettuare il login al server, attendere il completamento dell'installazione.

Per accedere all'interfaccia Web di Sentinel, specificare l'URL seguente nel browser Web:

`https://<IP_Address_Sentinel_server>:8443.`

<*Indirizzo_IP_server_Sentinel*> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

2.7 Modificare la configurazione dopo l'installazione

Una volta completata l'installazione di Sentinel, è possibile immettere una chiave di licenza valida, cambiare la password o modificare una qualsiasi delle porte assegnate eseguendo lo script `configure.sh`. Lo script si trova nella cartella `\opt\novell\sentinel\setup`.

1 Per eseguire lo script `configure.sh`, immettere il comando seguente nella riga di comando:

```
./configure.sh
```

2 Immettere `1` per eseguire una configurazione di Sentinel standard oppure `2` per eseguirne una personalizzata.

3 Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.

4 Immettere `yes` o `y` per accettare il contratto di licenza e continuare l'installazione.

Il processo di installazione potrebbe richiedere alcuni secondi per caricare i pacchetti di installazione.

5 Immettere `1` per utilizzare la chiave di licenza di valutazione di 90 giorni di default.

oppure

Immettere `2` per inserire una chiave di licenza di Sentinel acquistata.

6. Decidere se si desidera conservare la password esistente per l'utente amministratore `admin`.
   - Se si desidera conservare la password esistente, immettere `1`, quindi continuare con Passo 7.
   - Se si desidera cambiare la password esistente, immettere `2`, specificare la nuova password, confermarla, quindi continuare con Passo 7.
7. Decidere se si desidera conservare la password esistente per l'utente del database `dbauser`.
   - Se si desidera conservare la password esistente, immettere `1`, quindi continuare con Passo 8.
   - Se si desidera cambiare la password esistente, immettere `2`, specificare la nuova password, confermarla, quindi continuare con Passo 8.

   L'account `dbauser` rappresenta l'identità che Sentinel utilizza per interagire con il database. La password immessa in questa posizione può essere utilizzata per elaborare i task di manutenzione del database, incluso il ripristino della password admin qualora sia stata dimenticata o persa.
8. Decidere se si desidera conservare la password esistente per l'utente dell'applicazione `appuser`.
   - Se si desidera conservare la password esistente, immettere `1`, quindi continuare con Passo 9.
   - Se si desidera cambiare la password esistente, immettere `2`, specificare la nuova password, confermarla, quindi continuare con Passo 9.

   L'account `dbauser` rappresenta l'identità che Sentinel utilizza per interagire con il database. La password immessa in questa posizione può essere utilizzata per elaborare i task di manutenzione del database, incluso il ripristino della password admin qualora sia stata dimenticata o persa.
9. Modificare le assegnazioni delle porte per i servizi di Sentinel immettendo il numero desiderato della porta e, successivamente, specificando quello nuovo.
10. Una volta modificate le porte, specificare 7 per confermare il completamento.
11. Immettere `1` per autenticare gli utenti utilizzando solo il database interno.

    oppure

    Se nel dominio è stata configurata una directory LDAP, immettere `2` per autenticare gli utenti utilizzando l'autenticazione di tale directory.

    Il valore di default è `1`.

3 Installazione di Gestioni servizi di raccolta aggiuntive

Per default, Sentinel installa una Gestione servizi di raccolta. In base all'ambiente, potrebbe essere necessaria più di una Gestione servizi di raccolta. Utilizzare le informazioni seguenti per installare le Gestioni servizi di raccolta remote.

IMPORTANT: Nello stesso server in cui è in esecuzione Sentinel, non è possibile installare un'altra Gestione servizi di raccolta o un altro motore di correlazione.

3.1 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 possono analizzare sintatticamente ed elaborare i dati evento in un ambiente distribuito, potenziando la 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.
- **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 per i protocolli come syslog, che non supportano la memorizzazione nella cache degli eventi a livello nativo.

3.2 Istruzioni preliminari

Prima di iniziare il processo di installazione, verificare di aver completato i task seguenti.

❒ Assicurarsi che i requisiti hardware e software minimi siano soddisfatti. Per ulteriori informazioni, vedere Sezione 1.1, “Requisiti di sistema e piattaforme supportate”, a pagina 11.

- ❒ 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 Prima di iniziare il processo di installazione della Gestione servizi di raccolta, assicurarsi che a tutti i firewall e impostazioni di rete sia permesso comunicare su questa porta.

3.3 Installazione di una Gestione servizi di raccolta aggiuntiva

Installare la Gestione servizi di raccolta remota su un sistema diverso da quello in cui è installato Sentinel o il motore di correlazione remoto.

1. Avviare l'interfaccia Web di Sentinel immettendo l'URL seguente nel browser Web:

   `https://<IP_Address_Sentinel_server>:8443.`

   <*Indirizzo_IP_server_Sentinel*> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

   Effettuare il login con il nome utente e la password specificati durante l'installazione del server Sentinel.
2. Nella barra degli strumenti, fare clic su *Download*.
3. Sotto l'intestazione Gestione servizi di raccolta, fare clic su *Download del programma di installazione*.
4. Fare clic su *Salva file* per salvare il programma di installazione nell'ubicazione desiderata.
5. Per estrarre il file di installazione, immettere il comando seguente.

   `tar zxvf <install_filename>`

   Sostituire <*nomefile_installazione*> con il nome attuale del file di installazione.
6. Passare alla directory in cui è stato estratto il programma di installazione. Ad esempio:

   `cd sentinel_collector_mgr-7.0.0.0.x86_64`
7. Per installare la Gestione servizi di raccolta Sentinel, immettere il comando seguente:

   `./install-cm`

   Lo script di installazione verifica prima la memoria disponibile, quindi lo spazio su disco. Se si dispone di una quantità di memoria inferiore a 1.5 GB, lo script termina automaticamente l'installazione.
8. Immettere il numero relativo alla lingua che si desidera utilizzare per l'installazione.

   Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.
9. Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.
10. Immettere `yes` o `y` per accettare il contratto di licenza e continuare l'installazione.

    Il processo di installazione potrebbe impiegare alcuni secondi prima di richiedere con quale tipo di configurazione si intenda procedere.
11. Una volta richiesto, immettere 1 per procedere con la configurazione standard.
12. Immettere il nome host di default di Communication Server o l'indirizzo IP del computer in cui è installato Sentinel.
13. Specificare il nome utente e la password della Gestione servizi di raccolta.

Il nome utente e la password sono memorizzati nel file `/<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties` che risiede nel server Sentinel.

Ad esempio:

```
collectormanager=1c51ae55
```

In questo esempio, `collectormanager` è il nome utente e il valore corrispondente è la password.

14 Quando richiesto, accettare il certificato in modo permanente.

L'installazione di Gestione servizi di raccolta Sentinel remota è completata.

3.4 Aggiungere un utente personalizzato per una Gestione servizi di raccolta

Sentinel consiglia di utilizzare il nome utente di default di Gestione servizi di raccolta `collectormanager`. Tuttavia, se sono state installate più Gestioni servizi di raccolta e si desidera identificarle separatamente, è possibile creare dei nuovi utenti:

1 Effettuare il login al server come un utente che dispone dei diritti di accesso ai file di installazione di Sentinel.

2 Aprire il file `activemqgroups.properties`.

Questo file risiede nella directory `/<dir_installazione>/etc/opt/novell/sentinel/config/`.

3 Aggiungere il nuovo utente di Gestione servizi di raccolta nella sezione `cm`, separato da virgola. Ad esempio:

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

4 Salvare e chiudere il file.

5 Aprire il file `activemqusers.properties`.

Questo file risiede nella directory `/<dir_installazione>/etc/opt/novell/sentinel/config/`.

6 Aggiungere la password per l'utente creato in Passo 3.

La password può essere una stringa casuale qualsiasi. Ad esempio:

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

7 Salvare e chiudere il file.

8 Riavviare il server Sentinel.

4 Installazione di motori di correlazione aggiuntivi

Per default, Sentinel installa un motore di correlazione. Per gli ambienti che dispongono di un gran numero di regole di correlazione o frequenze eventi eccezionalmente elevate, potrebbe essere vantaggioso installare più motori di correlazione. Per ulteriori informazioni sulle frequenze eventi consigliate per il motore di correlazione, consultare Motore di correlazione in Capitolo 1, "Requisiti di sistema", a pagina 11.

IMPORTANT: Nel server in cui è in esecuzione Sentinel, non è possibile installare un'altra Gestione servizi di raccolta o un altro motore di correlazione.

4.1 Istruzioni preliminari

Prima di iniziare il processo di installazione, verificare di aver completato i task seguenti.

- ❒ Assicurarsi che i requisiti hardware e software minimi siano soddisfatti. Per ulteriori informazioni, vedere Sezione 1.1, "Requisiti di sistema e piattaforme supportate", a pagina 11.
- ❒ Sincronizzare l'orario mediante il protocollo NTP (Network Time Protocol).
- ❒ Per un motore di correlazione è necessaria una connettività di rete alla porta bus messaggi (61616) sul server Sentinel. Prima di iniziare il processo di installazione del motore di correlazione, assicurarsi che a tutti i firewall e a tutte le impostazioni di rete sia permesso comunicare su questa porta.

4.2 Installazione di un motore di correlazione aggiuntivo

Il motore di correlazione remoto deve essere installato su un sistema diverso da quello in cui è installato Sentinel o Gestione servizi di raccolta.

1. Avviare l'interfaccia Web di Sentinel immettendo l'URL seguente nel browser Web:

   `https://<IP_Address_Sentinel_server>:8443.`

   <Indirizzo_IP_server_Sentinel> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

   Effettuare il login con il nome utente e la password specificati durante l'installazione del server Sentinel.

2. Nella barra degli strumenti, fare clic su *Download*.
3. Sotto l'intestazione del motore di correlazione, fare clic su *Download del programma di installazione*.
4. Fare clic su *Salva file* per salvare il programma di installazione nell'ubicazione desiderata.
5. Per estrarre il file di installazione, immettere il comando seguente.

