Sentinel™

Guida all'installazione e alla configurazione

Luglio 2018

Note legali

Informazioni sulla Guida e Libreria

La *Guida all'installazione e alla configurazione* contiene informazioni introduttive su Sentinel e istruzioni su come installare e configurare il prodotto.

Destinatari

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

Altre informazioni incluse nella raccolta di documentazione

La raccolta di documentazione contiene le risorse seguenti:

Guida all'amministrazione

Informazioni sulle operazioni di amministrazione e altri task da eseguire per la gestione di un'installazione di Sentinel.

Guida dell'utente

Informazioni concettuali su Sentinel. La guida include inoltre una panoramica delle interfacce utente e istruzioni dettagliate per svariati task.

Informazioni su Sentinel

In questa sezione sono descritte dettagliatamente le caratteristiche di Sentinel e il modo in cui questa soluzione consente di gestire gli eventi all'interno di un'azienda.

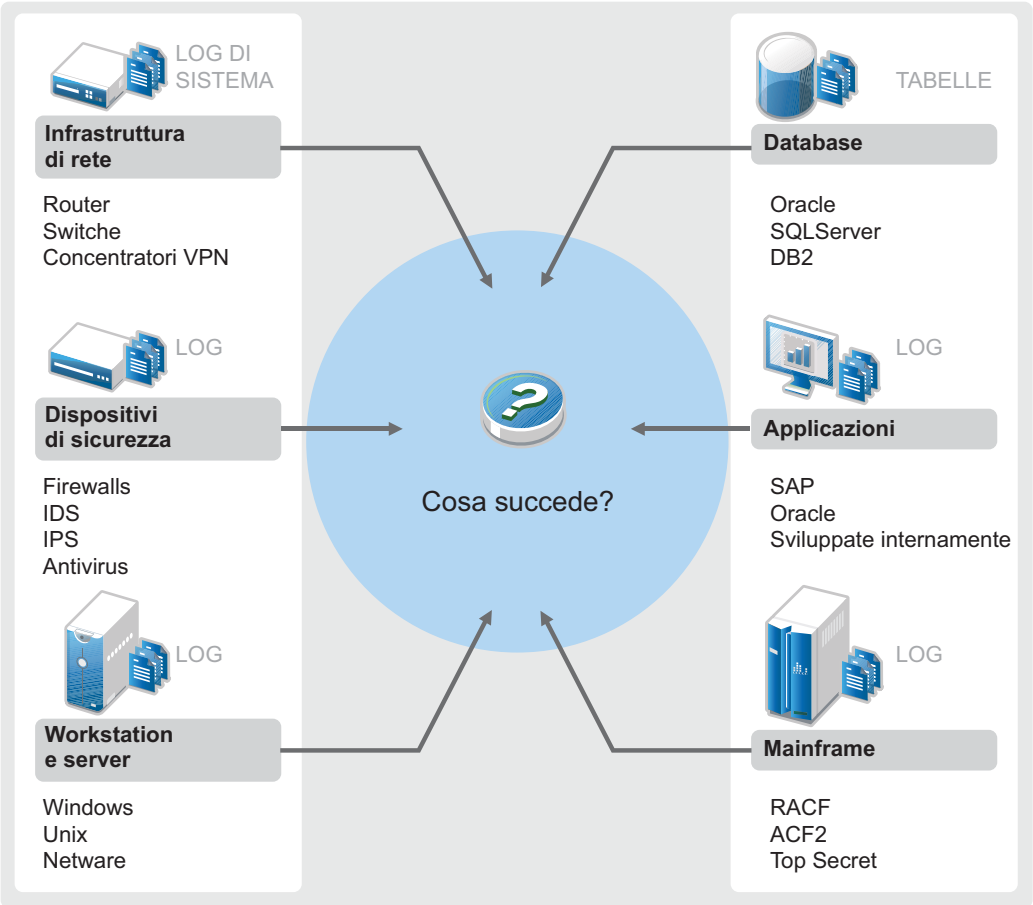
1 Cos'è Sentinel?

Sentinel è una soluzione SIEM (Security, Information and Event Management) e di monitoraggio della conformità. che monitora automaticamente gli ambienti IT più complessi e garantisce la sicurezza necessaria per proteggerli.

Sfide da affrontare per rendere sicuro l'ambiente IT

A causa della complessità che caratterizza gli ambienti IT, renderli sicuri è una vera e propria sfida. Generalmente, in un ambiente IT sono presenti molte applicazioni, database, mainframe, workstation e server e tutti generano log specifici degli eventi. A questi si aggiungono, inoltre, i dispositivi di sicurezza e quelli dell'infrastruttura di rete, ognuno dei quali fornisce log relativi agli eventi dell'ambiente IT.

Figura 1-1 *Eventi dell'ambiente IT*



Le soluzioni devono fornire una risposta efficace quando si verificano gli scenari seguenti:

- Nell'ambiente IT sono presenti numerosi dispositivi.
- I log sono in formati diversi.
- I log sono memorizzati in diverse ubicazioni.
- Il volume di informazioni acquisite nei file di log è molto elevato.
- Non è quindi possibile determinare i trigger degli eventi senza analizzare manualmente i file di log.

Per rendere utili le informazioni dei log è necessario eseguire le operazioni seguenti:

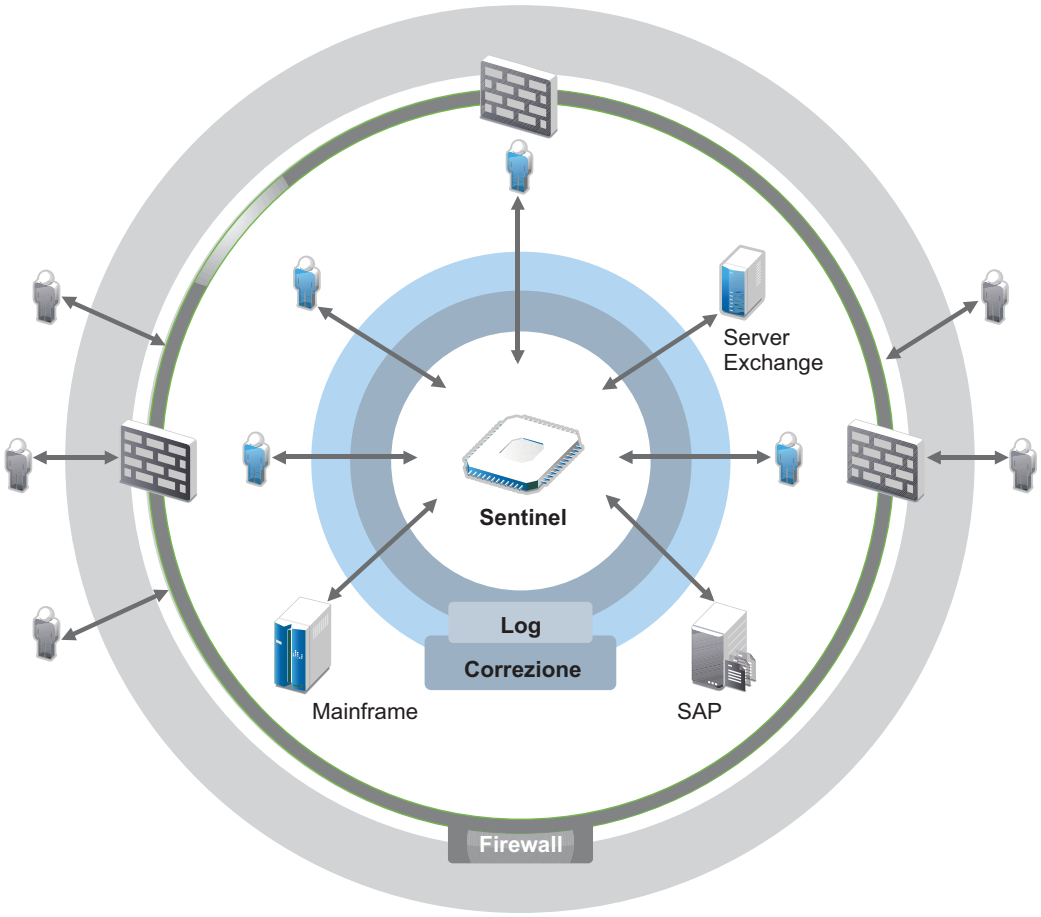
- Raccogliere i dati.
- Consolidare i dati.
- Standardizzazione di dati di tipo diverso in eventi facilmente confrontabili.
- Mappare gli eventi a normative standard.
- Analizzare i dati.
- Confrontare gli eventi di più sistemi per stabilire se sussistono problemi per la sicurezza.
- Inviare notifiche quando i dati non sono conformi alle norme previste.
- Avviare azioni a seguito delle notifiche, al fine di garantire la conformità alle policy aziendali.
- Generare rapporti per dimostrare la conformità.

Una volta comprese quali sono le operazioni critiche che devono essere realizzate per proteggere un ambiente IT, è necessario stabilire come rendere sicura l'azienda per gli utenti, ma anche come proteggerla da loro, senza comprometterne l'esperienza. Sentinel vi offre la soluzione.

La soluzione Sentinel

Sentinel funge da sistema nervoso centrale della sicurezza aziendale. Raccoglie i dati provenienti da tutta l'infrastruttura, vale a dire da applicazioni, database, server, dispositivi di memorizzazione e sicurezza, Consente di analizzare e mettere in correlazione i dati, automaticamente o manualmente, rendendoli più pratici.

Figura 1-2 *La soluzione Sentinel*



Grazie a Sentinel è possibile essere informati sugli eventi che si verificano nell'ambiente IT in un determinato momento ed è possibile collegare le azioni intraprese sulle risorse alle persone che le intraprendono. È così possibile conoscere i comportamenti degli utenti e monitorare efficacemente il controllo, onde prevenire eventuali attività dannose.

Sentinel raggiunge questi obiettivi grazie a:

- L'offerta di un'unica soluzione per gestire i controlli IT in funzione di normative diverse.
- La risoluzione del gap cognitivo fra ciò che le norme prevedono e quello che effettivamente avviene nell'ambiente IT.
- Il supporto adeguato che consente ai clienti di essere in linea con gli standard di sicurezza.
- Include programmi di monitoraggio della conformità e di reportistica pronti all'uso.

Sentinel automatizza i processi di raccolta log, analisi e generazione di rapporti per assicurare che i controlli IT siano in grado di supportare in modo efficace i requisiti di rilevamento e verifica delle minacce. Esegue il monitoraggio automatico degli eventi di sicurezza e di conformità e gestisce i controlli IT. Consente di intervenire tempestivamente qualora si produca una violazione alla sicurezza o un evento di non conformità. Sentinel permette inoltre di raccogliere informazioni di riepilogo relative all'ambiente, in modo da poterle condividere con le principali parti interessate.

2 Le funzioni di Sentinel

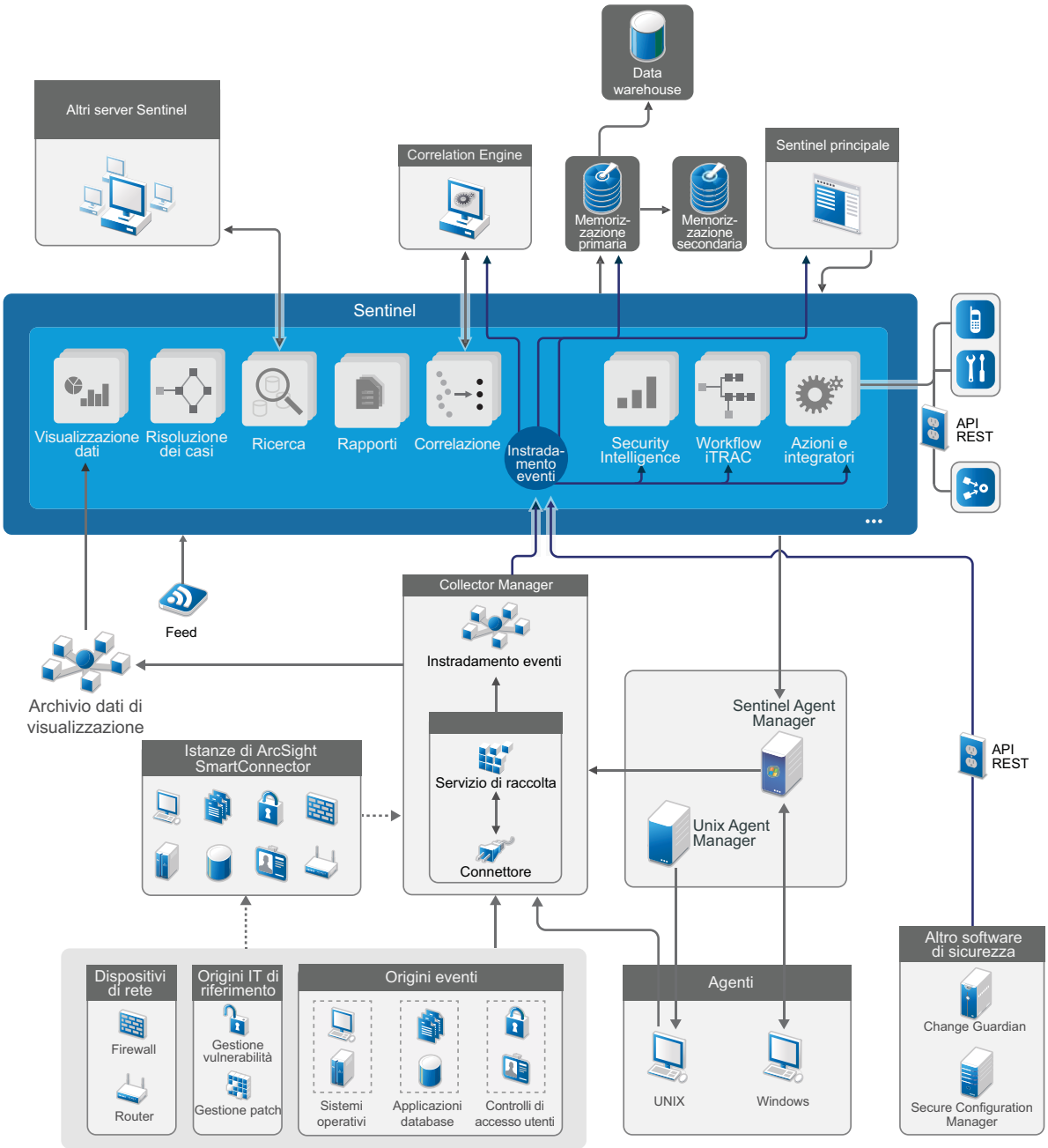
Sentinel gestisce costantemente le informazioni e gli eventi relativi alla sicurezza, sfruttando l'ambiente IT dell'utente per fornire una soluzione di monitoraggio completa.

Le funzioni di Sentinel sono:

- Raccolta di log, eventi e informazioni sulla sicurezza provenienti da tutte le diverse origini evento presenti nell'ambiente IT.
- Standardizzazione in un unico formato Sentinel di log, eventi e informazioni sulla sicurezza.
- Memorizzazione degli eventi in una memorizzazione dati basata su file o in una scalabile basata su Hadoop con policy di permanenza dei dati flessibili e personalizzabili.
- Raccolta di dati del flusso IP per facilitare il monitoraggio dettagliato delle attività di rete.
- Collegamento gerarchico di più sistemi Sentinel, incluso Sentinel Log Manager.
- Ricerca di eventi nel server Sentinel locale, ma anche in ulteriori server Sentinel situati in altre parti del mondo.
- Analisi statistica per definire una linea di base da mettere a confronto con quanto sta avvenendo, allo scopo di stabilire se esistono problemi che non sono stati ancora rilevati.
- Correlazione di un gruppo di eventi simili o confrontabili in un determinato periodo al fine di stabilire uno schema.
- Organizzazione degli eventi in incidenti ai fini della gestione delle risposte e del controllo.
- Rapporti basati sugli eventi in tempo reale e su quelli presenti nella cronologia.

Nella figura seguente è illustrato il funzionamento di Sentinel con la memorizzazione tradizionale come opzione di memorizzazione dati:

Figura 2-1 *Architettura di Sentinel*



Nelle sezioni seguenti si descrivono dettagliatamente i componenti di Sentinel:

- “Origini degli eventi” a pagina 21
- “Evento Sentinel” a pagina 21
- “Collector Manager” a pagina 23
- “ArcSight SmartConnectors” a pagina 24

Origini degli eventi

Sentinel raccoglie informazioni ed eventi relativi alla sicurezza da diverse origini all'interno dell'ambiente IT. Tali origini sono denominate origini degli eventi. Generalmente, quelle descritte di seguito sono le origini evento presenti in una rete:

Perimetro di sicurezza: Dispositivi di sicurezza, come hardware e software utilizzati per creare un perimetro di sicurezza dell'ambiente, come firewall, IDS (Intrusion Detective Systems, sistemi di rilevamento intrusioni) e VPN (Virtual Private Networks, reti virtuali private).

Sistemi operativi: Vari sistemi operativi in esecuzione nella rete.

Origini IT referenziali: software utilizzato per eseguire manutenzione e controllo di risorse, patch, configurazione e vulnerabilità.

Applicazioni: Varie applicazioni installate nella rete.

Controllo degli accessi degli utenti: applicazioni o dispositivi che consentono agli utenti di accedere alle risorse aziendali.

Per ulteriori informazioni sulla raccolta di eventi dalle origini evento, consultare “Collecting and Routing Event Data” (Raccolta e instradamento dei dati evento) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Evento Sentinel

Sentinel riceve le informazioni dai dispositivi, le normalizza in una struttura denominata evento che, successivamente, categorizza e invia per l'elaborazione.

Un evento rappresenta un record di log normalizzato segnalato a Sentinel da un dispositivo di sicurezza di terze parti, da un dispositivo di rete o in cui risiedono applicazioni, oppure da un'origine Sentinel interna. Esistono diversi tipi di eventi:

- Eventi esterni (ricevuti da un dispositivo di sicurezza), come ad esempio:
  - Un attacco rilevato da un sistema di rilevamento delle intrusioni (IDS)
  - Un login avvenuto correttamente segnalato da un sistema operativo
  - Una situazione definita dal cliente, ad esempio un utente che accede a un file

- Eventi interni (generati da Sentinel), fra i quali:
  - Una regola di correlazione disabilitata
  - Il riempimento del database

Sentinel aggiunge le informazioni di categoria (tassonomia) agli eventi, per semplificare il confronto degli eventi tra sistemi che li segnalano in modo diverso. Gli eventi vengono elaborati da Correlation Engine con visualizzazione in tempo reale, dai dashboard e dal server di back-end.

Un evento contiene oltre 200 campi. I campi evento sono di diverso tipo e vengono utilizzati per scopi diversi. Esistono alcuni campi predefiniti, ad esempio, quelli che fanno riferimento alla gravità, la criticità, l'indirizzo IP e la porta di destinazione.

Esistono due set di campi configurabili:

- Campi riservati: solo per uso interno di Sentinel, consentono espansioni future.
- Campi personalizzati: sono concepiti per permettere le personalizzazioni dei clienti.

L'origine di un campo può essere esterna o referenziale:

- Il valore di un campo esterno viene impostato esplicitamente dal dispositivo o dal servizio di raccolta corrispondente. Ad esempio, un campo può essere definito come il codice di costruzione della struttura contenente la risorsa menzionata come l'indirizzo IP di destinazione di un evento.
- Il valore di un campo referenziale viene calcolato come una funzione di uno o più campi diversi mediante il servizio di mappatura. Ad esempio, un campo può essere calcolato dal servizio di mappatura mediante una mappatura definita dal cliente che utilizza l'indirizzo IP di destinazione dell'evento.

- “Servizio di mappatura” a pagina 22
- “Streaming delle mappe” a pagina 23
- “Rilevamento degli exploit” a pagina 23

Servizio di mappatura

Il servizio di mappatura propaga i dati aziendali rilevanti nel sistema. Questi dati possono integrare gli eventi con informazioni referenziali.

L'utente può integrare i dati evento utilizzando le mappature per aggiungere ulteriori informazioni, quali i dettagli relativi a host e identità, agli eventi che vengono recuperati dai dispositivi di origine. Sentinel può utilizzare queste informazioni aggiuntive per realizzare correlazioni e generare rapporti avanzati. Sentinel supporta diverse mappature incorporate, oltre a quelle personalizzate definite dall'utente.

Le mappature definite in Sentinel vengono memorizzate in due modi:

- Le mappature incorporate sono memorizzate nel database, vengono aggiornate internamente ed esportate automaticamente nel servizio di mappatura.
- Le mappature personalizzate vengono memorizzate come file CSV e possono essere aggiornate sul file system o mediante la Map Data Configuration UI (interfaccia utente di configurazione dei dati di mappatura), per essere quindi caricate dal servizio di mappatura.

In entrambi i casi, i file CSV vengono conservati nel server Sentinel centrale ma le modifiche alle mappature sono distribuite a ciascuna istanza di Collector Manager e applicate localmente. Questa elaborazione distribuita assicura che l'attività di mappatura non sovraccarichi il server principale.

Streaming delle mappe

Il servizio di mappatura utilizza un modello di aggiornamento dinamico ed esegue lo streaming delle mappe da un punto all'altro, evitando la creazione di mappe statiche di grandi dimensioni nella memoria dinamica. Questa funzione è particolarmente efficace in un sistema in tempo reale mission-critical, come Sentinel, in cui è necessario uno spostamento di dati costante, prevedibile e veloce, indipendentemente da qualsiasi carico transitorio sul sistema.

Rilevamento degli exploit

Sentinel consente di creare riferimenti incrociati tra le firme dei dati relativi agli eventi e i dati della scansione delle vulnerabilità. Sentinel notifica automaticamente e immediatamente agli utenti quando si verifica un tentativo di exploit di una vulnerabilità. Sentinel realizza queste operazioni elaborando le funzioni seguenti:

- Feed di dati di Advisor
- rilevamento delle intrusioni
- scansione delle vulnerabilità
- Firewall

I feed di Advisor contengono informazioni relative alle vulnerabilità e alle minacce, oltre che una normalizzazione delle firme eventi e dei plug-in di vulnerabilità. Fornisce un riferimento incrociato tra le firme dei dati relativi agli eventi e i dati relativi alla scansione delle vulnerabilità. Per ulteriori informazioni sui feed di Advisor, consultare "Detecting Vulnerabilities and Exploits" (Rilevamento di vulnerabilità ed exploit) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Collector Manager

L'istanza di Collector Manager gestisce la raccolta dei dati, monitora i messaggi di stato del sistema ed esegue il filtraggio degli eventi. Le funzioni principali di Collector Manager sono:

- Raccolta di dati mediante l'utilizzo di connettori.
- Analisi sintattica e normalizzazione dei dati mediante l'utilizzo di connettori.

Servizi di raccolta

I servizi di raccolta raccolgono le informazioni dai connettori e li standardizzano. Elaborano le funzioni seguenti:

- Ricezione dei dati non elaborati dai servizi di raccolta.
- Analisi sintattica e normalizzazione dei dati:
  - Conversione dei dati specifici dell'origine evento in dati specifici di Sentinel.
  - Arricchimento degli eventi modificando le informazioni contenute in un formato leggibile da Sentinel.
  - Filtraggio degli eventi in base alle origini evento.
- Aggiunta di pertinenza aziendale agli eventi mediante il servizio di mappatura:
  - Mappatura degli eventi alle identità.
  - Mappatura degli eventi alle risorse.

- Instradamento degli eventi.
- Passaggio dei dati normalizzati, analizzati sintatticamente e formattati a Collector Manager.
- Invio di un messaggio di stato al server Sentinel.

Per ulteriori informazioni sui servizi di raccolta, consultare il sito Web dei plug-in di Sentinel.

Connettori

I connettori hanno la funzione di stabilire le connessioni fra le origini evento e il sistema Sentinel.

I connettori forniscono le funzionalità seguenti:

- Trasporto dei dati evento non elaborati dalle origini evento al servizio di raccolta.
- Filtraggio in base alla connessione.
- Connessione per la gestione degli errori.

ArcSight SmartConnectors

Sentinel utilizza ArcSight SmartConnector per raccogliere eventi da vari tipi di origini non direttamente supportate da Sentinel. Con SmartConnectors è possibile raccogliere eventi da dispositivi supportati, normalizzarli nel formato CEF (Common Event Format) e inoltrarli a Sentinel mediante il connettore Syslog. Quindi, il connettore inoltra gli eventi a Universal Common Event Format Collector per l'analisi sintattica.

Per ulteriori informazioni sulla configurazione di Sentinel con SmartConnectors, consultare la documentazione di Universal Common Event Format Collector sul sito Web dei plug-in di Sentinel.

Agent Manager

Con Agent Manager è possibile effettuare la raccolta di dati basata sull'host, complementando quella senza agenti, allo scopo di:

- Accedere ai log non disponibili sulla rete.
- Operare in ambienti di rete con un controllo rigido.
- Migliorare l'assetto di sicurezza per limitare la superficie di attacco nei server di importanza critica.
- Assicurare una maggiore affidabilità nella raccolta dati quando la rete non è disponibile..

Agent Manager consente di installare e gestire la configurazione degli agenti, oltre a fungere da punto di raccolta per gli eventi che confluiscono in Sentinel. Per ulteriori informazioni su Agent Manager, consultare la documentazione di Agent Manager.

Instradamento e memorizzazione dei dati in Sentinel

Sentinel fornisce numerose opzioni per instradare, memorizzare ed estrarre i dati raccolti. Per default, Sentinel riceve i dati evento analizzati sintatticamente e i dati non elaborati dalle istanze di Collector Manager. I dati non elaborati vengono memorizzati per fornire una catena di evidenze sicura, mentre i dati degli eventi analizzati sintatticamente vengono instradati in base alle regole definite dall'utente. È possibile filtrare i dati evento analizzati sintatticamente, memorizzarli o

analizzarli in tempo reale e instradarli verso sistemi esterni. Inoltre, Sentinel confronta tutti i dati degli eventi inviati alla memorizzazione con le policy di permanenza definite dall'utente, che controllano quando i dati degli eventi devono essere eliminati dal sistema.

In base alla frequenza degli eventi al secondo (EPS) e ai requisiti dell'installazione dell'utente, come opzione di memorizzazione dei dati è possibile scegliere fra la memorizzazione tradizionale basata su file e quella scalabile basata su Hadoop. Per ulteriori informazioni, consultare “Considerazioni sulla memorizzazione dei dati” a pagina 39.

Visualizzazioni degli eventi

In Sentinel sono ora disponibili visualizzazioni degli eventi che presentano i dati sotto forma di grafici, tabelle e mappe, per facilitare la visualizzazione e l'analisi di grandi volumi di eventi, inclusi quelli del flusso IP. È inoltre possibile creare visualizzazioni e dashboard personalizzati.

Le visualizzazioni degli eventi sono disponibili di default in Sentinel con la memorizzazione scalabile. Nelle configurazioni con memorizzazione tradizionale, le visualizzazioni degli eventi sono disponibili solo se è abilitato l'archivio dati di visualizzazione (Elasticsearch) per memorizzare e indicizzare i dati. Per ulteriori informazioni sull'abilitazione di Elasticsearch, vedere “Configurazione dell'archivio dati di visualizzazione” a pagina 43.

Correlazione

Anche se un evento singolo può risultare irrilevante, in combinazione con altri potrebbe avvisare della presenza di un problema potenziale. Sentinel consente di correlare questi eventi, utilizzando le regole create e implementate in Correlation Engine, e a intraprendere le azioni adeguate a contenere eventuali problemi.

Grazie alla correlazione, sono disponibili nuove funzioni di gestione degli eventi di sicurezza mediante l'automatizzazione dell'analisi del flusso di eventi in ingresso, che consente di individuare eventuali schemi di interesse. La correlazione consente di definire regole per l'identificazione di minacce critiche e modelli di attacco complessi, al fine di poter stabilire una priorità per gli eventi, nonché reagire e gestire i casi in modo efficace. Per ulteriori informazioni sulla correlazione, consultare “Correlating Event Data (Correlazione dei dati evento)” nella *Sentinel User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

Per monitorare gli eventi in base alle regole di correlazione, è necessario implementare le regole nell'istanza di Correlation Engine. Quando si verifica un evento che corrisponde ai criteri delle regole, l'istanza di Correlation Engine genera un evento di correlazione che descrive il modello. Per ulteriori informazioni, vedere “Correlation Engine” nella *Sentinel User Guide* (Guida dell'utente di NetIQ Sentinel 7.1).

Security Intelligence

La funzione di correlazione di Sentinel consente di cercare i modelli di attività noti, affinché possano essere analizzati per motivi di sicurezza, conformità o altro. La funzione Security Intelligence ricerca l'attività anomala e potenzialmente pericolosa, ma non confronta alcun modello noto.

La funzione Security Intelligence di Sentinel si concentra sull'analisi statistica dei dati relativi alla serie di orari, al fine di consentire agli analisti d'individuare e analizzare anomalie mediante un motore statistico automatico o la rappresentazione visiva dei dati statistici per un'interpretazione manuale. Per ulteriori informazioni, vedere “Analisi di tendenze nei dati” nella *Sentinel User Guide (Guida per l'utente di NetIQ Sentinel 7.0.1)*.

Contromisure per incidenti

Grazie alla gestione automatica delle risposte agli incidenti, Sentinel consente di documentare e formalizzare il processo di controllo, escalation e risposta ai casi e alle violazioni delle policy. Fornisce inoltre l'integrazione bidirezionale con sistemi di trouble-ticketing. Sentinel consente di reagire tempestivamente e risolvere i casi in modo efficiente. Per ulteriori informazioni, vedere "Configuring Incidents" (Configurazione dei casi) nella *Sentinel User Guide* (Guida dell'utente di NetIQ Sentinel 7.1).

Workflow iTRAC

I workflow iTRAC sono stati concepiti al fine di offrire una soluzione semplice e flessibile per l'automatizzazione e il controllo dei processi aziendali di risposta ai casi. iTRAC sfrutta il sistema interno dei casi di Sentinel per controllare la sicurezza o i problemi del sistema dall'identificazione, mediante regole di correlazione o identificazione manuale, fino alla risoluzione.

I workflow possono essere creati mediante una procedura manuale o automatizzata. I workflow iTrac supportano funzioni avanzate come la diramazione, escalation in base all'orario e variabili locali. L'integrazione con script e plug-in esterni consente l'interazione flessibile con sistemi di terze parti. I rapporti completi permettono agli amministratori di comprendere e ottimizzare i processi di risposta agli incidenti. Per ulteriori informazioni, vedere "Configuring iTRAC Workflows (Configurazione dei workflow di iTRAC)" in *Sentinel User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

Azioni e integratori

Le azioni eseguono manualmente o automaticamente alcune operazioni, come l'invio delle e-mail. Le azioni possono essere attivate da regole di instradamento, eseguendo manualmente un'operazione connessa a un evento o a un caso oppure da regole di correlazione. In Sentinel sono disponibili azioni preconfigurate. che è possibile riconfigurare secondo necessità oppure integrare con nuove azioni. Per ulteriori informazioni, vedere "Configuring Actions" (Configurazione delle azioni) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.1).

Un'azione può essere eseguita autonomamente oppure può utilizzare l'istanza di un integratore configurata dal relativo plug-in. I plug-in degli integratori ampliano funzioni e funzionalità delle azioni di correzione di Sentinel. Per eseguire un'azione, gli integratori consentono la connessione a un sistema esterno, ad esempio un server LDAP, SMTP o SOAP. Per ulteriori informazioni, vedere "Configuring Integrators" (Configurazione degli integratori) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.1).

Esecuzione di ricerche

In Sentinel è disponibile un'opzione per effettuare ricerche degli eventi. Con l'opportuna configurazione, è inoltre possibile effettuare ricerche degli eventi di sistema generati da Sentinel e visualizzare i dati non elaborati di ciascuno di essi. Per ulteriori informazioni, vedere "Viewing Events" (Visualizzazione degli eventi) nella *Sentinel User Guide* (Guida dell'utente di NetIQ Sentinel).

È possibile eseguire le ricerche anche in server Sentinel distribuiti in diverse ubicazioni geografiche. Per ulteriori informazioni, vedere "Configuring Data Federation" (Configurazione della federazione di dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Rapporti

Sentinel consente di eseguire rapporti sui dati raccolti e ha in dotazione diversi rapporti personalizzabili. Alcuni rapporti possono essere configurati e consentono di specificare le colonne da visualizzare nei risultati.

È possibile eseguire, pianificare e inviare via e-mail i rapporti in formato PDF. Tutti i rapporti possono inoltre essere eseguiti come una ricerca, per poi interagire con i risultati proprio come una qualsiasi ricerca, cioè perfezionandoli o eseguendo un'azione basata sui risultati recuperati. I rapporti possono anche essere eseguiti sui server Sentinel distribuiti in diverse ubicazioni geografiche. Per ulteriori informazioni, vedere “Reporting (Generazione di rapporti)” in *Sentinel User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

Controllo delle identità

In Sentinel è incluso un framework d'integrazione con i sistemi di gestione identità che permette di controllare le identità di ciascun account utente e gli eventi che esse hanno generato. Le informazioni fornite includono: dati di contatto, account utente, eventi d'autenticazione recenti, eventi di accesso recenti, modifiche delle autorizzazioni e così via. Grazie alla visualizzazione delle informazioni relative agli utenti che hanno inizializzato una determinata azione, Sentinel consente di migliorare i tempi di risposta ai casi e di elaborare analisi basate sul comportamento. Per ulteriori informazioni, vedere “Leveraging Identity Information” (Utilizzo delle informazioni sulle identità) nella *Sentinel User Guide* (Guida dell'utente di NetIQ Sentinel).

Analisi evento

Sentinel fornisce un potente set di strumenti che facilitano il reperimento e l'analisi di dati evento critici. Sentinel ottimizza il sistema in modo tale da assicurare la massima efficienza in qualsiasi tipo di analisi e consente, inoltre, di passare facilmente da un tipo di analisi a un altro, consentendo così transizioni più uniformi.

L'esame degli eventi in Sentinel spesso inizia con le viste eventi in tempo quasi reale. Sebbene siano disponibili molti altri strumenti avanzati, nelle viste eventi vengono visualizzati flussi di eventi filtrati insieme a grafici di riepilogo, che risultano particolarmente utili per effettuare analisi semplici e rapide delle tendenze e dei dati degli eventi e per identificare eventi specifici. Familiarizzando con il prodotto, l'utente sarà in grado di creare filtri configurati per classi specifiche di dati, come gli output provenienti dalla correlazione. Le viste eventi possono essere utilizzate come un dashboard, in cui viene visualizzato il comportamento complessivo a livello di sicurezza e operatività.