   ```
   tar zxvf <install_filename>
   ```

   Sostituire <*nomefile_installazione*> con il nome attuale del file di installazione.
6. Passare alla directory in cui è stato estratto il programma di installazione. Ad esempio:

   ```
   cd sentinel_correlation_engine-7.0.0.0.x86_64
   ```

7. Per installare il motore di correlazione Sentinel, immettere il comando seguente:

   ```
   ./install-ce
   ```

   Lo script di installazione verifica prima la memoria disponibile, quindi lo spazio su disco. Se si dispone di una quantità di memoria inferiore a 1.5 GB, lo script termina automaticamente l'installazione.
8. Immettere il numero relativo alla lingua che si desidera utilizzare per l'installazione.

   Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.
9. Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.
10. Immettere `yes` o `y` per accettare il contratto di licenza e continuare l'installazione.

    Il processo di installazione potrebbe richiedere alcuni secondi per effettuare l'upload dei pacchetti di installazione e richiedere il tipo di configurazione che si desidera utilizzare.
11. Una volta richiesto, immettere 1 per procedere con la configurazione standard.
12. Immettere il nome host di default di Communication Server o l'indirizzo IP del computer in cui è installato Sentinel.
13. Immettere il nome utente e la password del motore di correlazione.

    Il nome utente e la password sono memorizzati nel file `/<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties` che risiede nel server Sentinel.

    Ad esempio:

    ```
    correlationengine=68790d7a
    ```

    In questo esempio, `correlationengine` è il nome utente e il valore corrispondente è la password.
14. Quando richiesto, accettare il certificato in modo permanente.

    L'installazione del motore di correlazione Sentinel è completata.

4.3 Aggiungere un utente personalizzato per il motore di correlazione

Sentinel consiglia di utilizzare il nome utente di default del motore di correlazione `correlationengine`. Tuttavia, se sono stati installati più motori di correlazione remoti e si desidera identificarli separatamente, è possibile creare nuovi utenti:

1. Effettuare il login al server come un utente che dispone dei diritti di accesso ai file di installazione di Sentinel.
2. Aprire il file `activemqgroups.properties`.

   Questo file risiede nella directory `/<dir_installazione>/etc/opt/novell/sentinel/config/`.
3. Aggiungere i nuovi utenti del motore di correlazione nella sezione `admin`, separati da una virgola. Ad esempio:

   ```
   admins=system,correlationengine,ceuser1,ceuser2,...
   ```
4. Salvare e chiudere il file.
5. Aprire il file `activemqusers.properties`.

   Questo file risiede nella directory `/<dir_installazione>/etc/opt/novell/sentinel/config/`.
6. Aggiungere la password per l'utente creato in Passo 3.

   La password può essere una stringa casuale qualsiasi. Ad esempio:

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   correlationengine=68790d7a
   ceuser1=69700c6d
   ceuser2=70701b5c
   ```
7. Salvare e chiudere il file.
8. Riavviare il server Sentinel.

5 Installazione dell'applicazione

L'applicazione Sentinel è un'applicazione software pronta per l'esecuzione creata su SUSE Studio. L'applicazione unisce un sistema operativo SUSE Linux Enterprise Server (SLES) 11 SP 1 di protezione avanzata e il servizio di aggiornamento del software Sentinel 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 sull'hardware oppure in un ambiente virtuale.

5.1 Istruzioni preliminari

Prima di iniziare il processo di installazione dell'applicazione, assicurarsi di aver completato i task seguenti.

- ❒ Verificare che i requisiti hardware siano soddisfatti. Per ulteriori informazioni, vedere Sezione 1.1, “Requisiti di sistema e piattaforme supportate”, a pagina 11.
- ❒ Se si intende 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).
- ❒ Per la registrazione degli aggiornamenti del software, richiedere il codice di registrazione al Servizio clienti Novell (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22).

5.2 Installazione dell'applicazione VMware

5.2.1 Installazione di Sentinel

Per importare e installare l'immagine dell'applicazione Sentinel su un server VMware ESX:

1. Scaricare il file di installazione dell'applicazione VMware dal sito Web dei download di Novell (http://download.novell.com/index.jsp).

   Il file corretto per l'applicazione VMware contiene `vmx` nel nome file. Ad esempio, `sentinel_server_7.0.0.0.x86_64.vmx.tar.gz`
2. Stabilire un archivio dati ESX sul quale possa essere installata l'immagine dell'applicazione.
3. Eseguire il login come amministratore al server in cui si desidera installare l'applicazione.
4. Specificare il comando seguente per estrarre l'immagine compressa dell'applicazione dal computer in cui VM Converter è installato:

   ```
   tar zxvf <install_file>
   ```

   Sostituire <*file_installazione*> con il nome effettivo del file.
5. Per importare l'immagine di VMware al server ESX, utilizzare VMware Converter e seguire le istruzioni visualizzate sullo schermo durante l'installazione guidata.
6. Eseguire il login nel computer del server ESX.
7. Selezionare l'immagine VMware importata dell'applicazione e fare clic sull'icona *Power On (Accensione)*.
8. Selezionare la lingua che si desidera, quindi fare clic su *Avanti*.
9. Selezionare il layout della tastiera, quindi fare clic su *Avanti*.
10. Leggere e accettare il contratto di licenza del software SUSE Linux Enterprise Server (SLES) 11 SP1.
11. Leggere e accettare il contratto di licenza con l'utente finale di NetIQ Sentinel.
12. Nella pagina Nome host e Nome dominio, immettere il nome host e il nome di dominio, quindi assicurarsi che l'opzione *Assegnare il nome host all'IP di loopback* sia selezionata.
13. Fare clic su *Avanti*. La configurazione del nome host è salvata.
14. Effettuare una delle seguenti operazioni:
    - Per utilizzare le impostazioni di rete attuali, selezionare *Utilizzare la configurazione seguente* nella pagina Configurazione di rete II, quindi fare clic su *Avanti*.
    - Per modificare le impostazioni di connessione alla rete, selezionare *Cambia*, effettuare le modifiche desiderate, quindi fare clic su *Avanti*.

    Le impostazioni della connessione di rete sono salvate.
15. Impostare l'ora e la data, quindi fare clic su *Avanti*.

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

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

    ```
    rcntp restart
    ```
16. Impostare la password `root`, quindi fare clic su *Avanti*.

L'installazione controlla la quantità di memoria e spazio su disco disponibile. Se la quantità di memoria disponibile è inferiore a 2.5 GB, l'installazione non consente di continuare e il pulsante *Avanti* viene disattivato.

Se la quantità di memoria disponibile è superiore a 2.5 GB ma inferiore a 6.7 GB, l'installazione visualizza un messaggio per notificare che la quantità di memoria a disposizione è inferiore a quella consigliata. Quando viene visualizzato il messaggio, fare clic su *Avanti* per continuare con l'installazione.

17 Impostare la password admin di Sentinel, quindi scegliere *Avanti*.

Una volta eseguita l'installazione, l'avvio di tutti i servizi potrebbe richiedere alcuni minuti in quanto il sistema esegue una sola inizializzazione. Prima di effettuare il login al server, attendere il completamento dell'installazione.

18 Annotare l'indirizzo IP dell'applicazione mostrato nella console.

19 Procedere con Sezione 5.5, “Configurazione dell'applicazione successiva all'installazione”, a pagina 51.

5.2.2 Installazione di Gestione servizi di raccolta

Per importare e installare l'immagine dell'applicazione sul server VMWare ESX:

1 Scaricare il file di installazione dell'applicazione VMware dal sito Web dei download di Novell (http://download.novell.com/index.jsp).

Il file corretto per l'applicazione VMware contiene `vmx` nel nome file. Ad esempio, `sentinel_colletor_manager_7.0.0.0.x86_64.vmx.tar.gz`

2 Stabilire un archivio dati ESX sul quale possa essere installata l'immagine dell'applicazione.

3 Eseguire il login come amministratore al server in cui si desidera installare l'applicazione.

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

```
tar zxvf <install_file>
```

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

5 Per importare l'immagine di VMware al server ESX, utilizzare VMware Converter e seguire le istruzioni visualizzate sullo schermo durante l'installazione guidata.

6 Eseguire il login nel computer del server ESX.

7 Selezionare l'immagine VMware importata dell'applicazione e fare clic sull'icona *Power On (Accensione)*.

8 Specificare il nome host/indirizzo IP del server Sentinel al quale la Gestione servizi di raccolta deve connettersi.

9 Specificare il numero della porta di Communication Server. La porta bus messaggi di default è la `61616`.

10 Specificare il nome utente JMS, che rappresenta il nome utente di Gestione servizi di raccolta. Il nome utente di default è `collectormanager`.

11 Specificare la password per l'utente JMS.

Il nome utente e la password sono memorizzati nel file `/<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties` che risiede nel server Sentinel.

12 (Facoltativo) Per verificare la password, vedere la riga seguente nel file `activemqusers.properties`

```
collectormanager=<password>
```

In questo esempio, `collectormanager` è il nome utente e il valore corrispondente è la password.

13 Fare clic su *Avanti*.

14 Quando richiesto, accettare il certificato.

15 Per completare l'installazione, fare clic su *Avanti*.

Una volta completata l'installazione, viene visualizzato un messaggio per notificare che l'applicazione è la Gestione servizi di raccolta Sentinel, insieme all'indirizzo IP. Viene, inoltre, visualizzato l'indirizzo IP dell'interfaccia utente del server Sentinel.

5.2.3 Installazione del motore di correlazione

Il processo di installazione dell'applicazione del motore di correlazione è simile a quello realizzato per l'applicazione Gestione servizi di raccolta.

1 Scaricare il file di installazione dell'applicazione VMware dal sito Web dei download di Novell (http://download.novell.com/index.jsp).

Il file corretto del applicazione del motore di correlazione VMware include `vmx` nel nome del file. Ad esempio, `sentinel_correlation_engine_7.0.0.0.x86_64.vmx.tar.gz`

2 Stabilire un archivio dati ESX sul quale possa essere installata l'immagine dell'applicazione.

3 Eseguire il login come amministratore al server in cui si desidera installare l'applicazione.

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