Successivamente, è possibile utilizzare la ricerca interattiva per elaborare analisi degli eventi più dettagliate. In questo modo, è possibile eseguire ricerche più rapide e semplici e trovare i dati relativi a determinate interrogazioni, come attività in base a un utente specifico o a un determinato sistema. Selezionando i dati evento o utilizzando il riquadro di ottimizzazione a sinistra, è possibile concentrarsi rapidamente su eventi particolarmente interessanti.

Durante l'analisi di centinaia di eventi, le funzioni di generazione di rapporti offerte da Sentinel forniscono un controllo personalizzato del layout degli eventi, consentendo la visualizzazione di ampi volumi di dati. Sentinel semplifica la realizzazione di questa transizione consentendo di trasferire le ricerche interattive, create nell'interfaccia di ricerca, in un modello di generazione di rapporti. In questo modo, viene immediatamente creato un rapporto nel quale sono visualizzati gli stessi dati, ma in un formato più adatto a contenere un numero elevato di eventi.

A tale scopo, Sentinel include numerosi modelli di generazione di rapporti. Esistono due tipi di modelli di generazione di rapporti:

- I modelli ottimizzati per la visualizzazione di tipi particolari di informazioni, come i dati di autenticazione o la creazione degli utenti.
- I modelli a carattere più generale, che consentono di personalizzare interattivamente i gruppi e le colonne del rapporto.

Familiarizzando con il prodotto, l'utente sarà in grado di sviluppare i filtri e i rapporti più comuni semplificando notevolmente i workflow. Sentinel supporta la memorizzazione di queste informazioni e le distribuisce a tutto il personale dell'azienda. Per ulteriori informazioni, vedere (Generazione di rapporti) *Sentinel User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

II Pianificazione dell'installazione di Sentinel

Nei capitoli seguenti vengono fornite le istruzioni per pianificare l'installazione di Sentinel. Se si desidera installare una configurazione non descritta nei capitoli seguenti o per eventuali chiarimenti, rivolgersi al supporto tecnico di .

3 Elenco di controllo per l'implementazione

Utilizzare l'elenco di controllo seguente per pianificare, installare e configurare Sentinel.

Se si esegue l'upgrade da una versione precedente di Sentinel, non utilizzare l'elenco di controllo. Per informazioni sulla procedura di upgrade, consultare Parte V, “Esecuzione dell'upgrade di Sentinel,” a pagina 147.

❒	Task	Vedere
❒	Esaminare le informazioni relative all'architettura del prodotto per acquisire familiarità con i componenti di Sentinel.	Parte I, “Informazioni su Sentinel,” a pagina 13.
❒	Esaminare le condizioni di licenza di Sentinel per stabilire se è necessario utilizzare la licenza di valutazione o quella aziendale.	Capitolo 4, “Informazioni sulla licenza”, a pagina 33.
❒	Analizzare l'ambiente in uso per stabilire la configurazione dell'hardware. Accertarsi che i computer in cui si installano Sentinel e i relativi componenti siano conformi ai requisiti specificati.	Capitolo 5, “Requisiti di sistema”, a pagina 37.
❒	Determinare il tipo di installazione idonea al proprio ambiente in base agli eventi al secondo (EPS). Stabilire il numero di istanze di Collector Manager e Correlation Engine che è necessario installare per migliorare le prestazioni e il bilanciamento del carico.	Capitolo 6, “Considerazioni sull'installazione”, a pagina 39.
❒	Esaminare le note sulla versione di Sentinel per disporre delle informazioni sulle nuove funzionalità e i problemi noti.	Note di rilascio di Sentinel
❒	Installare Sentinel.	Parte III, “Installazione di Sentinel,” a pagina 71.
❒	Configurare Sentinel.	Parte IV, “Configurazione di Sentinel,” a pagina 115.
❒	Sentinel dispone di regole di correlazione pronte all'uso. Alcune regole di correlazione sono configurate per default, in modo tale da eseguire un'azione che invii un'e-mail quando la regola viene attivata, come l'azione di notifica all'amministratore della sicurezza. È quindi necessario configurare il server di posta nel server Sentinel, configurando l'integratore SMTP e l'azione Invia e-mail.	Documentazione sull'integratore SMTP e l'azione Send Email sul sito Web dei plug-in di Sentinel.
❒	Installare i connettori e i servizi di raccolta in base alle esigenze del proprio ambiente.	Capitolo 16, “Installazione di servizi di raccolta e connettori aggiuntivi”, a pagina 111.
❒	Installare istanze aggiuntive di Collector Manager e Correlation Engine in base alle esigenze del proprio ambiente.	Parte III, “Installazione di Sentinel,” a pagina 71.

4 Informazioni sulla licenza

Sentinel contiene un'ampia gamma di funzionalità che soddisfano le più diverse esigenze di molti dei suoi clienti. È possibile scegliere il modello di licenza più adatto al proprio scenario aziendale.

La piattaforma Sentinel fornisce i due modelli di licenza seguenti:

- **Sentinel Enterprise:** una soluzione completa di tutte le funzioni per effettuare le principali analisi visive in tempo reale e dotata di numerose altre funzionalità. Sentinel Enterprise è incentrata sui casi di utilizzo SIEM, quali il rilevamento delle minacce, la segnalazione di avvisi e le soluzioni in tempo reale.
- **Sentinel for Log Management:** una soluzione per i casi di utilizzo connessi alla gestione dei log, quali la raccolta, la memorizzazione, le ricerche e i rapporti sui dati.

  Sentinel for Log Management costituisce un upgrade significativo rispetto alle funzionalità di Sentinel Log Manager 1.2.2, oltre al fatto che in alcuni casi sono state modificate parti significative dell'architettura. Per pianificare l'upgrade a Sentinel for Log Management, consultare la pagina delle domande frequenti di Sentinel.

In base alle soluzioni e ai componenti aggiuntivi scelti, è possibile acquistare le chiavi di licenza e le autorizzazioni appropriate per abilitare le funzionalità adeguate in Sentinel. Sebbene le chiavi di licenza e le autorizzazioni gestiscano l'accesso alle funzioni e ai download del prodotto, è necessario fare riferimento al contratto di acquisto e al Contratto di licenza con l'utente finale per consultare i termini e le condizioni addizionali.

Nella tabella seguente sono riportati i servizi e le funzioni specifici disponibili in ciascuna soluzione:

Tabella 4-1 *Servizi e funzioni di Sentinel*

Servizi e funzioni	Sentinel Enterprise	Sentinel for Log Management
Funzionalità principali	Sì	Sì
◆ Raccolta, analisi sintattica, normalizzazione e classificazione tassonomica degli eventi ◆ Raccolta di dati diversi dagli eventi (dati delle risorse, di vulnerabilità e di identità degli utenti) ◆ Mappatura contestuale in linea ◆ Memorizzazione degli eventi con policy di permanenza e di non rifiuto ◆ Instradamento degli eventi alla memorizzazione tradizionale (interna ed esterna) ◆ Ricerche e visualizzazione degli eventi ◆ Raccolta, memorizzazione e visualizzazione del flusso IP ◆ Generazione di rapporti ◆ Abilitazione di FIPS 140-2 (Federal Information Processing Standard Publication 140-2, Standard federale dell'elaborazione delle informazioni, pubblicazione 140-2) ◆ Azioni attivate manualmente ◆ Creazione e gestione manuali dei casi		
Collegamento Sentinel	Sì	Sì
Sincronizzazione dei dati	Sì	Sì
Ripristino dei dati degli eventi dall'archivio	Sì	Sì
Federazione di dati (ricerca distribuita)	Sì	Sì
Rilevamento exploit (Advisor)*	Sì	Sì
Memorizzazione scalabile	Sì	Sì
Correlazione	Sì	No
◆ Correlazione di modelli degli eventi in tempo reale ◆ Azioni attivate da regole di correlazione ◆ Valutazione degli avvisi ◆ Visualizzazione degli avvisi		
Security Intelligence	Sì	No
◆ Regole di anomalie ◆ Analisi statistica in tempo reale		

*Advisor di Security Nexus è un servizio aggiuntivo. Per utilizzare il servizio è necessario acquistare una licenza aggiuntiva.

Licenze di Sentinel

In questa sezione vengono fornite informazioni sui tipi di licenza di Sentinel.

Licenza di valutazione

La licenza di valutazione di default consente di utilizzare tutte le funzioni di Sentinel Enterprise per un periodo di valutazione specifico con un valore EPS illimitato in base alla capacità dell'hardware in uso. Per informazioni sulle funzioni disponibili in Sentinel Enterprise, vedere la Tabella 4-1, “Servizi e funzioni di Sentinel”, a pagina 34.

La data di scadenza del sistema si basa sui dati più vecchi presenti nel sistema. Se nel sistema viene eseguito il ripristino di eventi relativi a date precedenti, Sentinel aggiorna di conseguenza la data di scadenza.

Quando la licenza di valutazione scade, Sentinel viene eseguito con una licenza base gratuita che abilita un numero limitato di funzioni e una frequenza eventi limitata a 25 EPS. Questa indicazione è valida solo se Sentinel è configurato con la memorizzazione tradizionale.

Nelle installazioni con memorizzazione scalabile, quando la licenza di valutazione scade, gli eventi e i dati non elaborati non vengono più memorizzati.

Quando si esegue l'upgrade a una licenza aziendale, vengono ripristinate tutte le funzionalità di Sentinel. Onde evitare la possibile interruzione di alcune funzionalità, è necessario eseguire l'upgrade del sistema a una licenza aziendale prima della scadenza della licenza di valutazione.

Licenza gratuita

La licenza gratuita consente l'utilizzo di un numero limitato di funzioni e una frequenza eventi limitata a 25 EPS. È valida solo per Sentinel con memorizzazione tradizionale.

La licenza gratuita consente di raccogliere e memorizzare gli eventi. Quando la frequenza eventi supera il valore di 25 EPS, gli eventi ricevuti vengono memorizzati ma nei risultati delle ricerche e nei rapporti non vengono visualizzati i relativi dettagli. Tali eventi vengono contrassegnati con il tag `OverEPSLimit`.

La licenza gratuita non include funzionalità in tempo reale. Eseguendo l'upgrade a una licenza aziendale è possibile ripristinare tutte le funzioni.

Nota: per la versione gratuita di Sentinel non sono disponibili il supporto tecnico e gli aggiornamenti del prodotto.

Licenze aziendali

Al momento dell'acquisto di Sentinel, viene ricevuta una chiave di licenza tramite il portale clienti. In base alla licenza acquistata, la chiave di licenza abilita alcune funzionalità, frequenze di raccolta dati e origini evento. Poiché potrebbero esservi ulteriori termini di licenza che non vengono applicati dalla chiave, si consiglia di leggere attentamente il contratto di licenza.

Per modificare la licenza, contattare il responsabile dell'account.

È possibile aggiungere la chiave della licenza aziendale sia durante l'installazione che successivamente in qualsiasi altro momento. Per aggiungere la chiave di licenza, consultare “Adding a License Key” (Aggiunta di una chiave di licenza) nella *Sentinel Administration Guide (Guida all'amministrazione di NetIQ Sentinel).*

5 Requisiti di sistema

L'implementazione di Sentinel può variare a seconda delle esigenze dell'ambiente IT, pertanto, prima di finalizzare l'architettura è necessario rivolgersi ai servizi Consulting o a un partner Sentinel.

Per informazioni sull'hardware consigliato, i sistemi operativi supportati, le piattaforme dell'applicazione e i browser, vedere il sito Web delle informazioni tecniche di Sentinel.

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 sul sito Web dei plug-in di Sentinel.

Ambiente virtuale

Sentinel è supportato su server VMware ESX. Quando viene configurato un ambiente virtuale, le macchine virtuali devono disporre di una o più CPU. Per ottenere in ESX, o in qualsiasi altro ambiente virtuale, prestazioni paragonabili ai risultati ottenuti nelle prove effettuate su computer fisici, memoria, CPU, spazio su disco e I/O dell'ambiente virtuale devono essere uguali a quelli consigliati per i computer fisici.

Per informazioni relative al computer fisico consigliato, consultare il sito Web della documentazione tecnica di Sentinel.

6 Considerazioni sull'installazione

L'architettura di Sentinel è scalabile è può essere ampliata in modo da gestire il carico necessario. In questo capitolo sono riportate le principali considerazioni da effettuare al fine di definire la scala dell'installazione di Sentinel. Per progettare il sistema Sentinel adatto al proprio ambiente IT, è possibile avvalersi di personale qualificato del supporto tecnico di o dei servizi partner di .

Considerazioni sulla memorizzazione dei dati

Per memorizzare e indicizzare i dati di Sentinel, è possibile scegliere, in base alla frequenza EPS, se utilizzare la memorizzazione tradizionale o la memorizzazione scalabile. Il tipo di installazione di Sentinel dipende dall'opzione di memorizzazione che si intende utilizzare.

Tabella 6-1 *Confronto tra memorizzazione tradizionale e memorizzazione scalabile*

Memorizzazione tradizionale	Memorizzazione scalabile
I dati vengono memorizzati di default nella memorizzazione tradizionale basata su file e l'indicizzazione viene eseguita in locale nel server Sentinel. Oltre alla memorizzazione dati basata su file, è possibile scegliere di memorizzare e indicizzare gli eventi nell'archivio dati di visualizzazione per sfruttare le funzionalità di visualizzazione dei dati. Per ulteriori informazioni, consultare “Configurazione dell'archivio dati di visualizzazione” a pagina 43.	I dati vengono memorizzati nella memorizzazione scalabile basata su Hadoop e per l'indicizzazione si utilizza un meccanismo scalabile distribuito.
È facilmente scalabile in verticale fino a circa 20000 EPS. Per ottenere EPS molto più elevati, è necessario aggiungere ulteriori server Sentinel.	È facilmente scalabile in orizzontale fino a EPS molto elevati, ad esempio 1 milione di eventi al secondo.
La raccolta dei dati è bilanciata in base al carico fra vari server Sentinel. Di conseguenza, i dati vengono distribuiti su diversi server Sentinel e devono essere gestiti singolarmente.	La raccolta dei dati viene gestita da un solo server Sentinel. Di conseguenza, la gestione di dati e risorse è centralizzata in un solo server Sentinel.
I dati vengono contrassegnati in base ai tenant, ma su disco non vengono suddivisi in base a tale criterio.	I dati vengono contrassegnati e suddivisi in base ai tenant su disco.
La replica dei dati e la disponibilità devono essere eseguite manualmente o tramite costosi meccanismi di memorizzazione, ad esempio dischi SAN.	Disponibilità e replica dei dati sono economicamente convenienti poiché Hadoop viene eseguito su hardware standard.

- “Pianificazione per la memorizzazione tradizionale” a pagina 41
- “Pianificazione per la memorizzazione scalabile” a pagina 44
- “Struttura delle directory di Sentinel” a pagina 46

Pianificazione per la memorizzazione tradizionale

La memorizzazione dati basata su file è strutturata su tre livelli:

Memorizzazione online	Memorizzazione primaria, in precedenza denominata memorizzazione locale.	ottimizzata per scrittura e recupero rapidi. Vengono memorizzati i dati degli ultimi eventi raccolti e quelli su cui vengono effettuate ricerche con maggiore frequenza.
	Memorizzazione secondaria, in precedenza denominata memorizzazione in rete. (facoltativo).	Ottimizzata per ridurre l'utilizzo dello spazio o, in alternativa, memorizzazione a costi inferiori che supporta comunque il recupero rapido. In Sentinel viene eseguita la migrazione automatica delle partizioni dei dati nella memorizzazione secondaria.
	Nota: l'utilizzo della memorizzazione secondaria è facoltativo. Le policy di conservazione dei dati, le ricerche e i rapporti vengono eseguiti sulle partizioni dei dati degli eventi a prescindere dal fatto che risiedano nella memorizzazione primaria, secondaria o in entrambe.	
Memorizzazione offline	Memorizzazione di archiviazione	Quando le partizioni vengono chiuse, è possibile eseguirne il backup su qualsiasi servizio di memorizzazione file, come Amazon Glacier. È possibile importare di nuovo temporaneamente le partizioni affinché possano essere utilizzate ogni volta che risulti necessario, ad esempio durante analisi forensi a lungo termine.

Infine, è possibile configurare Sentinel per l'estrazione dei dati e dei riepiloghi degli eventi in un database esterno utilizzando le policy di sincronizzazione. Per ulteriori informazioni, vedere "Configurazione della sincronizzazione dei dati" nella *Sentinel Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

Quando si installa Sentinel, montare la partizione del disco per la memorizzazione primaria nell'ubicazione in cui è installato Sentinel; di default la directory `/var/opt/novell`.

Affinché i calcoli di utilizzo del disco vengano eseguiti correttamente, l'intera struttura della directory `/var/opt/novell/sentinel` deve risiedere su una partizione con un solo disco. In caso contrario, le funzionalità automatiche di gestione dei dati potrebbero eliminare prematuramente alcuni dati degli eventi. Per ulteriori informazioni sulla struttura delle directory di Sentinel, vedere il "Struttura delle directory di Sentinel" a pagina 46.

Come best practice, questa directory deve essere ubicata in una partizione diversa da quella in cui risiedono i file eseguibili, di configurazione e del sistema operativo. La memorizzazione in una partizione separata dei dati variabili facilita il backup di set di file e il recupero in caso di danneggiamento, oltre a garantire maggiore solidità in caso di riempimento di una partizione del disco. 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.

Nota: Per i file system ext3 sussiste una limitazione relativa alla memorizzazione dei file, che impedisce a una directory di contenere più di 32000 file o sottodirectory. Qualora si preveda di avere un numero elevato di policy di permanenza o si intenda conservare i dati per lunghi periodi di tempo, ad esempio per un anno, è possibile utilizzare il file system XFS.

- "Utilizzo delle partizioni in installazioni tradizionali" a pagina 42
- "Utilizzo delle partizioni in installazioni in modalità applicazione" a pagina 42

- “Best practice per il layout delle partizioni” a pagina 42
- “Configurazione dell'archivio dati di visualizzazione” a pagina 43

Utilizzo delle partizioni in installazioni tradizionali

Nelle installazioni tradizionali è possibile modificare il layout della partizione del disco riservata al sistema operativo prima di installare Sentinel. L'amministratore deve creare e montare le partizioni desiderate nelle directory appropriate, in base alla struttura delle directory descritta in “Struttura delle directory di Sentinel” a pagina 46. Quando si esegue il programma di installazione, Sentinel viene installato nelle directory già predisposte, espandendosi in più partizioni.

Nota:

- Durante l'esecuzione del programma di installazione è possibile utilizzare l'opzione `--location` per specificare un'ubicazione di livello superiore 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`.

Utilizzo delle partizioni in installazioni in modalità applicazione

Se si utilizza il formato applicazione ISO DVD, è possibile configurare il partizionamento del filesystem dell'applicazione durante l'installazione seguendo le istruzioni visualizzate nelle schermate di YaST. Ad esempio, è possibile creare una partizione separata per il punto di montaggio `/var/opt/novell/sentinel` e collocare tutti i dati nella partizione separata. Per gli altri formati dell'applicazione è possibile configurare il partizionamento solo dopo l'installazione. Mediante lo strumento SuSE YaST di configurazione del sistema si possono aggiungere partizioni e spostare una directory in una nuova partizione. Per informazioni sulla creazione di partizioni dopo l'installazione, vedere la “Creazione di partizioni per la memorizzazione tradizionale” a pagina 107.

Best practice per il layout delle partizioni

Numerose organizzazioni utilizzano schemi specifici e documentati come best practice di layout delle partizioni dei sistemi installati. La proposta seguente relativa alle partizioni può essere utilizzata come linea guida dalle organizzazioni che non hanno una policy definita e si basa sull'utilizzo specifico che Sentinel fa del file system. In linea generale Sentinel è conforme allo standard FHS (Filesystem Hierarchy Standard) ove applicabile.

Partizione	Punto di montaggio	Dimensioni	Note
Radice	`/`	100 GB	Vi risiedono i file del sistema operativo e quelli binari/di configurazione di Sentinel.
Avvio	`/boot`	150 MB	Partizione di avvio

Partizione	Punto di montaggio	Dimensioni	Note
Memorizzazione primaria	`/var/opt/novell/sentinel`	Eseguire il calcolo utilizzando le informazioni sulle dimensioni del sistema.	In questa area risiedono i dati primari raccolti da Sentinel e altri dati variabili come i file di log. Questa partizione può essere condivisa con altri sistemi.
Memorizzazione secondaria	Ubicazione che dipende dal tipo di memorizzazione, NFS, CIFS o SAN.	Eseguire il calcolo utilizzando le informazioni sulle dimensioni del sistema.	Area della memorizzazione secondaria che può essere montata localmente come mostrato o in remoto.
Memorizzazione di archiviazione	Sistema remoto	Eseguire il calcolo utilizzando le informazioni sulle dimensioni del sistema.	Questa memorizzazione è riservata ai dati archiviati.

Configurazione dell'archivio dati di visualizzazione

In Sentinel sono ora disponibili visualizzazioni degli eventi che presentano i dati sotto forma di grafici, tabelle e mappe, per facilitare la visualizzazione e l'analisi di grandi volumi di eventi. È inoltre possibile creare visualizzazioni e dashboard personalizzati.

Sentinel utilizza Kibana, un dashboard di ricerca e analisi basato su browser che consente di cercare e visualizzare gli eventi. Kibana accede ai dati dall'archivio dati di visualizzazione (Elasticsearch) per presentare gli eventi nei dashboard. Sentinel include di default un nodo Elasticsearch in cui vengono memorizzati e indicizzati solo gli avvisi. Per memorizzare e indicizzare gli eventi in Elasticsearch è necessario abilitare la visualizzazione degli eventi.

Quando si abilita Elasticsearch per la memorizzazione e l'indicizzazione dei dati, in Sentinel vengono indicizzati solo alcuni campi evento specifici necessari per le visualizzazioni e i campi indicizzati vengono memorizzati in Elasticsearch. In Sentinel viene creato un apposito indice quotidiano e per calcolare la data d'indicizzazione si utilizza il fuso orario UTC (mezzanotte-mezzanotte). Il nome dell'indice è nel formato `security.events.normalized_aaaaMMgg`. Ad esempio, l'indice `security.events.normalized_20160101` contiene tutti gli eventi con EventTime 01 gennaio 2016.

La configurazione dell'archivio dati di visualizzazione comporta quanto segue:

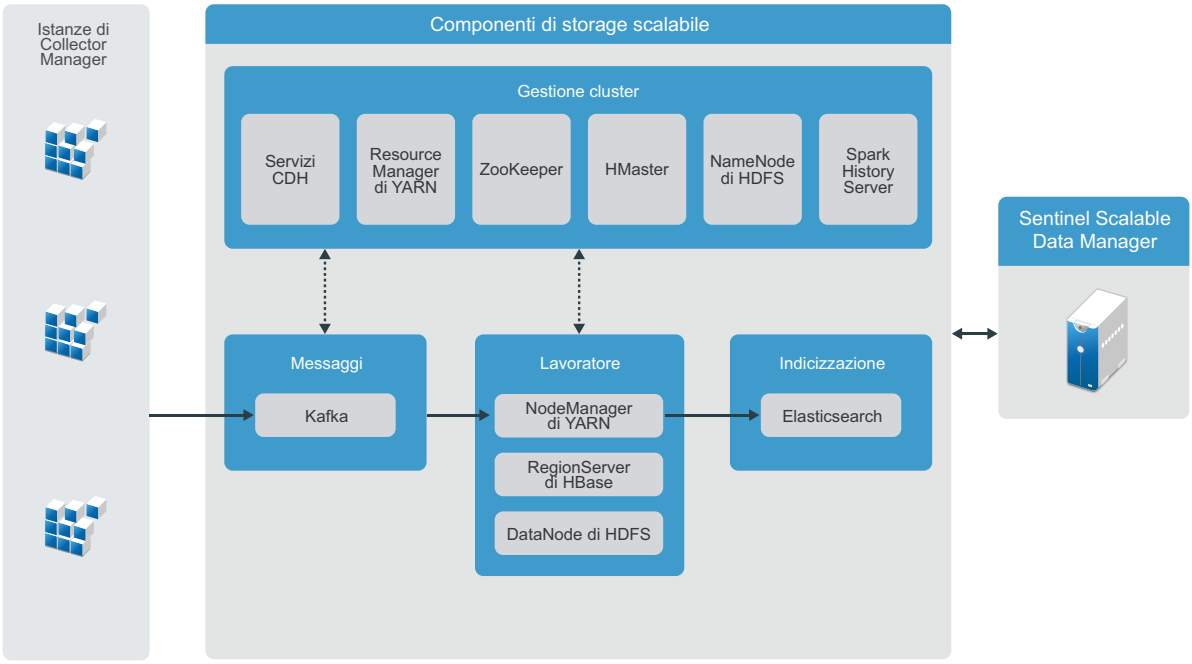
- **Installazione di nodi Elasticsearch in modalità cluster:** Sentinel include di default un nodo Elasticsearch. Per ottimizzare le prestazioni e la stabilità del server Sentinel, è necessario installare altri nodi Elasticsearch in modalità cluster. Per ulteriori informazioni, consultare Capitolo 12, “Installazione e configurazione di Elasticsearch”, a pagina 77.
- **Abilitazione della visualizzazione degli eventi:** la visualizzazione degli eventi è disabilitata di default. Per abilitare la visualizzazione degli eventi, vedere Capitolo 20, “Abilitazione della visualizzazione degli eventi”, a pagina 125.
- **Ottimizzazione delle prestazioni:** in Sentinel vengono configurate automaticamente alcune impostazioni di Elasticsearch per ottenere prestazioni ottimali. Tali impostazioni possono essere personalizzate in base alle proprie esigenze. Ad esempio, è possibile modificare i campi evento che si desidera indicizzare tramite Elasticsearch. Per ulteriori informazioni, consultare “Ottimizzazione delle prestazioni di Elasticsearch” a pagina 83.

Pianificazione per la memorizzazione scalabile

Per la memorizzazione e la gestione di grandi volumi di dati, Sentinel utilizza il framework CDH (Cloudera's Distribution Including Apache Hadoop). Per l'indicizzazione degli eventi, Sentinel utilizza un motore di indicizzazione scalabile e distribuito denominato Elasticsearch e sviluppato da Elastic.

Nella figura seguente sono illustrati i vari componenti utilizzati nella memorizzazione scalabile:

Figura 6-1 *Architettura della memorizzazione scalabile*



- **Messaggistica:** Sentinel utilizza Apache Kafka come sistema di messaggistica scalabile che riceve eventi normalizzati e dati non elaborati dalle istanze di Collector Manager. Le istanze di Collector Manager inviano i dati non elaborati e i dati degli eventi ai cluster Kafka.

  Per default, in Sentinel vengono creati gli argomenti Kafka seguenti:

  - **security.events.normalized:** memorizza tutti i dati degli eventi elaborati e normalizzati, inclusi quelli generati dal sistema e quelli interni.
  - **security.events.raw:** memorizza tutti i dati non elaborati provenienti dalle origini eventi.

  Eventi e dati non elaborati seguono lo schema Avro Apache. Per ulteriori informazioni, vedere la documentazione di Apache Avro. I file dello schema sono disponibili nella directory `/etc/opt/novell/sentinel/scalablestore`.

- **Dipendente:** in questo nodo vengono ospitati lavori di storage ed elaborazione in tempo reale. Apache Spark effettua l'elaborazione in tempo reale di grandi quantità di dati, come la suddivisione degli eventi in base agli ID dei tenant, la richiesta di grossi volumi di dati e la loro memorizzazione in un sistema di record (SOR), nonché l'indicizzazione scalabile.

  Apache HBase è un archivio dati distribuito e scalabile basato su Hadoop. Viene utilizzato come SOR per gli eventi normalizzati e i dati non elaborati, suddivisi in base agli ID dei tenant.

Utilizzando l'ID del tenant, in Sentinel viene creato uno spazio dei nomi separato per ciascun tenant. Ad esempio, lo spazio dei nomi per il tenant di default è 1. In ogni spazio dei nomi, Sentinel crea le tabelle seguenti e memorizza i dati in base all'orario degli eventi.

- ***<ID_tenant>*:security.events.normalized:** memorizza tutti i dati degli eventi elaborati e normalizzati, inclusi quelli generati dal sistema e quelli interni.
- ***<ID_tenant>*:security.events.raw:** memorizza tutti i dati non elaborati provenienti dalle origini eventi.

- **Gestione cluster:** in questo nodo sono ospitati tutti i servizi master e di gestione del cluster. Apache ZooKeeper funge da servizio centralizzato per la manutenzione delle informazioni di configurazione, i servizi di denominazione, la sincronizzazione distribuita e l'erogazione dei servizi di gruppo.
- **Indicizzazione:** Sentinel utilizza Elasticsearch come motore di indicizzazione scalabile e distribuito per gli eventi di indicizzazione. Per cercare e visualizzare gli eventi, è possibile accedere ai dati provenienti da Elasticsearch.

  In Sentinel viene creato un apposito indice quotidiano e per calcolare la data d'indicizzazione si utilizza il fuso orario UTC (mezzanotte-mezzanotte). Il nome dell'indice è nel formato `security.events.normalized_aaaaMMgg`. Ad esempio, l'indice `security.events.normalized_20160101` contiene tutti gli eventi con EventTime 01 gennaio 2016. Per garantire prestazioni ottimali, in Sentinel vengono indicizzati solo alcuni campi di eventi specifici. È possibile modificare i campi degli eventi che si desidera indicizzare tramite Elasticsearch. Per ulteriori informazioni, consultare “Ottimizzazione delle prestazioni di Elasticsearch” a pagina 83.

Configurazione della memorizzazione scalabile

Quando si abilita la memorizzazione scalabile, l'interfaccia utente del server Sentinel viene ridotta in modo da consentire soltanto alcune funzionalità, quali la raccolta dati, la correlazione e l'instradamento degli eventi, la ricerca e la visualizzazione degli eventi, nonché alcune attività di amministrazione. Questa versione ridotta di Sentinel è denominata Sentinel Scalable Data Manager (SSDM). Per le altre funzionalità di Sentinel, quali Security Intelligence e le normali funzioni di ricerca e generazione di rapporti, è necessario installare istanze separate di Sentinel con la memorizzazione tradizionale e instradare i dati specifici degli eventi da SSDM a Sentinel utilizzando Collegamento Sentinel.

Nell'elenco seguente vengono fornite informazioni sui servizi e le funzionalità non disponibili in SSDM:

- Rapporti
- Security Intelligence
- Esecuzione di operazioni evento
- Prova delle regole di correlazione
- Creazione e gestione dei casi
- Esecuzione manuale di azioni su eventi
- Sincronizzazione dei dati
- Workflow iTRAC
- Analisi forense sugli eventi che attivano l'evento correlato
- Visualizzazione di allegati evento per eventi Secure Configuration Manager e Change Guardian

L'abilitazione della memorizzazione scalabile è una configurazione che si esegue una sola volta e non può essere ripristinata. Per disabilitare la memorizzazione scalabile e passare alla memorizzazione tradizionale, è necessario reinstallare Sentinel.

Nell'elenco di controllo seguente sono riportate le informazioni generali sui task che è necessario eseguire per configurare la memorizzazione scalabile:

Tabella 6-2 *Elenco di controllo per la configurazione della memorizzazione scalabile*

	Task	Vedere
❒	Riesaminare le informazioni sull'installazione per verificare le operazioni da eseguire per installare Sentinel con la memorizzazione scalabile.	“Installazione su tre livelli con memorizzazione scalabile” a pagina 51
❒	Riesaminare i prerequisiti ed effettuare tutti i task necessari.	Capitolo 13, “Installazione e configurazione della memorizzazione scalabile”, a pagina 87.
❒	Abilitare la memorizzazione scalabile. È possibile abilitare la memorizzazione scalabile sia durante che dopo l'installazione.	Per abilitare la memorizzazione scalabile durante l'installazione, eseguire un'installazione personalizzata di Sentinel. Vedere “Installazione personalizzata del server Sentinel” a pagina 92.
	Nelle installazioni di upgrade, la memorizzazione scalabile può essere abilitata solo dopo aver eseguito l'upgrade di Sentinel.	Per abilitare la memorizzazione scalabile dopo l'installazione o dopo l'upgrade, vedere Enabling Scalable Storage Post-Installation (Abilitazione della memorizzazione scalabile dopo l'installazione) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).
❒	Configurare i componenti di CDH ed Elasticsearch con Sentinel.	Configuring Scalable Storage (Configurazione della memorizzazione scalabile) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Struttura delle directory di Sentinel

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 risiedono nella directory `/opt/novell/sentinel.`
- I file di log risiedono nella directory·`/var/opt/novell/sentinel/log`.
- I file temporanei risiedono nella directory·`/var/opt/novell/sentinel/tmp`.
- I file di configurazione risiedono nella directory `/etc/opt/novell/sentinel`.
- Il file ID di processo (PID) risiede nella directory `/home/novell/sentinel/server.pid`.

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

Vantaggi delle installazioni distribuite

Nel server Sentinel sono inclusi di default i componenti seguenti:

- **Collector Manager:** flessibile punto di raccolta dei dati utilizzato da Sentinel.

- **Correlation Engine:** elabora gli eventi contenuti nel flusso in tempo reale per stabilire se devono attivare una o più delle regole di correlazione.
- **Elasticsearch:** componente opzionale per memorizzare e indicizzare i dati. Sentinel include di default un nodo Elasticsearch. Se si prevede un elevato numero di EPS, superiore, ad esempio, ai 2500, è necessario installare nodi Elasticsearch aggiuntivi in un cluster.

Importante: per gli ambienti di produzione, si consiglia di configurare un'installazione distribuita poiché consente di raggruppare i componenti di raccolta dati in un computer separato, permettendo così di gestire picchi e altre anomalie preservando la massima stabilità del sistema.

In questa sezione sono descritti i vantaggi delle installazioni distribuite.