```
tar zxvf <install_file>
```

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

5 Per importare l'immagine di VMware al server ESX, utilizzare VMware Converter e seguire le istruzioni visualizzate sullo schermo durante l'installazione guidata.

6 Eseguire il login nel computer del server ESX.

7 Selezionare l'immagine VMware importata dell'applicazione e fare clic sull'icona *Power On (Accensione)*.

8 Specificare il nome host/indirizzo IP del server Sentinel al quale il motore di correlazione deve connettersi.

9 Specificare il numero della porta di Communication Server. La porta bus messaggi di default è la `61616`.

10 Specificare il nome utente JMS, che rappresenta il nome utente del motore di correlazione. Il nome utente di default è `correlationengine`.

11 Specificare la password per l'utente JMS.

Il nome utente e la password sono memorizzati nel file `/<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties` che risiede nel server Sentinel.

12 (Facoltativo) Per verificare la password, vedere la riga seguente nel file `activemqusers.properties` :

```
correlationengine=<password>
```

In questo esempio, `correlationengine` è il nome utente e il valore corrispondente è la password.

13 Fare clic su *Avanti*.

14 Quando richiesto, accettare il certificato.

15 Per completare l'installazione, fare clic su *Avanti*.

Una volta completata l'installazione, viene visualizzato un messaggio per notificare che l'applicazione è il motore di correlazione Sentinel, insieme all'indirizzo IP. Viene, inoltre, visualizzato l'indirizzo IP dell'interfaccia utente del server Sentinel.

5.3 Installazione dell'applicazione Xen

5.3.1 Installazione di Sentinel

1 Scaricare il file di installazione dell'applicazione virtuale Xen dal sito Web dei download di Novell (http://download.novell.com/index.jsp) in `/var/lib/xen/images`.

Il nome file corretto dell'applicazione virtuale Xen contiene `xen`. Ad esempio, `Sentinel_7.0.0.0.x86_64.xen.tar.gz`

2 Per decomprimere il file, specificare il seguente comando:

```
tar -zxvf <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:

- *<nome_file>*`.raw`
- *<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 il `name` e le impostazioni della `memory`.

Ad esempio:

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

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

```
xm create <file_name>.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 generato.

Ad esempio, se `name="Sentinel_7.0.0.0.x86_64"` è stato configurato nel file `.xenconfig`, la memoria virtuale viene visualizzata con quel nome.

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

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

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_7.0.0.0.x86_64
```

L'installazione controlla prima la quantità di memoria e lo spazio su disco disponibili. Se la quantità di memoria disponibile è inferiore a 2.5 GB, il processo di installazione viene automaticamente terminato. Se la quantità di memoria disponibile è superiore a 2.5 GB ma inferiore a 6.7 GB, l'installazione visualizza un messaggio per notificare che la quantità di memoria a disposizione è inferiore a quella consigliata. Immettere `y` in caso affermativo oppure `n` se non si desidera continuare.

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 del software SUSE Linux Enterprise Server (SLES) 11 SP1.

12 Leggere e accettare il contratto di licenza con l'utente finale di NetIQ Sentinel.

13 Nella pagina Nome host e Nome dominio, immettere il nome host e il nome di dominio, quindi 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 di rete attuali, selezionare *Utilizzare la configurazione seguente* sulla pagina *Configurazione di rete II*.
- Per modificare le impostazioni della connessione, selezionare *Change* (Modifica), quindi apportare le modifiche desiderate.

16 Selezionare *Avanti*. Le impostazioni della connessione di rete sono salvate.

17 Impostare la data e l'ora, fare clic su *Avanti*, quindi su *Fine*

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
```

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

19 Impostare la password admin di Sentinel, quindi scegliere *Avanti*.

L'installazione di Sentinel continua fino al completamento. Una volta eseguita l'installazione, l'avvio di tutti i servizi potrebbe richiedere alcuni minuti in quanto il sistema esegue un'inizializzazione unica. Prima di effettuare il login al server, attendere il completamento dell'installazione.

Annotare l'indirizzo IP dell'applicazione mostrato nella console.

20 Procedere con Sezione 5.5, “Configurazione dell'applicazione successiva all'installazione”, a pagina 51.

5.3.2 Installazione di Gestione servizi di raccolta

Gestione servizi di raccolta può essere installata come applicazione su un sistema Linux abilitato per Xen che soddisfi i requisiti hardware minimi per la Gestione servizi di raccolta. Per ulteriori informazioni, vedere Sezione 1.1.2, “Requisiti hardware”, a pagina 12.

1. Completare Passo 1 mediante Passo 14 in Sezione 5.3.1, “Installazione di Sentinel”, a pagina 45.

   Il nome file corretto del file di installazione dell'applicazione virtuale Gestione servizi di raccolta Xen è `sentinel_collector_manager_7.0.0.0.x86_64.xen.tar.gz`
2. Nella schermata Configurazione di rete II, selezionare *Cambia* e specificare l'indirizzo IP della macchina virtuale in cui si desidera installare l'applicazione motore di correlazione aggiuntiva.
3. Specificare la maschera di sottorete dell'IP indicato.
4. Selezionare *Avanti*. Le impostazioni della connessione di rete sono salvate.
5. Impostare l'ora e la data, quindi selezionare *Avanti*.

   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
   ```
6. Impostare la password `root` di SUSE Enterprise Server, quindi selezionare *Avanti*.
7. Specificare il nome host/indirizzo IP del server Sentinel al quale il motore di correlazione deve connettersi.
8. Specificare il numero della porta di Communication Server. La porta bus messaggi di default è la `61616`.
9. Specificare il nome utente JMS, che rappresenta il nome utente di Gestione servizi di raccolta. Il nome utente di default è `collectormanager`.
10. Specificare la password per l'utente JMS.

    Il nome utente e la password sono memorizzati nel file `/<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties` che risiede nel server Sentinel.
11. (Facoltativo) Per verificare la password, vedere la riga seguente nel file `activemqusers.properties` :

    ```
    collectormanager=<password>
    ```

    In questo esempio, `collectormanager` è il nome utente e il valore corrispondente è la password.
12. Selezionare *Avanti* per completare l'installazione.

    Una volta completata l'installazione, viene visualizzato un messaggio per notificare che l'applicazione è la Gestione servizi di raccolta di Sentinel, insieme all'indirizzo IP.

5.3.3 Installazione del motore di correlazione

Il motore di correlazione può essere installato come applicazione su un sistema Linux abilitato per Xen che soddisfi i requisiti hardware del motore di correlazione. Per ulteriori informazioni, vedere Sezione 1.1.2, “Requisiti hardware”, a pagina 12.

1. Completare Passo 1 mediante Passo 14 in Sezione 5.3.1, “Installazione di Sentinel”, a pagina 45.

Il nome file corretto del file di installazione dell'applicazione virtuale del motore di correlazione Xen è `sentinel_correlation_engine_7.0.0.0.x86_64.xen.tar.gz`

2. Nella schermata Configurazione di rete II, selezionare *Cambia* e specificare l'indirizzo IP della macchina virtuale in cui si desidera installare l'applicazione del motore di correlazione.
3. Specificare la maschera di sottorete dell'IP indicato.
4. Selezionare *Avanti*. Le impostazioni della connessione di rete sono salvate.
5. Impostare l'ora e la data, quindi selezionare *Avanti*.