- "Vantaggi apportati dalla presenza di più istanze di Collector Manager" a pagina 47
- "Vantaggi derivanti dall'uso di istanze aggiuntive di Correlation Engine" a pagina 48

Vantaggi apportati dalla presenza di più istanze di Collector Manager

Nel server Sentinel è inclusa di default un'istanza di Collector Manager. Tuttavia, negli ambienti di produzione le istanze distribuite di Collector Manager garantiscono un migliore isolamento in caso di ricezione di grandi quantità di dati. Con questa configurazione, una delle istanze distribuite di Collector Manager potrebbe andare in sovraccarico, ma il server Sentinel continuerebbe comunque a rispondere alle richieste dell'utente.

L'installazione di più istanze di Collector Manager in una rete distribuita apporta i vantaggi seguenti:

- **Miglioramento della prestazione del sistema:** le istanze aggiuntive di Collector Manager consentono di analizzare sintatticamente ed elaborare i dati degli eventi in un ambiente distribuito, incrementando così le prestazioni del sistema.
- **Una maggiore protezione dei dati e la richiesta di una larghezza di banda di rete più ridotta:** Se le istanze di Collector Manager 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:** le istanze aggiuntive di Collector Manager permettono di memorizzare una grande quantità di dati nella cache mentre il server è temporaneamente occupato nell'archiviazione degli eventi o nell'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.

È possibile installare istanze aggiuntive di Collector Manager in ubicazioni appropriate della rete. Le istanze remote di Collector Manager eseguono connettori e servizi di raccolta, quindi inoltrano i dati raccolti al server Sentinel affinché vengano memorizzati ed elaborati. Per informazioni sull'installazione di ulteriori istanze di Collector Manager, vedere la Parte III, "Installazione di Sentinel," a pagina 71.

Nota: in un sistema è possibile installare più istanze di Collector Manager. Le istanze aggiuntive di Collector Manager possono essere installate in sistemi remoti e successivamente connesse al server Sentinel.

Vantaggi derivanti dall'uso di istanze aggiuntive di Correlation Engine

È possibile installare istanze multiple di Correlation Engine, ognuna sul proprio server, senza dover replicare le configurazioni o aggiungere database. Per ambienti con un numero elevato di regole di correlazione o frequenze eventi molto elevate, risulta particolarmente vantaggioso installare più istanze di Correlation Engine e ridistribuire alcune regole sulle nuove istanze. Le istanze multiple di Correlation Engine offrono la scalabilità necessaria a far fronte a nuove origini di dati o all'aumento delle frequenze eventi del sistema Sentinel. Per informazioni sull'installazione di istanze aggiuntive di Correlation Engine, consultare Parte III, “Installazione di Sentinel,” a pagina 71.

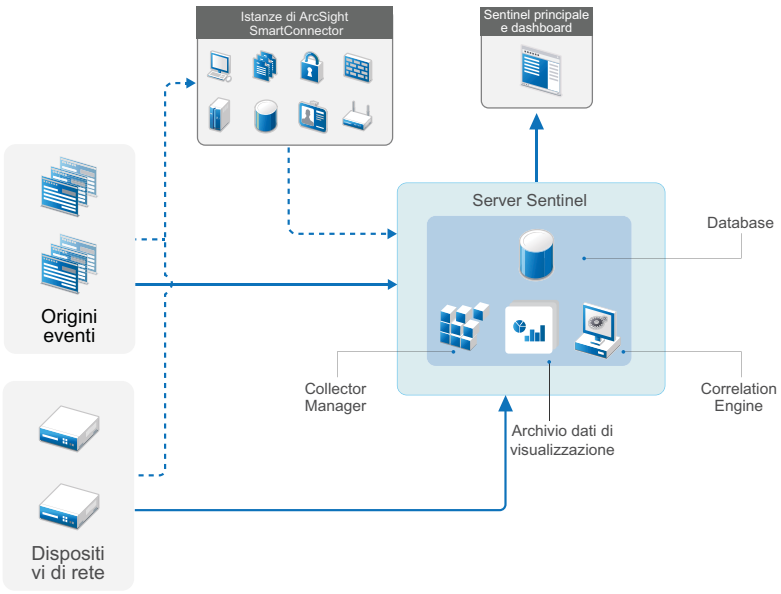
Nota: in un sistema è possibile installare una sola istanza di Correlation Engine. Le istanze aggiuntive di Correlation Engine possono essere installate in sistemi remoti e successivamente connesse al server Sentinel.

Installazione all-in-one

L'opzione d'installazione di base prevede un sistema all-in-one che include tutti i componenti di Sentinel in un solo computer. L'installazione all-in-one risulta adeguata soltanto se il carico del sistema è ridotto e non è necessario monitorare computer Windows. In numerosi ambienti è possibile che carichi non prevedibili e variabili, oltre a conflitti di risorse fra componenti difficili da rilevare, causino problemi di prestazioni.

Importante: per gli ambienti di produzione, si consiglia di configurare un'installazione distribuita poiché consente di raggruppare i componenti di raccolta dati in un computer separato, permettendo così di gestire picchi e altre anomalie preservando la massima stabilità del sistema.

Figura 6-2 *Installazione all-in-one*

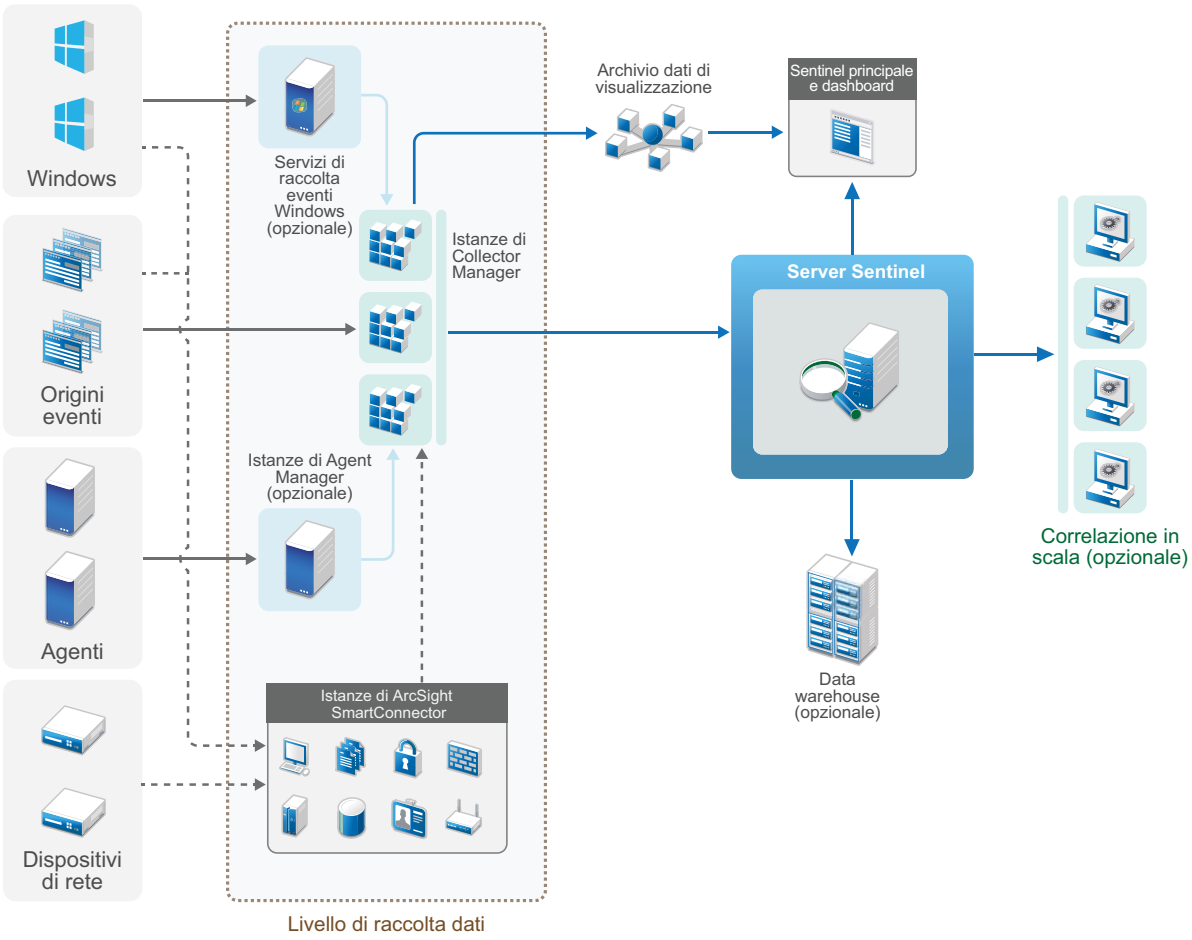


Installazione distribuita a un livello

Rispetto all'installazione all-in-one, l'installazione a un livello aggiunge la possibilità di monitorare i computer Windows e gestire un carico superiore. È possibile scalare orizzontalmente la raccolta e la correlazione dei dati aggiungendo computer che siano dotati di Collector Manager e Correlation Engine in modo tale da deviare l'elaborazione del carico dal server Sentinel centrale. Oltre alla gestione dei carichi di eventi e regole di correlazione, le istanze remote di Gestione servizi di raccolta e del motore di correlazione contribuiscono anche a liberare risorse nel server centrale di Sentinel, affinché possano essere utilizzate per soddisfare altre richieste quali la memorizzazione degli eventi e le ricerche. All'aumentare del carico del sistema, il server centrale di Sentinel finisce per diventare un collo di bottiglia e diventa necessaria un'installazione con più livelli.

In alternativa è possibile configurare Sentinel in modo da copiare i dati degli eventi in un data warehouse, utile per spostare su un altro sistema il carico di rapporti personalizzati, funzionalità di analisi e altre elaborazioni.

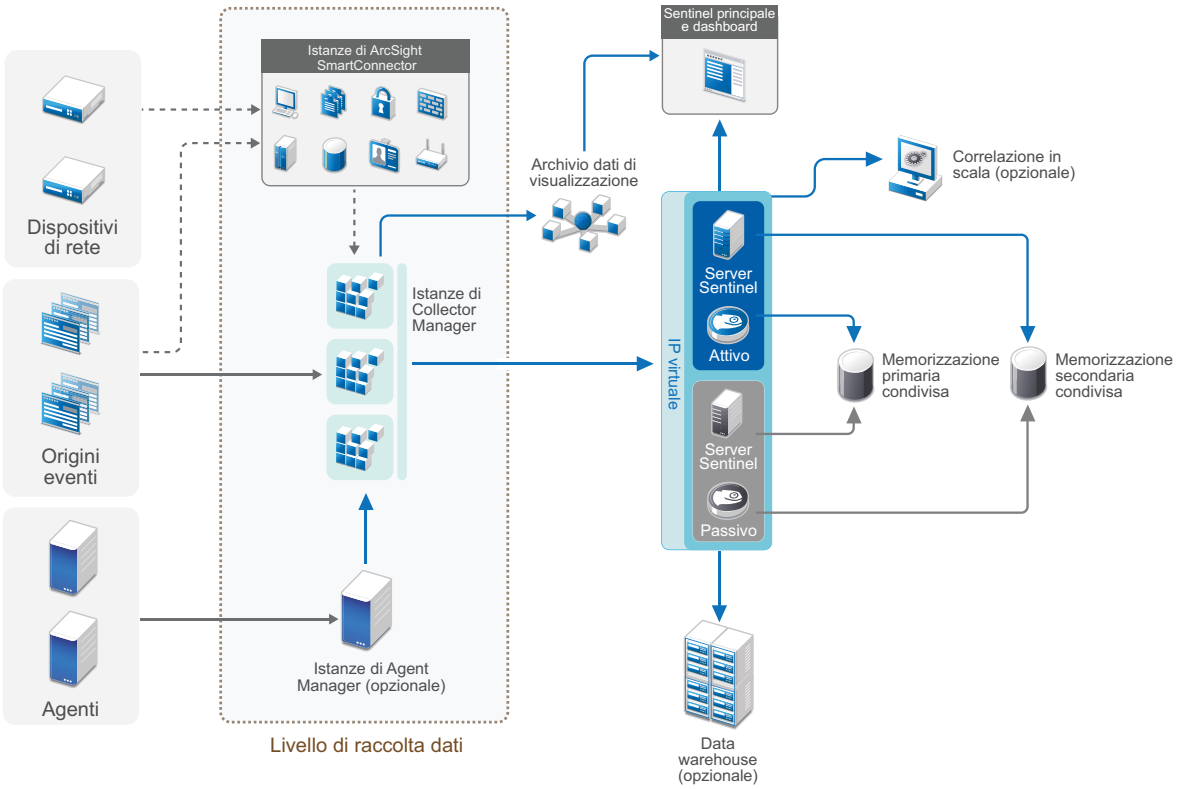
Figura 6-3 *Installazione distribuita a un livello*



Installazione distribuita a un livello con alta disponibilità

L'installazione distribuita a un livello può essere trasformata in un sistema ad alta disponibilità con ridondanza per il failover. Per ulteriori informazioni sull'installazione di Sentinel in configurazione ad alta disponibilità, vedere l'Parte VII, “Installazione di Sentinel per alta disponibilità,” a pagina 187.

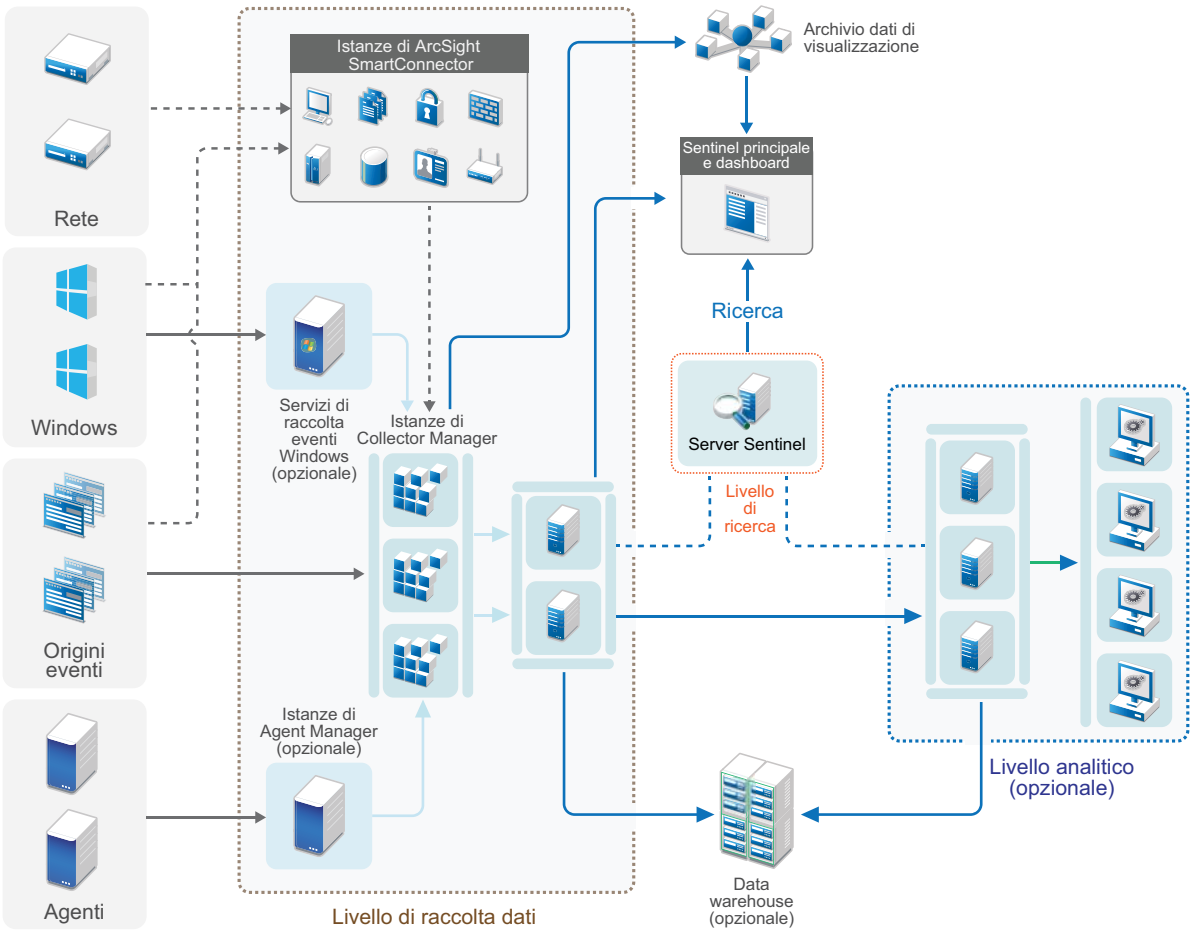
Figura 6-4 *Installazione distribuita a un livello con alta disponibilità*



Installazione distribuita a due e tre livelli

Questi tipi d'installazione consentono di migliorare le capacità di gestione del carico di un solo server Sentinel centrale e di condividere il carico di elaborazione tra più istanze di Sentinel, mediante le funzionalità Collegamento Sentinel e Federazione dati Sentinel. Il carico della raccolta dati viene bilanciato su più server Sentinel, ognuno dei quali prevede varie istanze di Collector Manager, come indicato nel livello di raccolta dati. Se si desidera eseguire operazioni di correlazione degli eventi o di security intelligence, è possibile inoltrare i dati fino al livello di analisi utilizzando Collegamento Sentinel. Il livello di ricerca fornisce un punto di accesso singolo pratico per effettuare le ricerche in tutti i livelli dei sistemi mediante la funzione Federazione dati Sentinel. Poiché la richiesta di ricerca viene federata fra numerose istanze di Sentinel, questo tipo d'installazione dispone anche di proprietà di bilanciamento del carico delle ricerche utili per la gestione graduale di carichi di ricerca elevati.

Figura 6-5 *Installazione distribuita a due e tre livelli*



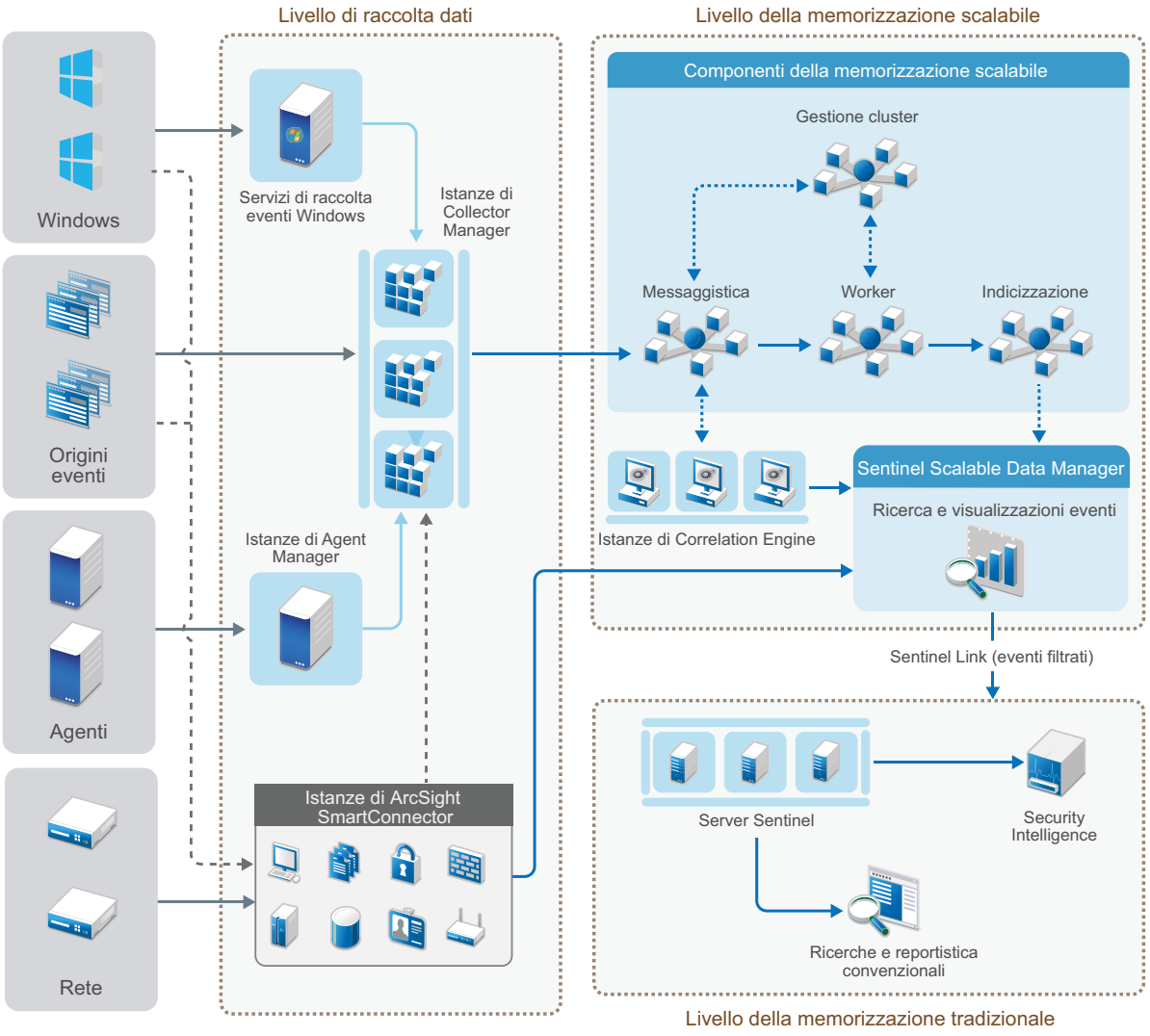
Installazione su tre livelli con memorizzazione scalabile

Per la memorizzazione e l'elaborazione di grandi quantità di dati in cui non si desidera distribuire gli eventi fra più server Sentinel e duplicare le impostazioni di configurazione in più istanze, è possibile configurare un'installazione distribuita su tre livelli con la memorizzazione scalabile. Questo tipo di installazione consente di memorizzare e gestire grandi quantità di dati utilizzando un solo server Sentinel con la memorizzazione scalabile, invece di più server Sentinel.

È possibile configurare un nuovo server Sentinel con la memorizzazione scalabile oppure eseguire l'upgrade del server Sentinel esistente per abilitare la memorizzazione scalabile.

A seconda delle funzionalità di Sentinel che si desidera utilizzare, è possibile determinare come si desidera configurare la distribuzione di Sentinel.

Figura 6-6 *Installazione su tre livelli per la memorizzazione scalabile*



Questa installazione include i seguenti livelli:

- **Livello di raccolta dati:** per raccogliere gli eventi da un'ampia gamma di origini. In alternativa, se si desidera mantenere tutte le impostazioni esistenti della raccolta dati di Sentinel con la memorizzazione tradizionale e comunque sfruttare i vantaggi delle funzioni di memorizzazione scalabile, è possibile inoltrare gli eventi desiderati direttamente dalla memorizzazione tradizionale a quella scalabile utilizzando lo script `data_uploader.sh`. Per ulteriori informazioni, consultare Capitolo 32, “Migrazione dei dati nella memorizzazione scalabile”, a pagina 177.
- **Livello della memorizzazione scalabile:** per memorizzazione, indicizzazione e analisi di grandi quantità di dati. In questo livello, il server SSDM consente di gestire la raccolta e la correlazione dei dati; inoltre, fornisce altre funzionalità SSDM. Per utilizzare le funzionalità di Sentinel che non sono disponibili in SSDM, è possibile configurare il livello di memorizzazione tradizionale. È possibile inoltrare i dati raccolti a qualsiasi altro sistema SIEM. In alternativa, è possibile abilitare altri strumenti di business intelligence affinché interroghino i dati oppure effettuino l'analisi direttamente nella distribuzione Hadoop utilizzando le ben supportate API di Hadoop, Kafka, Spark ed Elasticsearch.

- **Livello di memorizzazione tradizionale:** per funzionalità di Sentinel quali security intelligence, ricerca convenzionale e generazione di rapporti è necessario installare istanze separate di Sentinel con memorizzazione tradizionale. È possibile configurare le regole d'instradamento degli eventi in modo che quelli desiderati siano inoltrati da SSDM a Sentinel attraverso Collegamento Sentinel.

  Si possono eseguire ricerche e generare rapporti anche nel livello di memorizzazione tradizionale, utilizzando uno qualsiasi dei server Sentinel. Facoltativamente, è possibile configurare un livello di ricerca separato che fornisce un pratico punto di accesso singolo per effettuare ricerche e generare rapporti tra tutti i server di Sentinel che si trovano nel livello di memorizzazione tradizionale. Per cercare gli eventi nella memorizzazione scalabile, utilizzare l'opzione di ricerca in SSDM.

Per ulteriori informazioni sull'installazione e la configurazione della memorizzazione scalabile, vedere il Capitolo 13, “Installazione e configurazione della memorizzazione scalabile”, a pagina 87.

7 Considerazione sull'installazione per la modalità FIPS140-2

Opzionalmente, Sentinel può essere configurato per utilizzare Network Security Services (NSS) di Mozilla, vale a dire un provider che ha ottenuto la convalida FIPS 140-2 per la cifratura interna e altre funzioni. L'obiettivo di questo tipo di configurazione consiste nell'integrare la certificazione FIPS 140-2 in Sentinel, rendendolo conforme alle policy e gli standard federali statunitensi in materia di acquisti.

L'abilitazione della modalità FIPS 140-2 in Sentinel fa sì che le comunicazioni fra il server Sentinel, le istanze remote di Collector Manager, le istanze remote di Correlation Engine, l'interfaccia principale di Sentinel, Sentinel Control Center e il servizio Sentinel Advisor utilizzino la cifratura certificata FIPS 140-2.

Importante: la modalità FIPS è supportata solo per Sentinel. Se il sistema operativo è in modalità FIPS, Sentinel non è supportato.

Implementazione di FIPS in Sentinel

Sentinel utilizza le librerie NSS di Mozilla incluse nel sistema operativo. Red Hat Enterprise Linux (RHEL) e SUSE Linux Enterprise Server (SLES) utilizzano set diversi di pacchetti NSS.

Il modulo di cifratura NSS incluso in RHEL 6.3 e versioni successive ha ottenuto la convalida FIPS 140-2. Il modulo di cifratura NSS incluso in SLES 11 non è stato ancora ufficialmente convalidato come conforme a FIPS 140-2, ma le procedure di convalida del modulo SUSE conforme a FIPS 140-2 sono in corso. Una volta ottenuta la convalida, non si prevede che saranno necessarie modifiche per l'integrazione della certificazione FIPS 140-2 in Sentinel sulla piattaforma SUSE.

Per ulteriori informazioni sulla certificazione RHEL FIPS 140-2, vedere le pagine https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2711 e https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1837.

Pacchetti NSS di RHEL

Per supportare la modalità FIPS 140-2 sono necessari i pacchetti NSS a 64 bit elencati di seguito:

- nspr-*
- nss-sysinit-*
- nss-util-*
- nss-softokn-freebl-*

- nss-softokn-*
- nss-*
- nss-tools-*

Se uno o più dei pacchetti seguenti non sono installati, effettuare l'installazione prima di abilitare la modalità FIPS 140-2 in Sentinel.

Pacchetti NSS di SLES

Per supportare la modalità FIPS 140-2 sono necessari i pacchetti NSS a 64 bit elencati di seguito:

- libfreebl3-*
- mozilla-nspr-*
- mozilla-nss-*
- mozilla-nss-tools-*

Se uno o più dei pacchetti seguenti non sono installati, effettuare l'installazione prima di abilitare la modalità FIPS 140-2 in Sentinel.

Componenti di Sentinel che supportano FIPS

Di seguito sono elencati i componenti di Sentinel che supportano FIPS 140-2:

- Tutti i componenti della piattaforma Sentinel sono stati aggiornati per supportare la modalità FIPS 140-2.
- I plug-in di Sentinel seguenti che supportano la cifratura sono stati aggiornati per il supporto della modalità FIPS 140-2:
  - Connettore di Agent Manager 2011.1r1 e versioni successive
  - Connettore del database (JDBC) 2011.1r2 e versioni successive
  - Connettore file 2011.1r1 e versioni successive, solo se l'origine eventi file è di tipo locale o NFS.
  - Integratore LDAP 2011.1r1 e versioni successive
  - Connettore di Collegamento Sentinel 2011.1r3 e versioni successive
  - Integratore di Collegamento Sentinel 2011.1r2 e versioni successive
  - Integratore SMTP 2011.1r1 e versioni successive
  - Connettore Syslog 2011.1r2 e versioni successive
  - Connettore degli eventi di Windows (WMI) 2011.1r2 e versioni successive
  - Connettore di Check Point (LEA) 2011.1r2 e versioni successive
  - Integratore Syslog 2011.1r1 e versioni successive

  Per ulteriori informazioni sulla configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2, vedere “Configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2” a pagina 136.

Al momento della pubblicazione del presente documento, i connettori Sentinel seguenti che supportano la cifratura opzionale non sono ancora stati aggiornati per il supporto della modalità FIPS 140-2. È comunque possibile continuare a raccogliere gli eventi utilizzando tali connettori. Per istruzioni sull'utilizzo dei connettori con Sentinel in modalità FIPS 140-2, consultare “Utilizzo di connettori non FIPS con Sentinel in modalità FIPS 140-2” a pagina 142.

- Connettore di Cisco SDEE 2011.1r1
- Connettore file 2011.1r1 - Le funzionalità CIFS ed SCP prevedono la cifratura e pertanto non funzionano in modalità FIPS 140-2.
- Audit Connector 2011.1r1
- SNMP Connector 2011.1r1

Al momento della pubblicazione del presente documento, gli integratori Sentinel seguenti che supportano il protocollo SSL non sono ancora stati aggiornati per il supporto della modalità FIPS 140-2. Tuttavia, se si utilizzano questi integratori con Sentinel in modalità FIPS 140-2, è possibile continuare a usare connessioni non cifrate.

- Integratore di Remedy 2011.1r1 o versioni successive
- Integratore SOAP 2011.1r1 o versioni successive

Eventuali altri plug-in di Sentinel non elencati precedentemente non utilizzano la cifratura e l'abilitazione della modalità FIPS 140-2 non ha alcun effetto su di essi. Per utilizzarli con Sentinel in modalità FIPS 140-2, non è necessario eseguire altre operazioni.

Per ulteriori informazioni sui plug-in di Sentinel, visitare il sito Web dei plug-in di Sentinel. Se si desidera richiedere che uno dei plug-in non ancora aggiornati venga reso disponibile con il supporto FIPS, inviare una richiesta mediante Bugzilla.

Connessioni dati interessate dalla modalità FIPS

Se Sentinel è in modalità FIPS 140-2, non è possibile eseguire connessioni cifrate a Microsoft SQL Server. Questa considerazione riguarda i seguenti tipi di operazioni di Sentinel:

- Policy di sincronizzazione dati con SQL Server
- Comunicazione del server Sentinel con il database Agent Manager
- Connettore del database che raccoglie dati da SQL Server

Elenco di controllo per l'implementazione

Nella tabella seguente è riportata una panoramica dei task da eseguire per configurare Sentinel affinché funzioni in modalità FIPS 140-2.

Task	Per ulteriori informazioni, consultare…
Pianificare l'installazione.	“Scenari di distribuzione” a pagina 58.

Task	Per ulteriori informazioni, consultare…
Stabilire se si desidera abilitare la modalità FIPS 140-2 durante l'installazione di Sentinel o se si preferisce farlo successivamente. Per abilitare la modalità FIPS 140-2 di Sentinel durante l'installazione, è necessario selezionare l'installazione personalizzata o quella in modalità automatica.	"Installazione personalizzata del server Sentinel" a pagina 92. "Installazione in modalità automatica" a pagina 97 Capitolo 23, "Abilitazione della modalità FIPS 140-2 in un'installazione esistente di Sentinel", a pagina 131
Configurare i plug-in di Sentinel affinché vengano eseguiti in modalità FIPS 140-2.	"Configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2" a pagina 136.
Importare i certificati nell'archivio chiavi FIPS di Sentinel.	"Importazione di certificati nel database di archivio chiavi FIPS" a pagina 143

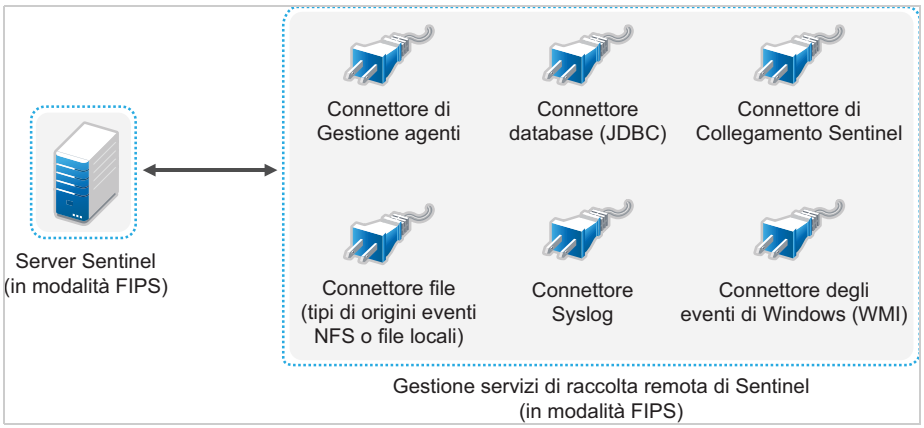
Nota: prima di iniziare la conversione alla modalità FIPS, eseguire il backup dei sistemi Sentinel in uso. Se successivamente il server dovrà essere riportato alla modalità non FIPS, l'unica procedura plausibile prevede il ripristino da una copia di backup. Per ulteriori informazioni sul ripristino della modalità non FIPS, vedere "Ripristino di Sentinel nella modalità non FIPS" a pagina 143.

Scenari di distribuzione

In questa sezione sono riportate informazioni sugli scenari di installazione di Sentinel nella modalità FIPS 140-2.

Scenario 1: raccolta dati esclusivamente in modalità FIPS 140-2

In questo scenario la raccolta dati viene eseguita interamente mediante i connettori che supportano la modalità FIPS 140-2. Le istruzioni che seguono presuppongono che l'ambiente includa un server Sentinel e che i dati vengano raccolti mediante un'istanza remota di Collector Manager. Le istanze remote di Collector Manager possono anche essere più di una.



La procedura seguente deve essere eseguita soltanto nel caso in cui i connettori utilizzati nell'ambiente per la raccolta dati dalle origini eventi supportino la modalità FIPS 140-2.