   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
   ```
6. Impostare la password `root` di SUSE Enterprise Server, quindi selezionare *Avanti*.
7. Specificare il nome host/indirizzo IP del server Sentinel al quale il motore di correlazione deve connettersi.
8. Specificare il numero della porta di Communication Server. La porta bus messaggi di default è la `61616`.
9. Specificare il nome utente JMS, che rappresenta il nomeutente del motore di correlazione. Il nome utente di default è `correlationengine`.
10. Specificare la password per l'utente JMS.
11. Fare clic su *Avanti*.

    Il nome utente e la password sono memorizzati nel file `/<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties` che risiede nel server Sentinel.
12. Per verificare la password, vedere la riga seguente nel file `activemqusers.properties` :

    ```
    correlationengine=<password>
    ```

    In questo esempio, `correlationengine` è il nome utente e il valore corrispondente è la password.
13. Quando richiesto, accettare il certificato.
14. Per completare l'installazione, fare clic su *Avanti*.

    Una volta completata l'installazione, viene visualizzato un messaggio per notificare che l'applicazione è il motore di correlazione Sentinel, insieme all'indirizzo IP. Viene, inoltre, visualizzato l'indirizzo IP dell'interfaccia utente del server Sentinel.

5.4 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 tale immagine sia stata decompressa e sia disponibile su DVD.

IMPORTANT: L'installazione su hardware mediante l'immagine disco ISO (hardware e Hyper-V) richiede una memoria minima di 4,5 GB per il completamento. Per ulteriori informazioni sui requisiti hardware, vedere Sezione 1.1.2, “Requisiti hardware”, a pagina 12.

5.4.1 Installazione di Sentinel

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.

   L'installazione controlla prima la quantità di memoria e lo spazio su disco disponibili. Se la quantità di memoria disponibile è inferiore a 2.5 GB, il processo di installazione viene automaticamente terminato. Se la quantità di memoria disponibile è superiore a 2.5 GB ma inferiore a 6.7 GB, l'installazione visualizza un messaggio per notificare che la quantità di memoria a disposizione è inferiore a quella consigliata. Immettere `y` in caso affermativo oppure `n` se non si desidera continuare.
4. Selezionare la lingua che si desidera, quindi fare clic su *Avanti*.
5. Selezionare il layout della tastiera, quindi fare clic su *Avanti*.
6. Leggere e accettare il contratto di licenza di SUSE Enterprise Server Software.
7. Leggere e accettare il contratto di licenza con l'utente finale di NetIQ Sentinel.
8. Selezionare *Avanti*.
9. Nella pagina Nome host e Nome dominio, immettere il nome host e il nome di dominio, quindi assicurarsi che l'opzione *}Assegnare il nome host all'IP di loopback* sia selezionata.
10. Selezionare *Avanti*. La configurazione del nome host è salvata.
11. Effettuare una delle seguenti operazioni:
    - Per utilizzare le impostazioni della connessione di rete attuali, selezionare *Utilizzare la configurazione seguente* nella pagina Configurazione di rete II.
    - Per modificare le impostazioni della connessione, selezionare *Change* (Modifica), quindi apportare le modifiche desiderate.
12. Selezionare *Avanti*. Le impostazioni della connessione di rete sono salvate.
13. Impostare l'ora e la data, quindi fare clic su *Avanti*.

    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
    ```
14. Impostare la password `root`, quindi fare clic su *Avanti*.
15. Impostare la password admin di Sentinel, quindi scegliere *Avanti*.

16 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 quella impostata in Passo 14.

17 Interrompere il server Sentinel:

   ```
   service sentinel stop
   ```

18 Per reimpostare l'interfaccia utente e disporre di una visualizzazione più chiara in YaST, immettere il comando seguente:

   ```
   reset
   ```

19 Per installare l'applicazione nel server fisico, eseguire il comando seguente:

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

   Una volta eseguita l'installazione, l'avvio di tutti i servizi potrebbe richiedere alcuni minuti in quanto il sistema esegue un'inizializzazione unica. Prima di effettuare il login al server, attendere il completamento dell'installazione.

20 Annotare l'indirizzo IP dell'applicazione mostrato nella console.

21 Procedere con Sezione 5.5, “Configurazione dell'applicazione successiva all'installazione”, a pagina 51.

5.4.2 Installazione di Gestione servizi di raccolta

Gestione servizi di raccolta può essere installata come applicazione su un sistema che soddisfi i requisiti hardware minimi per la Gestione servizi di raccolta. Per ulteriori informazioni, vedere Sezione 1.1.2, “Requisiti hardware”, a pagina 12.

1 Completare Passo 1 mediante Passo 14 in Sezione 5.4.1, “Installazione di Sentinel”, a pagina 49.

2 Specificare il nome host/indirizzo IP del server Sentinel al quale la Gestione servizi di raccolta deve connettersi.

3 Specificare il numero della porta di Communication Server. La porta bus messaggi di default è la `61616`.

   L'installazione tenta la connessione al server utilizzando le credenziali specificate. Se uno qualsiasi di questi valori non è stato immesso correttamente, l'installazione restituisce un errore.

4 Specificare il nome utente JMS, che rappresenta il nome utente di Gestione servizi di raccolta. Il nome utente di default è `collectormanager`.

5 Specificare la password per l'utente JMS.

6 Fare clic su *Avanti*.

   Il nome utente e la password sono memorizzati nel file `/<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties` che risiede nel server Sentinel.

7 Per verificare la password, vedere la riga seguente nel file `activemqusers.properties` :

   ```
   collectormanager=<password>
   ```

   In questo esempio, `collectormanager` è il nome utente e il valore corrispondente è la password.

8 Quando richiesto, accettare il certificato.

9 Per completare l'installazione, fare clic su *Avanti*.

   Una volta completata l'installazione, viene visualizzato un messaggio per notificare che l'applicazione è la Gestione servizi di raccolta di Sentinel, insieme all'indirizzo IP. Viene, inoltre, visualizzato l'indirizzo IP dell'interfaccia utente del server Sentinel.

5.4.3 Installazione del motore di correlazione

Il motore di correlazione può essere installato come applicazione su un sistema che soddisfi i requisiti hardware minimi del motore di correlazione. Per ulteriori informazioni, vedere Sezione 1.1.2, “Requisiti hardware”, a pagina 12.

1. Completare Passo 1 mediante Passo 14 in Sezione 5.4.1, “Installazione di Sentinel”, a pagina 49.
2. Specificare il nome host/indirizzo IP del server Sentinel al quale il motore di correlazione deve connettersi.
3. Specificare il numero della porta di Communication Server. La porta bus messaggi di default è la `61616`.
4. Specificare il nome utente JMS, che rappresenta il nome utente del motore di correlazione. Il nome utente di default è `correlationengine`.
5. Specificare la password per l'utente JMS.
6. Fare clic su *Avanti*.

   Il nome utente e la password sono memorizzati nel file `/<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties` che risiede nel server Sentinel.
7. Per verificare la password, vedere la riga seguente nel file `activemqusers.properties` :

   ```
   correlationengine=<password>
   ```

   In questo esempio, `correlationengine` è il nome utente e il valore corrispondente è la password.
8. Quando richiesto, accettare il certificato.
9. Per completare l'installazione, fare clic su *Avanti*.

   Una volta completata l'installazione, viene visualizzato un messaggio per notificare che l'applicazione è il motore di correlazione Sentinel, insieme all'indirizzo IP. Viene, inoltre, visualizzato l'indirizzo IP dell'interfaccia utente del server Sentinel.
10. Procedere con Sezione 5.5, “Configurazione dell'applicazione successiva all'installazione”, a pagina 51.

5.5 Configurazione dell'applicazione successiva all'installazione

5.5.1 Installazione dei VMware Tools

Per un funzionamento ottimale di Sentinel 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)

5.5.2 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, dove 8443 è la porta di default del server Sentinel. Viene visualizzata la pagina Web di Sentinel.

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

2. Configurare l'applicazione Sentinel per la memorizzazione e la raccolta dei dati.

   Per ulteriori informazioni sulla configurazione dell'applicazione, consultare la *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

3. Registrazione per gli aggiornamenti.

   Per ulteriori informazioni, vedere Sezione 5.9, "Registrazione degli aggiornamenti", a pagina 54.

5.6 Configurazione di WebYaST

L'interfaccia utente dell'applicazione Sentinel include WebYaST, una console Web remota che consente di controllare le applicazioni basate su SUSE Linux Enterprise. Mediante WebYaST è possibile accedere, configurare e controllare le applicazioni di Sentinel 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 all'applicazione Sentinel.
2. Fare clic su *Applicazione*.
3. Configurare il server di Sentinel per ricevere gli aggiornamenti come descritto in Sezione 5.9, "Registrazione degli aggiornamenti", a pagina 54.
4. Fare clic su *Avanti* per completare la configurazione iniziale.

5.7 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 di Sentinel, non appena queste vengono rilasciate. SMT è un sistema proxy a pacchetti integrato in Novell Customer Center completo di importanti funzionalità.

5.7.1 Prerequisiti

- Disporre delle credenziali di Novell Customer Center per Sentinel 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, vedere 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.

5.7.2 Configurazione dell'applicazione

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

5.8 Interruzione e avvio del server mediante l'interfaccia Web

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

1. Effettuare il login all'applicazione Sentinel.
2. Fare clic su *Applicazione* per avviare WebYaST.
3. Fare clic su *Servizi di sistema*.
4. Per interrompere il server Sentinel, fare clic su *interrompi*.
5. Per avviare il server Sentinel, fare clic su *avvia*.

5.9 Registrazione degli aggiornamenti

1. Effettuare il login all'applicazione Sentinel.
2. Fare clic su *Applicazione* per avviare WebYaST.
3. Fare clic su *Registrazione*.
4. Specificare l'ID dell'e-mail in cui si desidera ricevere gli aggiornamenti, il nome del sistema e il codice di registrazione dell'applicazione.
5. Fare clic su *Salva*.

6 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.

6.1 Installazione non riuscita a causa di una configurazione della rete non corretta

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

Per risolvere questo problema, configurare le impostazioni di rete nel modo appropriato. Per verificare la configurazione, utilizzare il comando `ifconfig` per ottenere l'indirizzo IP valido e quello `hostname -f` per ottenere il nome host valido.

6.2 Non viene creato l'UUID per le Gestioni servizi di raccolta o il Motore di raccolta

Se un server Gestione servizi di raccolta viene creato mediante un'immagine utilizzando, ad esempio, ZENworks Imaging e, successivamente, l'immagine creata viene ripristinata su computer diversi, Sentinel non identifica in modo univoco le nuove istanze della Gestione servizi di raccolta. Ciò si verifica a causa degli UUID duplicati.

Nei sistemi in cui la Gestione servizi di raccolta è stata appena installata, è necessario generare un nuovo UUID eseguendo la procedura seguente:

1. Eliminare il file `host.id` o `sentinel.id` situato nella cartella `/var/opt/novell/sentinel/data`.
2. Riavviare Gestione servizi di raccolta.

   L'UUID viene generato automaticamente da Gestione servizi di raccolta.

7 Operazione successiva

Una volta installato Sentinel, esistono due guide che forniscono tutte le istruzioni necessarie per eseguirne la configurazione: la *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)* e la *NetIQ Sentinel 7.0.1 User Guide (Guida per l'utente di NetIQ Sentinel 7.0.1)*.

La guida all'amministrazione contiene informazioni sulla configurazione per attività che solo gli utenti amministratori sono autorizzati ad eseguire. Ad esempio:

- "Configurazione di utenti e ruoli"