1 Il server Sentinel deve essere in modalità FIPS 140-2.

Nota: se subito dopo l'installazione o l'upgrade, il server Sentinel non è in modalità FIPS, abilitare FIPS nel server Sentinel. Per ulteriori informazioni, vedere il “Abilitazione dell'esecuzione in modalità FIPS 140-2 nel server Sentinel” a pagina 131.

2 È necessario che un'istanza remota di Collector Manager di Sentinel sia in esecuzione in modalità FIPS 140-2.

Nota: se subito dopo l'installazione o l'upgrade, l'istanza remota di Collector Manager non è in modalità FIPS, abilitare FIPS nell'istanza remota di Collector Manager. Per ulteriori informazioni, vedere il “Abilitazione della modalità FIPS 140-2 in istanze remote di Collector Manager e di Correlation Engine” a pagina 132.

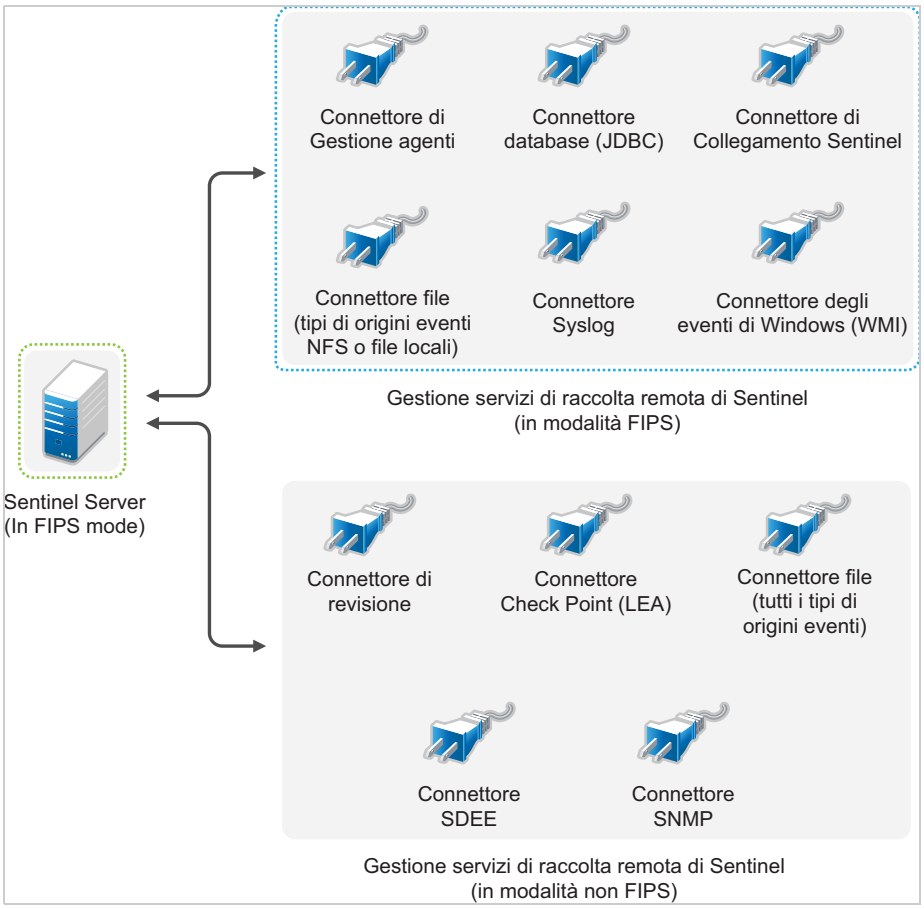
3 Accertarsi che il server FIPS e le istanze remote di Collector Manager comunichino fra di loro.

4 Se sono presenti istanze remote di Correlation Engine, configurarle affinché vengano eseguite in modalità FIPS. Per ulteriori informazioni, vedere il “Abilitazione della modalità FIPS 140-2 in istanze remote di Collector Manager e di Correlation Engine” a pagina 132.

5 Configurare i plug-in di Sentinel affinché vengano eseguiti in modalità FIPS 140-2. Per ulteriori informazioni, vedere il “Configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2” a pagina 136.

Scenario 2: raccolta dati parzialmente in modalità FIPS 140-2

In questo scenario la raccolta dati viene eseguita mediante connettori che supportano la modalità FIPS 140-2 e connettori che invece non la supportano. Si suppone che i dati siano raccolti mediante un'istanza remota di Collector Manager. Le istanze remote di Collector Manager possono anche essere più di una.



Per gestire la raccolta dati mediante connettori che supportano e che non supportano la modalità FIPS 140-2, è necessario utilizzare due istanze remote di Collector Manager, una eseguita in modalità FIPS 140-2 per i connettori con supporto FIPS e l'altra eseguita in modalità non FIPS (normale) per i connettori che non supportano la modalità FIPS 140-2.

La procedura seguente deve essere eseguita nel caso in cui per la raccolta dati dalle origini eventi vengano utilizzati connettori che supportano la modalità FIPS 140-2 e connettori che invece non la supportano.

1 Il server Sentinel deve essere in modalità FIPS 140-2.

Nota: se subito dopo l'installazione o l'upgrade, il server Sentinel non è in modalità FIPS, abilitare FIPS nel server Sentinel. Per ulteriori informazioni, vedere il “Abilitazione dell'esecuzione in modalità FIPS 140-2 nel server Sentinel” a pagina 131.

---

2 Verificare che un'istanza remota di Collector Manager sia eseguita in modalità FIPS 140-2 e che un'altra istanza remota sia eseguita in modalità non FIPS.

2a Se non si dispone di un'istanza remota di Collector Manager in modalità FIPS 140-2, abilitare FIPS nell'istanza remota di Collector Manager. Per ulteriori informazioni, vedere il “Abilitazione della modalità FIPS 140-2 in istanze remote di Collector Manager e di Correlation Engine” a pagina 132.

2b Aggiornare il certificato del server nell'istanza remota di Gestione servizi di raccolta in modalità non FIPS. Per ulteriori informazioni, vedere il “Aggiornamento dei certificati del server nelle istanze remote di Collector Manager e di Correlation Engine” a pagina 135.

3 Verificare che le due istanze remote di Collector Manager comunichino con il server Sentinel abilitato per la modalità FIPS 140-2.

4 Se presenti, configurare le istanze remote di Correlation Engine vengano eseguite in modalità FIPS 140-2. Per ulteriori informazioni, vedere il “Abilitazione della modalità FIPS 140-2 in istanze remote di Collector Manager e di Correlation Engine” a pagina 132.

5 Configurare i plug-in di Sentinel affinché vengano eseguiti in modalità FIPS 140-2. Per ulteriori informazioni, vedere il “Configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2” a pagina 136.

   5a Installare i connettori che supportano la modalità FIPS 140-2 nell'istanza remota di Collector Manager in modalità FIPS.

   5b Installare i connettori che non supportano la modalità FIPS 140-2 nell'istanza remota di Collector Manager in modalità normale.

8 Porte utilizzate

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 tradizionale, per aprire le porte sul firewall è necessario configurare il sistema operativo in cui si sta eseguendo l'installazione di Sentinel.

Porte del server Sentinel

Il server Sentinel utilizza le porte seguenti per la comunicazione interna ed esterna.

Porte locali

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

Porte	Descrizione
TCP 27017	Utilizzata per il database di configurazione di Security Intelligence.
TCP 28017	Utilizzata per la console Web del database di Security Intelligence.
TCP 32000	Utilizzata per la comunicazione interna tra il processo del wrapper e quello del server.
TCP 9200	Utilizzata per la comunicazione con il servizio di indicizzazione degli avvisi mediante REST.
TCP 9300	Utilizzata per la comunicazione con il servizio di indicizzazione degli avvisi mediante il protocollo nativo.

Porte di rete

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

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 5432	In entrata	Facoltativo. Per default, questa porta è in ascolto solo dell'interfaccia di loopback.	Utilizzata per il database PostgreSQL. Non è necessario aprire questa porta per default. Tuttavia, è necessario aprire la porta quando si generano i rapporti mediante l'SDK di Sentinel. Per ulteriori informazioni, vedere Sentinel Plug-in SDK (SDK per i plug-in di Sentinel).

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 1099 e 2000	In entrata	Obbligatoria	Vengono utilizzate congiuntamente dagli strumenti di monitoraggio per connettersi al processo del server Sentinel mediante Java Management Extensions (JMX).
TCP 1289	In entrata	Facoltativo	Utilizzata per le connessioni di Audit.
UDP 1514	In entrata	Facoltativo	Utilizzata per i messaggi syslog.
TCP 8443	In entrata	Obbligatoria	Utilizzata per la comunicazione HTTPS.
TCP 1443	In entrata	Facoltativo	Utilizzata per i messaggi syslog cifrati mediante il protocollo SSL.
TCP 61616	In entrata	Facoltativo	Utilizzata per connessioni in entrata da istanze di Collector Manager e di Correlation Engine.
TCP 10013	In entrata	Obbligatoria	Utilizzata da Sentinel Control Center e Solution Designer.
TCP 1468	In entrata	Facoltativo	Utilizzata per i messaggi syslog.
TCP 10014	In entrata	Facoltativo	Utilizzata dalle istanze remote di Collector Manager per connettersi al server mediante il proxy SSL. Tale procedura, tuttavia, non è comune. Infatti, per connettersi al server delle istanze remote di Collector Manager utilizzano la porta SSL 61616 per default.
TCP 443	In uscita	Facoltativo	Se si utilizza Advisor, la porta avvia una connessione al servizio Advisor via Internet verso l'URL degli aggiornamenti di Advisor.
TCP 8443	In uscita	Facoltativo	Se si utilizza la federazione dati, la porta stabilisce la connessione ad altri sistemi Sentinel per effettuare la ricerca distribuita.
TCP 389 o 636	In uscita	Facoltativo	Se si utilizza l'autenticazione LDAP, la porta attiva la connessione con il server LDAP.
TCP/UDP 111 e TCP/UDP 2049	In uscita	Facoltativo	Se la memorizzazione secondaria è configurata per l'uso del protocollo NFS.
TCP 137, 138, 139, 445	In uscita	Facoltativo	Se la memorizzazione secondaria è configurata per l'uso del protocollo CIFS.
TCP JDBC (a seconda del database)	In uscita	Facoltativo	Se si utilizza la sincronizzazione dei dati, la porta avvia la connessione con il database di destinazione mediante JDBC. La porta utilizzata varia a seconda del database di destinazione.
TCP 25	In uscita	Facoltativo	Avvia una connessione con il server e-mail.
TCP 1290	In uscita	Facoltativo	Quando Sentinel inoltra gli eventi a un altro sistema Sentinel, la porta avvia una connessione con tale sistema tramite Collegamento Sentinel.
UDP 162	In uscita	Facoltativo	Quando Sentinel inoltra gli eventi al sistema che riceve i trap SNMP, la porta invia un pacchetto al destinatario.
UDP 514 o TCP 1468	In uscita	Facoltativo	La porta viene utilizzata quando Sentinel inoltra gli eventi al sistema che riceve i messaggi Syslog. Se la porta è UDP, invia un pacchetto al destinatario. Se la porta è TCP, avvia una connessione con il destinatario.

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 9443	In entrata	Facoltativo	La porta consente a un sistema Sentinel di ricevere gli eventi da altri software SIEM, come ad esempio Change Guardian e Secure Configuration Manager.

Porte specifiche per l'applicazione server Sentinel

In aggiunta a quelle riportate precedentemente, per l'applicazione vengono aperte anche le porte seguenti.

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 22	In entrata	Obbligatoria	Utilizzata per l'accesso shell sicuro a Sentinel Appliance.
TCP 4984	In entrata	Obbligatoria	Utilizzata anche dall'applicazione Sentinel per il servizio di aggiornamento.
TCP 289	In entrata	Facoltativo	Inoltrata a 1289 per le connessioni Audit.
TCP 443	In entrata	Facoltativo	Inoltrata alla 8443 per la comunicazione HTTPS.
UDP 514	In entrata	Facoltativo	Inoltrata a 1514 per i messaggi.
TCP 1290	In entrata	Facoltativo	Porta di Collegamento Sentinel a cui è consentito connettersi attraverso il firewall di SUSE.
UDP e TCP 40000 - 41000	In entrata	Facoltativo	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.
TCP 443 o 80	In uscita	Obbligatoria	Avvia una connessione con l'archivio degli aggiornamenti software per l'applicazione , disponibile su Internet, o con un servizio Subscription Management Tool (SMT) nella propria rete.
TCP 80	In uscita	Facoltativo	Avvia una connessione con Subscription Management Tool (SMT).
TCP 7630	In entrata	Obbligatoria	Utilizzata da High Availability Web Konsole (Hawk).
TCP 9443	In entrata	Obbligatoria	Utilizzata dalla console di gestione dell'applicazione Sentinel.
TCP 1098 e 2000	In entrata	Obbligatoria	Vengono utilizzate congiuntamente dagli strumenti di monitoraggio per connettersi al processo del server Sentinel mediante Java Management Extensions (JMX).

Porte di Collector Manager

L'istanza di Collector Manager comunica con gli altri componenti mediante le porte seguenti.

Porte di rete

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

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 1289	In entrata	Facoltativo	Utilizzata per le connessioni di Audit.
UDP 1514	In entrata	Facoltativo	Utilizzata per i messaggi syslog.
TCP 1443	In entrata	Facoltativo	Utilizzata per i messaggi syslog cifrati mediante il protocollo SSL.
TCP 1468	In entrata	Facoltativo	Utilizzata per i messaggi syslog.
TCP 1099 e 2000	In entrata	Obbligatoria	Vengono utilizzate congiuntamente dagli strumenti di monitoraggio per connettersi al processo del server Sentinel mediante Java Management Extensions (JMX).
TCP 61616	In uscita	Obbligatoria	Avvia una connessione con il server Sentinel.
TCP 8443	In uscita	Obbligatoria	Avvia una connessione con la porta del server Web Sentinel. Durante l'installazione e la configurazione di Collector Manager, lasciare aperta questa porta.

Porte specifiche per l'applicazione Collector Manager

In aggiunta a quelle riportate precedentemente, per l'applicazione Collector Manager di Sentinel vengono aperte anche le porte seguenti.

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 22	In entrata	Obbligatoria	Utilizzata per l'accesso shell sicuro a Sentinel Appliance.
TCP 4984	In entrata	Obbligatoria	Utilizzata anche dall'applicazione Sentinel per il servizio di aggiornamento.
TCP 289	In entrata	Facoltativo	Inoltrata a 1289 per le connessioni Audit.
UDP 514	In entrata	Facoltativo	Inoltrata a 1514 per i messaggi.
TCP 1290	In entrata	Facoltativo	È la porta di Collegamento Sentinel cui è consentito connettersi attraverso il firewall SuSE.
UDP e TCP 40000 - 41000	In entrata	Facoltativo	Utilizzata durante la configurazione dei server di raccolta dei dati, come syslog. Per default, Sentinel non è in ascolto su queste porte.
TCP 443	In uscita	Obbligatoria	Avvia una connessione con l'archivio degli aggiornamenti software per l'applicazione , disponibile su Internet, o con un servizio Subscription Management Tool (SMT) nella propria rete.
TCP 80	In uscita	Facoltativo	Avvia una connessione con Subscription Management Tool (SMT).

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 9443	In entrata	Obbligatoria	Utilizzata dalla console di gestione dell'applicazione Sentinel.
TCP 1098 e 2000	In entrata	Obbligatoria	Vengono utilizzate congiuntamente dagli strumenti di monitoraggio per connettersi al processo del server Sentinel mediante Java Management Extensions (JMX).

Porte di Correlation Engine

L'istanza di Correlation Engine comunica con gli altri componenti mediante le porte seguenti.

Porte di rete

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

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 1099 e 2000	In entrata	Obbligatoria	Vengono utilizzate congiuntamente dagli strumenti di monitoraggio per connettersi al processo del server Sentinel mediante Java Management Extensions (JMX).
TCP 61616	In uscita	Obbligatoria	Avvia una connessione con il server Sentinel.
TCP 8443	In uscita	Obbligatoria	Avvia una connessione con la porta del server Web Sentinel. Durante l'installazione e la configurazione di Correlation Engine, lasciare aperta questa porta.

Porte specifiche per l'applicazione Correlation Engine

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

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 22	In entrata	Obbligatoria	Utilizzata per l'accesso shell sicuro a Sentinel Appliance.
TCP 4984	In entrata	Obbligatoria	Utilizzata anche dall'applicazione Sentinel per il servizio di aggiornamento.
TCP 443	In uscita	Obbligatoria	Avvia una connessione con l'archivio degli aggiornamenti software per l'applicazione , disponibile su Internet, o con un servizio Subscription Management Tool (SMT) nella propria rete.
TCP 80	In uscita	Facoltativo	Avvia una connessione con Subscription Management Tool (SMT).
TCP 9443	In entrata	Obbligatoria	Utilizzata dalla console di gestione dell'applicazione Sentinel.

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 1098 e 2000	In entrata	Obbligatoria	Vengono utilizzate congiuntamente dagli strumenti di monitoraggio per connettersi al processo del server Sentinel mediante Java Management Extensions (JMX).