- "Configurazione della memorizzazione dei dati"
- "Configurazione della raccolta di dati"
- "Ricerca e generazione di rapporti su eventi in ambienti distribuiti"

Per ulteriori informazioni relative a questi e ad altri task amministrativi, consultare la *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

Nella Guida per l'utente sono contenute le istruzione necessarie per eseguire i task in Sentinel. Ad esempio:

- "Ricerca di eventi"
- "Analisi di tendenze nei dati"
- "Generazione di rapporti"
- "Configurazione di incidenti"

Per ulteriori informazioni relative a questi e ad altri task dell'utente, consultare la *NetIQ Sentinel 7.0.1 User Guide* (Guida per l'utente di NetIQ Sentinel 7.0.1).

Sentinel, inoltre, può essere configurato per analizzare gli eventi, aggiungere i dati mediante le regole di correlazione, impostare le linee di base, configurare i workflow per intervenire sulle informazioni e molto altro ancora. Per configurare queste funzioni di Sentinel utilizzare le istruzioni contenute nella *NetIQ Sentinel 7.0.1 Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).

II Configurazione

Una volta completata l'installazione, è possibile configurare Sentinel affinché sia eseguito in un determinato ambiente.

8 Accesso all'interfaccia Web di Sentinel

Una volta completata l'installazione di Sentinel, è possibile effettuare il login all'interfaccia Web di Sentinel per eseguire i task amministrativi e configurare Sentinel per la raccolta dei dati.

1. Aprire un browser Web ed effettuare il login a https://<*Indirizzo IP*>:8443, dove 8443 è la porta di default del server Sentinel.
2. (Condizionale) La prima volta che si effettua l'accesso a Sentinel, accettare il certificato quando richiesto.

   La pagina di login di Sentinel viene visualizzata al momento dell'accettazione del certificato.
3. Specificare il nome utente e la password dell'amministratore di Sentinel
4. Fare clic su *Login*.

   Viene visualizzata l'interfaccia Web di NetIQ Sentinel.

9 Aggiunta di ulteriori componenti di Sentinel

Per default, Sentinel dispone di un connettore syslog e un servizio di raccolta già installati e configurati, oltre a diversi connettori di revisione e servizi di raccolta per prodotti Novell. Nelle sezioni seguenti viene descritta la procedura di installazione e configurazione di connettori e servizi di raccolta aggiuntivi.

9.1 Installazione dei servizi di raccolta e dei connettori

Per default, tutti i servizi di raccolta e connettori rilasciati vengono installati al momento dell'installazione di Sentinel 7. Se successivamente all'installazione di Sentinel 7 viene rilasciato un nuovo servizio di raccolta o connettore, prima di eseguirne la configurazione è necessario installarne i file.

9.1.1 Installazione di un servizio di raccolta

1. Effettuare il download del servizio di raccolta corretto dalla pagina Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
2. Effettuare il login all'interfaccia Web di Sentinel all'indirizzo https://<*IP address*>:8443, dove 8443 è la porta di default del server Sentinel.
3. Fare clic su *Applicazioni* nella barra degli strumenti, quindi scegliere *Applicazioni*.
4. Fare clic su *Avvia Control Center* per avviare Sentinel Control Center.
5. Nella barra degli strumenti, fare clic su *Gestione origini eventi* > *Visualizzazione in diretta*, quindi scegliere *Strumenti* > *Importa plug-in*.
6. Individuare e selezionare il file relativo al servizio di raccolta di cui è stato effettuato il download in Passo 1, quindi fare clic su *Avanti*.
7. Rispondere alle richieste rimanenti, quindi fare clic su *Fine*.

Per configurare il servizio di raccolta, consultare la documentazione relativa presente nella pagina Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.1.2 Installazione di un connettore

1. Effettuare il download del connettore corretto dalla pagina Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
2. Effettuare il login all'interfaccia Web di Sentinel all'indirizzo https://<*IP address*>:8443, dove 8443 è la porta di default del server Sentinel.
3. Fare clic su *Applicazione* nella barra degli strumenti, quindi scegliere *Applicazioni*.
4. Fare clic su *Avvia Control Center* per avviare Sentinel Control Center.
5. Nella barra degli strumenti, fare clic su *Gestione origini eventi* > *Visualizzazione in diretta*, quindi scegliere *Strumenti* > *Importa plug-in*.
6. Individuare e selezionare il file relativo al connettore di cui è stato effettuato il download in Passo 1, quindi fare clic su *Avanti*.
7. Rispondere alle richieste rimanenti, quindi fare clic su *Fine*.

Per configurare un connettore, consultare la documentazione relativa presente nella pagina Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2 Aggiunta di ulteriori servizi di raccolta e connettori

9.2.1 Aggiunta di ulteriori servizi di raccolta

Per normalizzare i dati provenienti da altre origini, è possibile aggiungere ulteriori servizi di raccolta.

1. Effettuare il login all'interfaccia Web di Sentinel all'indirizzo https://<*IP address*>:8443, dove 8443 è la porta di default del server Sentinel.
2. Fare clic su *Applicazione* nella barra degli strumenti, quindi scegliere *Applicazioni*.
3. Fare clic su *Avvia Connector Center* per avviare Sentinel Control Center.
4. Nella barra degli strumenti, fare clic su *Gestione origini eventi* > *Visualizzazione in diretta*.
5. Fare clic con il pulsante destro del mouse su Gestione servizi di raccolta, quindi fare clic su *Add Collector* (Aggiungi servizio di raccolta).
6. Selezionare il servizio di raccolta nella colonna *Fornitore*, quindi scegliere *Avanti*.
7. I campi per ciascun servizio di raccolta sono diversi, quindi, in questo punto, per configurare il servizio di raccolta è necessario attenersi alla documentazione specifica.

   La documentazione del servizio di raccolta si trova nella pagina Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2.2 Aggiunta di ulteriori connettori

Per raccogliere informazioni da altre origini, è possibile aggiungere ulteriori connettori.

1. Effettuare il login all'interfaccia Web di Sentinel all'indirizzo https://<*IP address*>:8443, dove 8443 è la porta di default del server Sentinel.
2. Fare clic su *Applicazione* nella barra degli strumenti, quindi scegliere *Applicazioni*.

3 Fare clic su *Avvia Control Center* per avviare Sentinel Control Center.

4 Nella barra degli strumenti, fare clic su *Gestione origini eventi* > *Visualizzazione in diretta*.

5 Fare clic con il pulsante destro del mouse sul servizio di raccolta che si desidera aggiungere al connettore, quindi scegliere *Aggiungi connettore*.

6 Selezionare il connettore desiderato nella colonna *Nome*, quindi scegliere *Avanti*.

7 I campi per ciascun connettore sono diversi, quindi, in questo punto, per configurare il connettore è necessario attenersi alla documentazione specifica.

   La documentazione del connettore si trova nella pagina Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

10 Gestione dei dati

10.1 Struttura della directory

Per default, le directory di Sentinel risiedono nelle ubicazioni seguenti:

- I file di dati risiedono nelle directory `/var/opt/novell/sentinel/data` e `/var/opt/novell/sentinel/3rdparty`.
- I file eseguibili e le librerie sono archiviate nelle directory seguenti:
  - `/opt/novell/sentinel/bin`
  - `/opt/novell/sentinel/setup`
  - `/opt/novell/sentinel/3rdparty`
- I file di log risiedono nella directory `/var/opt/novell/sentinel/log`
- I file di configurazione risiedono nella directory seguente: `/etc/opt/novell/sentinel`
- Il file ID processo (PID) risiede nella directory `/var/run/sentinel/server.pid`.

  Mediante il file PID, gli amministratori possono identificare il processo superiore del server Sentinel e controllare o terminare il processo.

10.2 Considerazioni sulla memorizzazione

Durante la memorizzazione dei file di dati di Sentinel, assicurarsi che questi vengano memorizzati in una partizione diversa da quella in cui risiedono i file eseguibili, di configurazione e del sistema operativo. Il vantaggio derivato dalla memorizzazione in una partizione separata offre la possibilità di creare più facilmente l'immagine di un set di file e di recuperarla qualora si verifichino dei danneggiamenti. Inoltre, viene migliorata la prestazione complessiva dei sistemi in cui i file system di dimensioni più ridotte risultano più efficienti. Per ulteriori informazioni, vedere “Partizione del disco” (http://en.wikipedia.org/wiki/Disk_partitioning#Benefits_of_multiple_partitions).

È possibile decidere di installare Sentinel su più partizioni oppure su un'unica partizione, in base ai tipi di installazione seguenti:

- Installazione in modalità autonoma
- Installazione in modalità applicazione.

10.2.1 Utilizzo della partizione in un'installazione in modalità autonoma

Se si sta eseguendo l'installazione di Sentinel in modalità autonoma, prima di tale procedura è possibile modificare il layout della partizione del sistema operativo. L'amministratore deve creare e montare le partizioni desiderate nelle directory appropriate, in base alla struttura delle directory descritta dettagliatamente in Sezione 10.1, “Struttura della directory”, a pagina 67. Quando viene eseguito il programma di installazione, Sentinel viene installato nelle directory già predisposte, espandendosi in più partizioni.

NOTE:

- Durante l'esecuzione del programma di installazione è possibile utilizzare l'opzione `--location` per specificare un'ubicazione diversa da quella delle directory di default in cui memorizzare il file. Il valore impostato per l'opzione `--location` è posto all'inizio dei percorsi delle directory. Ad esempio, se viene specificato `--location=/foo`, la directory dati sarà `/foo/var/opt/novell/sentinel/data` e la directory di configurazione sarà `/foo/etc/opt/novell/sentinel/config`.
- Non utilizzare i collegamenti del file system (ad esempio, i collegamenti simbolici) per l'opzione `--location`.

10.2.2 Utilizzo del partizionamento in un'installazione in modalità applicazione

Se si sta eseguendo l'installazione di Sentinel in modalità applicazione, non è possibile configurare nuovamente il sistema operativo prima dell'installazione di Sentinel in quanto il sistema operativo viene installato insieme a Sentinel. Tuttavia, è possibile aggiungere la partizione nell'applicazione e spostarvi una directory mediante lo strumento YaST.

La procedura seguente consente di creare una nuova partizione e spostare i file di dati dalla directory in cui risiedono alla partizione appena creata:

1. Effettuare il login a Sentinel come `root`.
2. Per interrompere Sentinel nell'applicazione, eseguire il comando seguente:

   ```
   /etc/init.d/sentinel stop
   ```
3. Specificare il comando seguente per modificare l'utente `novell`:

   ```
   su -novell
   ```
4. Spostare i contenuti presenti nella directory `/var/opt/novell/sentinel/` in un'ubicazione temporanea.
5. Passare a utente `root`.
6. Per accedere a YaST2 Control Center, immettere il comando seguente:

   ```
   yast
   ```
7. Selezionare *Sistema* > *Partitioner*.
8. Leggere gli avvisi e selezionare *Sì* per aggiungere la nuova partizione non ancora utilizzata.
9. Montare la nuova partizione in `/var/opt/novell/sentinel`.
10. Specificare il comando seguente per modificare l'utente `novell`:

    ```
    su -novell
    ```

11 Spostare nuovamente i contenuti della directory dati dall'ubicazione temporanea (in cui sono stati salvati in Passo 4) nella nuova partizione in `/var/opt/novell/sentinel/`.

12 Passare a utente `root`.

13 Per riavviare l'applicazione Sentinel, eseguire il comando seguente:

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

11 Configurazione del contenuto pronto all'uso

Sentinel viene distribuito insieme a un'ampia gamma di contenuti molto utili e pronti all'uso, che è possibile utilizzare subito per fornire una soluzione a molti dei problemi relativi alle analisi. Gran parte di questo contenuto proviene da un pacchetto soluzione principale preinstallato. Per ulteriori informazioni, consultare "Using Solution Packs (Utilizzo dei pacchetti soluzione)" nella *NetIQ Sentinel 7.0.1 User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

Il pacchetto soluzione consente di categorizzare e raggruppare il contenuto in vari set di "controlli" o policy che vengono elaborati come un'unica unità. I controlli inclusi nel pacchetto soluzione principale di Sentinel vengono preinstallati in modo da poter fornire il contenuto pronto all'uso. Tuttavia, tali controlli devono essere formalmente implementati o provati mediante l'interfaccia Web di Sentinel.

Se è richiesta una verifica rigorosa per dimostrare che l'implementazione di Sentinel funziona come previsto, è possibile utilizzare il processo di attestazione formale incorporato nei pacchetti soluzione. Tale processo implementa e prova i controlli principali di Sentinel allo stesso modo in cui un utente esegue l'implementazione e la prova dei controlli di qualsiasi altro pacchetto soluzione. Come parte integrante del processo, i programmi incaricati di eseguire l'implementazione e la prova attestano che il lavoro da loro svolto è stato completato. Successivamente, tali attestazioni diventano parte di un audit trail che può essere analizzato per dimostrare che ogni controllo è stato installato in modo adeguato.

È possibile eseguire il processo di attestazione mediante Solution Manager. Per ulteriori informazioni sull'implementazione e l'esecuzione della prova dei controlli, consultare "Installing and Managing Solution Packs (Installazione e gestione dei pacchetti soluzione)" nella *NetIQ Sentinel 7.0.1 User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

12 Orario di configurazione

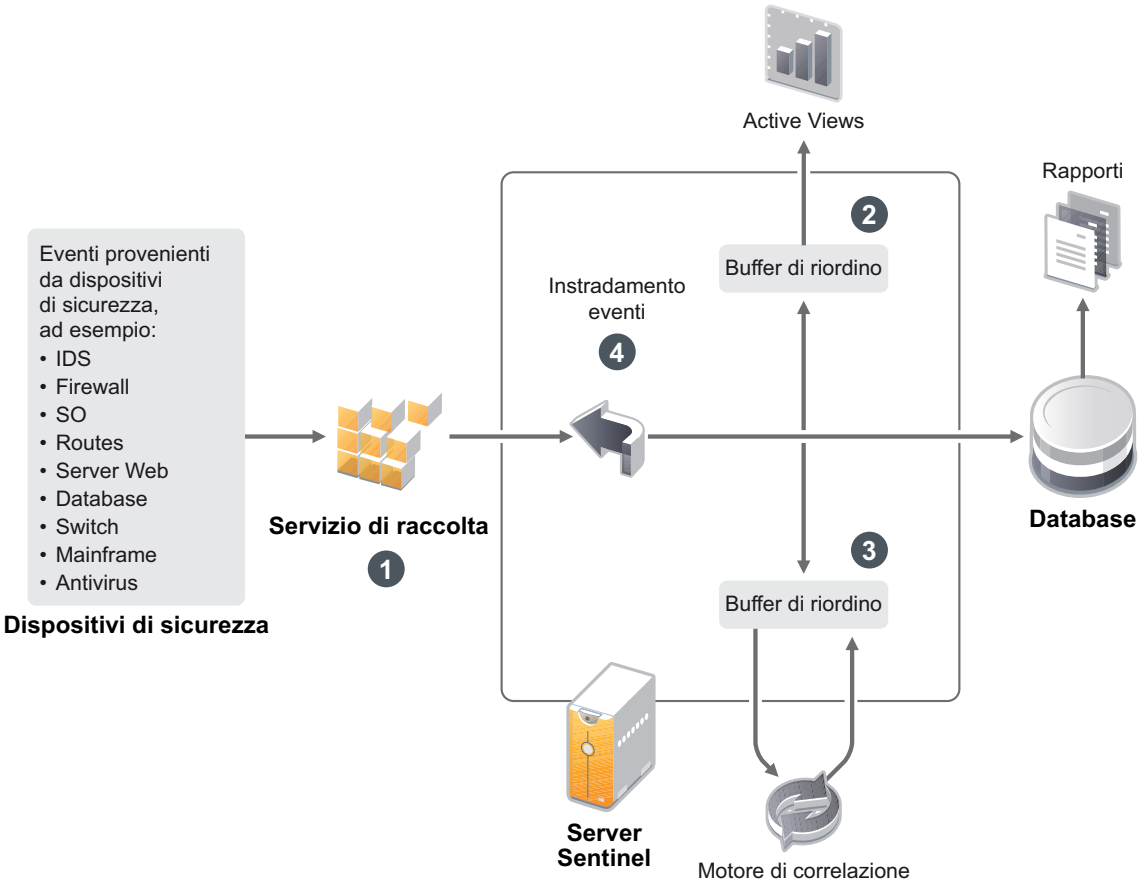
L'ora di un evento è una caratteristica rilevante per la sua elaborazione in Sentinel. La sua importanza incide sulla generazione dei rapporti, la revisione e l'elaborazione in tempo reale.

12.1 L'orario in Sentinel

Sentinel è un sistema distribuito e consiste in diversi processi che possono essere realizzati in varie parti della rete. Il dispositivo potrebbe inoltre indurre alcuni ritardi. Per gestire al meglio tali ritardi, prima dell'elaborazione i processi di Sentinel ordinano nuovamente gli eventi in un flusso organizzato in base all'orario.

Nell'illustrazione seguente, viene fornita la spiegazione del modo in cui Sentinel realizza questa operazione:

Figura 12-1 *Orario Sentinel*



1. Per default, l'orario evento è impostato sull'orario della Gestione servizi di raccolta. L'orario ideale è quello del dispositivo. È consigliabile, quindi, impostare l'orario evento tenendo come riferimento l'orario del dispositivo, qualora questo sia disponibile, accurato e analizzato sintatticamente nel modo adeguato dal servizio di raccolta.
2. Gli eventi vengono ordinati a intervalli di 30 secondi, affinché possano essere visualizzati in Active Views. Per default, gli eventi che dispongono di una registrazione orario compresa in un intervallo di 5 minuti dall'orario del server (in passato o futuro) vengono elaborati normalmente. Gli eventi che dispongono di una registrazione orario superiore ai 5 minuti rispetto al futuro non vengono visualizzati in Active Views, ma vengono inseriti nella memorizzazione eventi. Gli eventi che dispongono di una registrazione orario superiore ai 5 minuti ma inferiore alle 24 ore rispetto al passato vengono ancora mostrati nei grafici, ma non sono visualizzati nei dati evento di tali grafici. Per recuperare quegli eventi dalla memorizzazione eventi, è necessario eseguire il drill-down.
3. Se l'orario evento è superiore ai 30 secondi anteriori rispetto all'orario del server, il motore di correlazione non è in grado di elaborare gli eventi.
4. Se l'orario evento è anteriore di 5 minuti rispetto all'orario della Gestione servizi di raccolta (orario corretto), gli eventi vengono direttamente instradati alla memorizzazione eventi.

12.2 Configurazione dell'orario in Sentinel

Il motore di correlazione elabora i flussi degli eventi ordinati in base all'orario e rileva i modelli inclusi negli eventi insieme ai modelli temporali presenti nel flusso. Tuttavia, il dispositivo che genera l'evento a volte non include l'orario nei messaggi del log. Per configurare l'orario di lavoro affinché funzioni correttamente con Sentinel, sono possibili due opzioni:

- Configurare NTP nella Gestione servizi di raccolta e deselezionare *Ora origine evento elemento attendibile* nell'origine evento presente in Gestione origini eventi. Gestione servizi di raccolta viene utilizzata da Sentinel come l'origine dell'orario per gli eventi.
- Selezionare *Ora origine evento elemento attendibile* nell'origine evento in Gestione origini eventi. Sentinel utilizza l'ora del messaggio del log come ora corretta.

Per modificare questa impostazione sull'origine evento:

1. Effettuare il login a Gestione origini eventi.

   Per ulteriori informazioni, consultare "Accessing Event Source Management (Accesso alla Gestione origini eventi)" nella *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.
2. Selezionare con il pulsante destro del mouse l'origine evento della quale si desidera modificare le impostazioni relative all'orario, quindi scegliere *Modifica*.
3. Selezionare o meno l'opzione *Origine evento elemento attendibile* presente nella parte inferiore della scheda *Generale*.
4. Fare clic su *OK* per salvare la modifica.

12.3 Gestione dei fusi orari

In un ambiente distribuito, la gestione dei fusi orari può essere molto complessa. Ad esempio, potrebbe presentarsi la situazione in cui un'origine evento si trova in un fuso orario, Gestione servizi di raccolta in un altro, il server Sentinel di back end in un altro e il client che sta visualizzando i dati in un altro fuso orario ancora. Quando vengono aggiunti elementi quali l'ora legale e le molte origini evento che non segnalano il fuso orario che è stato loro impostato (come tutte le origini syslog), i problemi da gestire potrebbero essere diversi. La flessibilità caratteristica di Sentinel consente di rappresentare nel modo più adeguato l'orario in cui effettivamente si verificano gli eventi e comparare tali eventi con altri provenienti da altre origini evento presenti nello stesso o in un diverso fuso orario.

Generalmente, vi sono tre scenari diversi in base ai quali le origini evento segnalano le registrazioni orario:

- L'origine evento segnala l'ora in base al fuso orario UTC (Coordinated Universal Time, tempo coordinato universale). Ad esempio, tutti gli eventi standard del log eventi di Windows sono sempre segnalati secondo il fuso orario UTC.
- L'origine evento riporta l'ora locale, ma include sempre il fuso orario nella registrazione orario. Ad esempio, qualsiasi origine evento che si attiene al formato RFC3339 nella struttura delle registrazioni orario include il fuso orario come offset. Altre origini, invece, riportano ID di fuso orario in formato lungo, come Americhe/New York, o abbreviato come EST (Eastern Standard Time, orario orientale standard) che possono presentare qualche problema a causa di conflitti e risoluzioni non adeguate.
- L'origine evento riporta l'ora locale, ma non indica il fuso orario. Sfortunatamente, il formato syslog più comune si attiene a questo modello.

Per il primo scenario, è sempre possibile calcolare l'orario UTC assoluto in cui si è verificato un evento (supponendo che venga utilizzato un protocollo per la sincronizzazione dell'orario), in modo da semplificare la comparazione tra l'orario di tale evento con una qualsiasi altra origine evento del mondo. Tuttavia, non è possibile determinare automaticamente l'ora locale in cui si è verificato l'evento. Per questo motivo, Sentinel consente ai clienti di impostare manualmente il fuso orario di un'origine evento modificando il nodo dell'origine evento nella Gestione origini eventi e specificando il fuso orario appropriato. Queste informazioni non incidono sul calcolo di OrarioDispositivoEvento o OrarioEvento, ma vengono poste nel campo FOSensore e utilizzate per calcolare vari campi FOSensore, come OraFOSensore. Questi campi sono sempre espressi secondo l'ora locale.

Il secondo scenario è, spesso, il più semplice. Se vengono utilizzati ID di fuso orario in formato lungo oppure offset, è possibile passare semplicemente al formato UTC per recuperare l'orario UTC assoluto canonico (memorizzato in OrarioEventoDispositivo), ma è possibile anche calcolare facilmente i campi FOSensore dell'ora locale. Se viene utilizzato l'ID del fuso orario in formato abbreviato, potrebbero generarsi dei conflitti potenziali.

Il terzo scenario può essere il più complicato in quanto richiede che l'amministratore imposti manualmente il fuso orario dell'origine evento per tutte le origini interessate, affinché Sentinel sia in grado di calcolare nel modo più appropriato l'orario UTC. Se il fuso orario non viene specificato adeguatamente modificando il nodo dell'origine evento nella Gestione origini eventi, OrarioEventoDispositivo (e probabilmente OrarioEvento) possono risultare non corretti così come FOSensore e i campi associati.

Generalmente, il servizio di raccolta per un determinato tipo di origine evento (come Microsoft Windows) è a conoscenza del modo in cui un'origine evento presenta una registrazione orario e si regola di conseguenza. È comunque consigliato impostare sempre manualmente il fuso orario di tutti i nodi delle origini evento nella Gestione origini eventi, eccetto qualora si sia a conoscenza che l'origine evento riporta l'ora locale e include sempre il fuso orario nella registrazione orario.

L'elaborazione della presentazione dell'origine evento della registrazione orario si verifica nel servizio di raccolta e nella Gestione servizi di raccolta. OraEventoDispositivo e OraEvento sono memorizzati come UTC e i campi FOSensore sono memorizzati come stringhe impostate per l'ora locale dell'origine evento. Queste informazioni vengono inviate dalla Gestione servizi di raccolta al server Sentinel e memorizzate nella memorizzazione eventi. Il fuso orario in cui si trova Gestione servizi di raccolta o il server Sentinel non ha alcuna implicazione sul processo o sui dati memorizzati. Tuttavia, quando un client visualizza l'evento in un browser Web, l'OraEvento UTC viene convertita nell'ora locale relativa a tale browser, affinché tutti gli eventi siano presentati ai client nel fuso orario locale. Se gli utenti desiderano visualizzare l'ora locale dell'origine, possono disporre di ulteriori dettagli consultando i campi FOSensore.

13 Informazioni sulle licenze

Questa sezione descrive le diverse licenze di Sentinel e fornisce le informazioni necessarie per la loro gestione.

13.1 Le licenze di Sentinel

Sentinel dispone di diversi tipi di licenze da utilizzare. Per default, Sentinel viene fornito con una licenza di valutazione.

13.1.1 Licenza di valutazione

La licenza di Sentinel di default consente di utilizzare tutte le funzioni aziendali di Sentinel per un periodo di valutazione di 90 giorni.. Nell'interfaccia Web di un sistema in cui è in esecuzione una licenza di valutazione viene visualizzato un indicatore che segnala che è attualmente in uso una chiave di licenza temporanea. Inoltre, vengono visualizzati i giorni rimanenti prima della scadenza della funzionalità, fornendo le istruzioni necessarie per eseguire l'upgrade a una licenza di tipo completo.

NOTE: La data di scadenza del sistema si basa sui dati più vecchi presenti nel sistema. Se vengono ripristinati eventi obsoleti nel sistema, la data di scadenza verrà regolata di conseguenza.

Dopo il periodo di valutazione di 90 giorni, molte funzionalità vengono disabilitate, ma è sempre possibile effettuare il login e aggiornare il sistema per utilizzare una chiave di licenza aziendale.

Una volta eseguito l'upgrade a una licenza aziendale, vengono ripristinate tutte le funzionalità. Onde evitare l'interruzione di qualsiasi funzionalità, è necessario eseguire l'upgrade del sistema a una licenza aziendale prima della data di scadenza.

13.1.2 Licenze aziendali

Al momento dell'acquisto di Sentinel, viene ricevuta una chiave di licenza tramite il portale clienti. In base all'acquisto realizzato, la chiave di licenza permette alcune funzionalità, frequenze di raccolta dati e origini evento. Potrebbero esservi ulteriori termini di licenza che non vengono applicati dalla chiave di licenza per cui si consiglia di leggere attentamente il contratto di licenza.

Per modificare la licenza, contattare il responsabile dell'account. Per aggiungere la chiave di licenza al sistema, vedere Sezione 13.2.1, “Aggiunta di una chiave di licenza mediante l'interfaccia Web”, a pagina 78.

13.2 Aggiunta di una chiave di licenza

NOTE: Per aggiungere o eliminare una licenza è necessario disporre dei diritti di amministratore.

È possibile aggiungere una chiave di licenza mediante l'interfaccia Web oppure utilizzando la riga di comando.

13.2.1 Aggiunta di una chiave di licenza mediante l'interfaccia Web

1. Accedere all'interfaccia Web di Sentinel come amministratore.
2. Fare clic sul collegamento *Informazioni su*presente nell'angolo superiore sinistro della pagina.
3. Fare clic sulla scheda *Licenz*e.
4. Nella sezione Licenze, fare clic su *Aggiungi licenza*.
5. Specificare la chiave di licenza nel campo *Chiave*. Una volta specificata la licenza, nella sezione Anteprima vengono visualizzate le informazioni seguenti:

   Funzioni: le funzioni disponibili con la licenza.

   Nome host: questo campo è solo per utilizzo interno di NetIQ.

   Seriale: questo campo è solo per utilizzo interno di NetIQ.

   EPS: Frequenza eventi integrata nella chiave di licenza. Oltre questa frequenza, Sentinel genera degli avvisi ma continua la raccolta dei dati.

   Scade: data di scadenza della licenza. È necessario specificare una chiave di licenza valida prima della data di scadenza onde evitare l'interruzione delle funzionalità.
6. Fare clic su *Salva*.

13.2.2 Aggiunta di una chiave di licenza utilizzando la riga di comando

È possibile aggiungere la licenza mediante la riga di comando utilizzando lo script `softwarekey.sh`.

1. Eseguire il login al server di Sentinel come utente `root`.
2. Passare alla directory `/opt/novell/sentinel/bin`.
3. Per passare all'utente novell, immettere il comando seguente:

   ```
   su novell
   ```

4. Specificare il comando seguente per eseguire lo script `softwarekey.sh`.

   ```
   ./softwarekey.sh
   ```

5. Immettere 1 per inserire la chiave di licenza.
6. Specificare la chiave di licenza, quindi premere Invio.

14 Configurazione di Sentinel per alta disponibilità

Sentinel è stato sottoposto a prove ed è stato certificato per funzionare in un ambiente ad alta disponibilità per cui supporta le architetture di disaster recovery. NetIQ Consulting e i partner NetIQ possono facilitare l'implementazione dell'alta disponibilità e del disaster recovery di Sentinel.

Per abilitare i server Sentinel per l'alta disponibilità, è necessario attenersi alla procedura seguente:

- Nodi Sentinel in cluster, ridondanti.
- Accedere alla memorizzazione di dati condivisa.
- Indirizzi IP virtuali che possono essere utilizzati per passare in modo trasparente da un nodo non riuscito a un altro nodo.
- Script per avviare, interrompere e controllare l'applicazione in base alle policy definite nelle soluzioni cluster. È possibile utilizzare soluzioni cluster come Cluster Resource Agents o gli script init LSB su sistemi Linux Enterprise ad alta disponibilità.

Sul mercato, sono presenti diversi pacchetti che consentono di abilitare l'alta disponibilità. Sono state eseguite delle prove di Sentinel con *SUSE Linux Enterprise High Availability (HA) Extension* (http://www.novell.com/products/highavailability/), unità RAID di memorizzazione condivisa e script personalizzati. Questa architettura può essere replicata attraverso i data center per assicurare la disponibilità di tutti i processi procedenti dal server Sentinel verso le Gestioni servizi di raccolta e i servizi di raccolta.

L'alta disponibilità per le origini evento deve essere valutata volta per volta a causa della grande varietà di dispositivi che possono essere utilizzati.

III Esecuzione dell'upgrade di Sentinel

15 Esecuzione dell'upgrade del server Sentinel

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

   Per ulteriori informazioni sull'esecuzione del backup dei dati, consultare "Backup e ripristino dati" nella *NetIQ Sentinel 7.0.1 Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).

2. Scaricare la versione più recente del programma di installazione dal sito dei download di Novell (http://download.novell.com).

3. Effettuare il login come utente `root` al server in cui si desidera eseguire l'upgrade di Sentinel.

4. 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.

5. Passare alla directory in cui è stato estratto il file d'installazione.

6. Per eseguire l'upgrade di Sentinel, specificare il comando seguente:

   ```
   ./install-sentinel
   ```

7. 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.

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

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

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

10. (Condizionale) Per eseguire l'upgrade dei sistemi della Gestione servizi di raccolta, consultare Capitolo 17, "Esecuzione dell'upgrade della Gestione servizi di raccolta", a pagina 89.

11. (Condizionale) Per eseguire l'upgrade del sistema del motore di correlazione, consultare Capitolo 18, "Esecuzione dell'upgrade del motore di correlazione", a pagina 91.

16 Esecuzione dell'upgrade dell'applicazione Sentinel

Questa procedura descrive come eseguire l'upgrade dell'applicazione Sentinel e delle applicazioni Gestione servizi di raccolta e Motore di correlazione.

1. Eseguire il login all'applicazione Sentinel come utente in un ruolo amministrativo.
2. ***Se si desidera eseguire l'upgrade dell'applicazione Sentinel***, fare clic su *Applicazione* per avviare WebYaST.
3. ***Se si desidera eseguire l'upgrade di un'applicazione Gestione servizi di raccolta o Motore di correlazione***, specificare l'URL del computer in cui risiede l'applicazione Gestione servizi di raccolta o Motore di correlazione e usare la porta 54984 per avviare WebYaST.
4. Eseguire un backup della configurazione, quindi creare un'esportazione ESM.

   Per ulteriori informazioni sull'esecuzione del backup dei dati, consultare "Backup e ripristino dati" nella *NetIQ Sentinel 7.0.1 Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).
5. (Condizionale) Se non è già stato fatto, registrare l'applicazione per l'esecuzione automatica degli aggiornamenti.

   Per ulteriori informazioni, vedere Sezione 5.9, "Registrazione degli aggiornamenti", a pagina 54.

   Se non è stata registrata, viene visualizzato un avviso di colore giallo per indicare che l'applicazione non è registrata.
6. Per verificare se vi sono aggiornamenti disponibili, fare clic su *Aggiorna*.

   Gli aggiornamenti disponibili vengono visualizzati.
7. 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. Una volta completato l'upgrade, questo servizio deve essere riavviato manualmente.
8. Riavviare il servizio Sentinel mediante l'interfaccia Web.

   Per ulteriori informazioni, vedere Sezione 5.8, "Interruzione e avvio del server mediante l'interfaccia Web", a pagina 54.

17 Esecuzione dell'upgrade della Gestione servizi di raccolta

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

   Per ulteriori informazioni, consultare "Backing Up and Restoring Data" (Backup e ripristino dati) nella *NetIQ Sentinel 7.0.1 Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).
2. Eseguire il login all'interfaccia Web di Sentinel come un utente in un ruolo amministrativo.
3. Selezionare *Download*.
4. Fare clic su *Download del programma di installazione* nella sezione Programma di installazione della Gestione servizi di raccolta.

   Viene visualizzata una finestra contenente le opzioni per aprire o salvare il file del programma di installazione nel computer locale.
5. Salvare il file.
6. Copiare il file in un'ubicazione temporanea.
7. Estrarre i contenuti del file.
8. Eseguire lo script seguente:

   ./install-cm
9. Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo.

18 Esecuzione dell'upgrade del motore di correlazione

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

   Per ulteriori informazioni, consultare "Backing Up and Restoring Data" (Backup e ripristino dati) nella *NetIQ Sentinel 7.0.1 Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).
2. Eseguire il login all'interfaccia Web di Sentinel come un utente in un ruolo amministrativo.
3. Selezionare *Download*.
4. Fare clic su *Download del programma di installazione* nella sezione Programma di installazione del motore di correlazione.

   Viene visualizzata una finestra contenente le opzioni per aprire o salvare il file del programma di installazione nel computer locale.
5. Salvare il file.
6. Copiare il file in un'ubicazione temporanea.
7. Estrarre i contenuti del file.
8. Eseguire lo script seguente:

   ./install-ce
9. Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo.

19 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.

IV Migrazione

20 Scenari di migrazione supportati

Questa versione di Sentinel non supporta alcun scenario di migrazione. Anziché eseguire una migrazione o un upgrade, è necessario realizzare una nuova installazione di Sentinel. Tuttavia, tra breve verrà rilasciato uno strumento per eseguire la migrazione dei dati.

Per istruzioni sull'installazione, vedere il Capitolo 2, “Installazione di Sentinel”, a pagina 23.

21 Operazione successiva

Una volta installato Sentinel, esistono due guide che forniscono tutte le istruzioni necessarie per eseguirne la configurazione: la *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)* e la *NetIQ Sentinel 7.0.1 User Guide (Guida per l'utente di NetIQ Sentinel 7.0.1)*.

La guida all'amministrazione contiene informazioni sulla configurazione per attività che solo gli utenti amministratori sono autorizzati ad eseguire. Ad esempio:

- "Configurazione di utenti e ruoli"
- "Configurazione della memorizzazione dei dati"
- "Configurazione della raccolta di dati"
- "Ricerca e generazione di rapporti su eventi in ambienti distribuiti"

Per ulteriori informazioni relative a questi e ad altri task amministrativi, consultare la *NetIQ Sentinel 7.0.1 Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

Nella Guida per l'utente sono contenute le istruzione necessarie per eseguire i task in Sentinel. Ad esempio:

- "Ricerca di eventi"
- "Analisi di tendenze nei dati"
- "Generazione di rapporti"
- "Configurazione di incidenti"

Per ulteriori informazioni relative a questi e ad altri task dell'utente, consultare la *NetIQ Sentinel 7.0.1 User Guide* (Guida per l'utente di NetIQ Sentinel 7.0.1).

Sentinel, inoltre, può essere configurato per analizzare gli eventi, aggiungere i dati mediante le regole di correlazione, impostare le linee di base, configurare i workflow per intervenire sulle informazioni e molto altro ancora. Per configurare queste funzioni di Sentinel utilizzare le istruzioni contenute nella *NetIQ Sentinel 7.0.1 Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).

V Disinstallazione

Per disinstallare Sentinel, eseguire i task seguenti:

22 Disinstallazione di Sentinel

Per disinstallare Sentinel è disponibile uno script di disinstallazione. Alcuni file, inclusi i file di log, che vengono conservati, possono essere rimossi manualmente, se necessario. Prima di realizzare una nuova installazione, eseguire tutti i passaggi seguenti per assicurarsi che non rimanga alcun file o impostazione del sistema appartenente all'installazione precedente.

WARNING: Le istruzioni seguenti comportano la modifica dei file e delle impostazioni di sistema. Se non si ha familiarità con la modifica di queste impostazioni e file di sistema, rivolgersi all'amministratore del sistema.

22.1 Disinstallazione del server Sentinel

1. Eseguire il login al server di Sentinel come utente `root`.

   NOTE: Se l'installazione è stata eseguita come un utente `root`, non è possibile eseguire la disinstallazione del server Sentinel come utente non root. Tuttavia, se l'installazione è stata eseguita da un utente non root, questi può disinstallare il server Sentinel.

2. Accedere alla directory seguente:

   ```
   /opt/novell/sentinel/setup/
   ```

3. Eseguire il comando seguente:

   ```
   ./uninstall-sentinel
   ```

4. Quando richiesto di confermare nuovamente che si desidera continuare con la disinstallazione, premere s.

   Lo script prima interrompe il servizio, quindi lo rimuove completamente.

22.2 Disinstallazione della Gestione servizi di raccolta remota e del motore di correlazione

1. Eseguire il login come utente `root`.

   NOTE: Se l'installazione è stata eseguita come un utente `root`, non è possibile eseguire la disinstallazione di Gestione servizi di raccolta remota o Motore di correlazione remoto come un utente non root. Tuttavia, se l'installazione è stata eseguita da un utente non root, questi può eseguirne la disinstallazione.

2 Passare all'ubicazione seguente:

```
/opt/novell/sentinel/setup
```

3 Eseguire il comando seguente:

```
./uninstall-sentinel
```

Lo script visualizza un avviso in cui viene notificato che Gestione servizi di raccolta o Motore di correlazione sarà rimosso insieme a tutti i dati associati.

4 Immettere s per rimuovere la Gestione servizi di raccolta o il motore di correlazione.

Lo script prima interrompe il servizio, quindi lo rimuove completamente.

23 Task successivi alla disinstallazione

NOTE: La disinstallazione del server Sentinel non implica la rimozione dell'utente amministratore di Sentinel dal sistema operativo. Qualora si desideri rimuoverlo, l'operazione deve essere eseguita manualmente.

23.1 Rimozione delle impostazioni di sistema di Sentinel

Una volta disinstallato Sentinel, alcune impostazioni di sistema permangono. Prima di realizzare una nuova installazione di Sentinel, tali impostazioni devono essere rimosse, specialmente se durante la disinstallazione si sono verificati degli errori.

Per rimuovere manualmente le impostazioni di sistema di Sentinel:

1. Eseguire il login come utente `root`.
2. Verificare che tutti i processi di Sentinel siano stati interrotti.
3. Rimuovere i contenuti presenti in `/opt/novell/sentinel` od ovunque sia stato installato il software Sentinel.
4. Assicurarsi che nessun utente abbia effettuato il login come utente del sistema operativo amministratore di Sentinel (novell per default), quindi rimuovere l'utente, la home directory e il gruppo.

   ```
   userdel -r novell
   ```

   ```
   groupdel novell
   ```
5. Riavviare il sistema operativo.

23.1.1 Completamento della disinstallazione del motore di correlazione

Dopo aver eseguito lo script di disinstallazione per disinstallare il motore di correlazione, nell'interfaccia Web l'icona del motore di correlazione viene ancora visualizzata nello stato inattivo. Per eliminare manualmente il motore di correlazione dall'interfaccia Web, è necessario elaborare la seguente procedura aggiuntiva:

1. Accedere all'interfaccia Web di Sentinel come amministratore.
2. Espandere *Correlazione*, quindi selezionare il motore di correlazione che si desidera eliminare.
3. Fare clic sul pulsante *Elimina* (icona del cestino).

23.1.2 Completamento della disinstallazione della Gestione servizi di raccolta

Dopo aver eseguito lo script di disinstallazione per disinstallare la Gestione servizi di raccolta, nell'interfaccia Web l'icona di Gestione servizi di raccolta viene ancora visualizzata nello stato inattivo. Per eliminare manualmente la Gestione servizi di raccolta dall'interfaccia Web, è necessario elaborare la seguente procedura aggiuntiva:

1. Accedere a *Gestione origini eventi* > *Visualizzazione in diretta*.
2. Fare clic con il pulsante destro del mouse sulla Gestione servizi di raccolta che si desidera eliminare, quindi scegliere *Elimina*.