Porte della memorizzazione scalabile

Ai fini della corretta comunicazione di SSDM con CDH ed Elasticsearch, verificare che le porte specificate durante la configurazione della memorizzazione scalabile siano aperte nel firewall, così come le porte necessarie per Cloudera e quelle elencate nella sezione Porte del server Sentinel.

9 Opzioni di installazione

Sentinel può essere installato in modo tradizionale oppure in modalità applicazione. In questo capitolo sono riportate le informazioni relative a entrambe le opzioni di installazione.

Installazione tradizionale

Con la procedura tradizionale si esegue l'installazione di Sentinel in un sistema operativo esistente utilizzando il programma di installazione dell'applicazione. È possibile installare Sentinel in uno dei due modi seguenti:

- **Interattivo:** l'installazione procede mediante gli input dell'utente. Durante l'installazione è possibile registrare in un file le opzioni di installazione (input dell'utente o valori di default) e utilizzarle successivamente per un'installazione in modalità automatica. L'installazione può essere standard o personalizzata.

Installazione standard	Installazione personalizzata
Per la configurazione vengono utilizzati i valori di default. L'input dell'utente è richiesto solo per la password.	Viene richiesto di specificare i valori di configurazione. È possibile selezionare i valori di default oppure specificare quelli necessari.
L'installazione viene eseguita con la chiave di valutazione di default.	Consente di eseguire l'installazione utilizzando la chiave della licenza di valutazione di default 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.
Sentinel viene installato in modalità non FIPS.	Consente di installare Sentinel in modalità FIPS 140-2.
Utilizza la memorizzazione tradizionale per memorizzare dati non elaborati ed eventi.	Consente di utilizzare la memorizzazione scalabile per memorizzare dati non elaborati ed eventi.
Autentica utenti con il database interno.	Consente di scegliere per Sentinel l'autenticazione LDAP oltre a quella del database. Quando Sentinel viene configurato per l'autenticazione LDAP, gli utenti possono effettuare il login al server mediante le proprie credenziali Novell eDirectory o Microsoft Active Directory.

Per ulteriori informazioni sull'installazione interattiva, vedere la “Installazione interattiva” a pagina 91.

- **Modalità automatica:** se si desidera installare più server Sentinel nella propria distribuzione, è possibile registrare le opzioni di installazione in un file di configurazione durante l'installazione standard o personalizzata e, successivamente, utilizzare tale file per eseguire un'installazione in modalità automatica. Per ulteriori informazioni sull'installazione in modalità automatica, vedere la “Installazione in modalità automatica” a pagina 97.

Installazione in modalità applicazione

Con l'installazione in modalità applicazione si installa sia il sistema operativo SLES 12 SP3 a 64 bit che Sentinel.

L'applicazione Sentinel è disponibile nei seguenti formati:

- Immagine dell'applicazione OVF
- Immagine ISO dell'applicazione

Per ulteriori informazioni sull'installazione in modalità applicazione, vedere il Capitolo 15, “Installazione in modalità applicazione”, a pagina 101.

II Installazione di Sentinel

In questa sezione sono riportate le informazioni relative all'installazione di Sentinel e dei componenti aggiuntivi.

10 Panoramica relativa all'installazione

Con l'installazione di default di Sentinel si installano nel server Sentinel i componenti seguenti:

- **Processi del server Sentinel e del server Web:** Il processo eseguito dal server Sentinel elabora le richieste provenienti dagli altri componenti e consente al sistema di funzionare senza interruzioni. Tale processo gestisce richieste quali il filtraggio dei dati, l'elaborazione delle interrogazioni di ricerca e la gestione di task amministrativi che includono autenticazione e autorizzazione degli utenti.

  Il server Web di Sentinel consente la connessione sicura all'interfaccia principale di Sentinel.
- **Database PostgreSQL:** Sentinel è dotato di un database integrato in cui sono memorizzate le informazioni relative alla sua configurazione, i dati sulle risorse e le vulnerabilità, le informazioni sulle identità, gli stati dei casi e dei workflow e così via.
- **Database MongoDB:** Memorizza i dati di Security Intelligence e degli avvisi.
- **Elasticsearch:** indicizza eventi e avvisi per la ricerca e la visualizzazione.
- **Collector Manager:** flessibile punto di raccolta dei dati utilizzato da Sentinel. Il programma di installazione di Sentinel installa per default anche un'istanza di Collector Manager.
- **Elasticsearch:** componente opzionale per memorizzare e indicizzare i dati. Sentinel include di default un nodo Elasticsearch. Se si prevede un elevato numero di EPS, superiore, ad esempio, ai 2500, è necessario installare nodi Elasticsearch aggiuntivi in un cluster.
- **Correlation Engine:** elabora gli eventi contenuti nel flusso in tempo reale per stabilire se devono attivare una o più delle regole di correlazione.
- **Advisor:** Advisor di Security Nexus è un servizio facoltativo di sottoscrizione dati che fornisce una correlazione a livello di dispositivi tra gli eventi in tempo reale provenienti da sistemi di prevenzione e rilevamento delle intrusioni e da risultati di scansioni delle vulnerabilità aziendali. Per ulteriori informazioni su Advisor, vedere “Detecting Vulnerabilities and Exploits” (Rilevamento di vulnerabilità ed exploit) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).
- **Plug-in di Sentinel:** Sentinel supporta una serie di plug-in per ampliare e migliorare le funzionalità del sistema. Alcuni di questi plug-in sono preinstallati. È possibile effettuare il download di plug-in aggiuntivi e aggiornamenti dal sito Web dei plug-in di Sentinel. I plug-in di Sentinel includono:
  - Servizi di raccolta
  - Connettori
  - Regole di correlazione e azioni
  - Rapporti
  - Workflow iTRAC
  - Pacchetti soluzione

11 Elenco di controllo per l'installazione

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

- ❒ Verificare che hardware e software soddisfino i requisiti di sistema elencati in Capitolo 5, “Requisiti di sistema”, a pagina 37.
- ❒ 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 il Appendice B, “Disinstallazione”, a pagina 231.
- ❒ Se si prevede di installare la versione con licenza, richiedere la chiave di licenza al servizio di assistenza clienti .
- ❒ Assicurarsi che le porte elencate in Capitolo 8, “Porte utilizzate”, a pagina 63 siano aperte sul firewall.
- ❒ Affinché il programma di installazione di Sentinel funzioni correttamente, il sistema deve restituire il nome host o un indirizzo IP valido. A tale scopo, aggiungere il nome host al file `/etc/hosts` nella riga contenente l'indirizzo IP, quindi immettere `hostname -f` affinché il nome host venga visualizzato correttamente.
- ❒ Sincronizzare l'orario mediante il protocollo NTP (Network Time Protocol).
- ❒ Se si prevede di installare Sentinel nella configurazione con memorizzazione scalabile, verificare di aver installato CDH ed Elasticsearch. Per ulteriori informazioni sull'installazione di Sentinel con la memorizzazione scalabile, vedere “Installazione e configurazione della memorizzazione scalabile” a pagina 87.
- ❒ **Su sistemi RHEL:** per ottenere 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 installazioni tradizionali:**

  il sistema operativo del server Sentinel deve includere almeno i componenti di base del server SLES o del server RHEL 6. Per Sentinel sono necessarie le versioni a 64 bit dei seguenti RPM:

  - bash
  - bc
  - coreutils
  - gettext
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof

- net-tools
- openssl
- python-libs
- sed
- zlib

❒ **Per Sentinel con la memorizzazione tradizionale:**

Per ottenere le visualizzazioni degli eventi, impostare la memoria virtuale aggiungendo la proprietà `vm.max_map_count=262144` nel file `/etc/sysctl.conf`.

12 Installazione e configurazione di Elasticsearch

Per l'indicizzazione scalabile e distribuita degli eventi, è necessario installare Elasticsearch in modalità cluster. Il cluster di Elasticsearch che si installa per Sentinel deve essere utilizzato per indicizzare solo i dati di Sentinel.

Prerequisiti

Prima di installare Elasticsearch, eseguire le operazioni preliminari seguenti:

- In base alla frequenza EPS, installare Elasticsearch in modalità cluster con il numero di nodi e di repliche consigliato nella pagina delle informazioni tecniche su Sentinel.
- Impostare i descrittori di file aggiungendo la proprietà seguente nel file `/etc/security/limits.conf`:

```
elasticsearch hard nofile 65536
elasticsearch soft nofile 65536
elasticsearch soft as unlimited
```

Nota: Una volta completati i prerequisiti precedenti, eseguire il comando `sysctl -p` per caricare di nuovo le modifiche apportate ai file.

Installazione e configurazione di Elasticsearch

Installare Elasticsearch e i plug-in necessari in ciascun nodo del cluster Elasticsearch.

Per installare e configurare Elasticsearch:

1. Installare la versione di JDK supportata da Elasticsearch.
2. Effettuare il download della versione certificata dell'RPM di Elasticsearch. Per ulteriori informazioni sulla versione vertificata di Elasticsearch e l'URL di download, vedere la pagina delle informazioni tecniche su Sentinel.
3. Installare Elasticsearch:

   ```
   rpm -i elasticsearch-<versione>.rpm
   ```

4. Eseguire i task specificati nelle istruzioni successive all'installazione di RPM.
5. Accertarsi che l'utente Elasticsearch abbia accesso a Java.

6 Configurare il file `/etc/elasticsearch/elasticsearch.yml` aggiornando o aggiungendo le seguenti informazioni:

Proprietà e valore	Note
cluster.name: <*nome_cluster_Elasticsearch*>	Il nome del cluster specificato deve essere lo stesso per tutti i nodi.
node.name: <*nome_nodo*>	Il nome di ciascun nodo deve essere univoco.
network.host: _<*interfacciaRete*>:ipv4_	
discovery.zen.ping.unicast.hosts: [< FQDN del nodo Elasticsearch nel server Sentinel >, <*FQDN del nodo 1 Elasticsearch*>, <*FQDN del nodo 2 Elasticsearch*> e così via]	
thread_pool.bulk.queue_size: 300	
thread_pool.search.queue_size: 10000	Quando la coda di ricerca raggiunge il limite massimo, Elasticsearch scarta eventuali richieste di ricerca in sospeso presenti nella coda. È possibile aumentare le dimensioni della coda di ricerca in base al calcolo seguente: threadpool.search.queue_size = numero medio di interrogazioni del widget per utente di un dashboard x numero di partizioni (indice giornaliero) x numero di giorni (durata della ricerca).
index.codec: best_compression	
path.data: ["/<*es1*>", "/<*es2*>"]	Distribuire i dati su più dischi o ubicazioni indipendenti per ridurre la latenza I/O del disco. Configurare più percorsi per la memorizzazione dei dati di Elasticsearch, ad esempio /es1, /es2 e così via. Per ottimizzare le prestazioni e la gestibilità, montare ciascun percorso in un disco fisico separato (JBOD).

7 Aggiornare la dimensione di default dell'heap Elasticsearch nel file `/etc/elasticsearch/jvm.options`.

La dimensione dell'heap deve essere pari al 50% della memoria del server. Ad esempio, in un nodo Elasticsearch di 24 GB, allocare 12 GB alla dimensione dell'heap per ottenere prestazioni ottimali.

8 Ripetere tutti i passaggi precedenti in ciascun nodo del cluster di Elasticsearch.

9 Nel nodo Elasticsearch del server Sentinel, configurare `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` come indicato di seguito:

9a Verificare che i valori di `cluster.name` e `discovery.zen.ping.unicast.hosts` nel file `elasticsearch.yml` siano gli stessi del file `elasticsearch.yml` nel nodo Elasticsearch esterno.

9b Specificare l'indirizzo IP dell'host locale seguito dall'indirizzo IP del nodo Elasticsearch locale nella proprietà `network.host` come descritto di seguito:

```
network.host: ["127.0.0.1","<indirizzo IP del nodo Elasticsearch in Sentinel>"]
```

10 (Condizionale) Per Sentinel con la memorizzazione tradizionale, aggiungere gli indirizzi dei nodi Elasticsearch esterni alla proprietà `ServerList` nel file `/etc/opt/novell/sentinel/config/elasticsearch-index.properties`.

Ad esempio: `ServerList=<IP 1 di Elasticsearch>:<Porta>,<IP 2 di Elasticsearch>:<Porta>`

11 Riavviare Sentinel:

```
rcsentinel restart
```

12 Riavviare tutti i nodi Elasticsearch:

```
/etc/init.d/elasticsearch start
```

13 Per ottimizzare le prestazioni e la stabilità del server Sentinel, configurare il nodo Elasticsearch nel server Sentinel come nodo dedicato `idoneo per il master` in modo che tutti i dati di visualizzazione degli eventi vengano indicizzati in nodi Elasticsearch esterni:

13a Eseguire il login al server Sentinel come utente novell.

13b Assicurarsi che tutti i dati esistenti degli avvisi siano stati spostati in nodi Elasticsearch esterni.

13c Aprire il file `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` e aggiungere le informazioni seguenti:

```
node.master: true
node.data: false
node.ingest: false
search.remote.connect: false
```

13d Riavviare Elasticsearch:

```
rcsentinel stopSIdb
```

```
rcsentinel startSIdb
```

14 Procedere con la “Sicurezza dei dati in Elasticsearch” a pagina 79.

Sicurezza dei dati in Elasticsearch

I nodi del cluster Elasticsearch sono accessibili tramite vari client fra i quali:

- Sentinel: per recuperare e presentare i dati degli eventi nel dashboard di visualizzazione degli eventi.
- Lavori Spark in esecuzione nei nodi YARN NodeManager: per eseguire indicizzazioni in blocco degli eventi ricevuti da Kafka (per SSDM).
- Collector Manager: per eseguire indicizzazioni in blocco degli eventi in Sentinel con la memorizzazione tradizionale.
- Altri client esterni: per eseguire operazioni personalizzate, ad esempio analisi personalizzate.

In Sentinel è disponibile un plug-in di sicurezza per Elasticsearch denominato **elasticsearch-security-plugin** che esegue l'autenticazione e autorizza l'accesso a Elasticsearch.

Nel plug-in viene utilizzato un token SAML o una white list per la convalida, a seconda della modalità di connessione dei client:

- Quando un client invia un token SAML insieme alla richiesta, il plug-in autentica il token nel server di autenticazione di Sentinel. Quando l'autenticazione ha esito positivo, il plug-in consente l'accesso solo agli eventi filtrati a cui il client è autorizzato.

  Ad esempio, nel dashboard di visualizzazione degli eventi (client) vengono visualizzati solo gli eventi provenienti da Elasticsearch che il ruolo dell'utente è autorizzato a visualizzare.

  Per informazioni sui ruoli e le autorizzazioni, vedere “Creating a Role” (Creazione di un ruolo) nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel).
- Quando un client non può inviare un token SAML, il plug-in controlla la propria white list di client legittimi. Una volta eseguita la convalida, il plug-in consente l'accesso a tutti gli eventi senza filtraggio.
- Quando un client non invia un token SAML valido o la white list non concede l'autorizzazione, il plug-in lo considera come un client non legittimo e rifiuta l'accesso.

In questa sezione vengono fornite informazioni sull'installazione e la configurazione del plug-in di sicurezza per Elasticsearch:

- “Installazione del plug-in di sicurezza per Elasticsearch” a pagina 80
- “Accesso sicuro ai client Elasticsearch aggiuntivi” a pagina 81
- “Aggiornamento della configurazione del plug-in di Elasticsearch” a pagina 82

Installazione del plug-in di sicurezza per Elasticsearch

È necessario installare il plug-in di sicurezza per Elasticsearch in ciascun nodo del cluster Elasticsearch e anche nel nodo Elasticsearch incluso in Sentinel.

Per installare elasticsearch-security-plug-in nel nodo Elasticsearch incluso in Sentinel:

1. Eseguire il login a Sentinel principale o al server SSDM.
2. Impostare il percorso della variabile di ambiente JAVA_HOME come segue:

   ```
   export JAVA_HOME=/<Sentinel_installation_path>/opt/novell/sentinel/jdk/
   ```

3. Installare il plug-in:

   Per Linux, eseguire il login come utente che esegue Elasticsearch ed eseguire il comando seguente:

   ```
   <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/
   elasticsearch-plugin install file://localhost/<Sentinel_installation_path>/
   etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip --
   verbose
   ```

   Quando viene richiesto di continuare l'installazione, immettere `y`.
4. (Condizionale) Se Elasticsearch non è in ascolto sulla porta HTTP di default (9200), è necessario aggiornare il numero di porta di Elasticsearch in tutte le voci del file `<percorso_di_installazione_di_Sentinel>>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.tx`.

Per ulteriori informazioni, consultare “Accesso ai client Elasticsearch mediante white list” a pagina 82.

5 Riavviare i servizi di indicizzazione in Sentinel utilizzando il comando:

```
rcsentinel stopSIdb
rcsentinel startSIdb
```

Per installare elasticsearch-security-plug-in in nodi Elasticsearch esterni:

Eseguire i passaggi seguenti in ciascun nodo del cluster Elasticsearch:

1 Eseguire il login a Sentinel principale o al server SSDM.

2 Copiare il file `<percorso_di_installazione_di_Sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip` in un'ubicazione temporanea in ciascun nodo del cluster Elasticsearch.

3 Installare il plug-in:

Per Linux, eseguire il login come utente che esegue Elasticsearch ed eseguire il comando seguente:

```
<elasticsearch_install_directory>/bin/elasticsearch-plugin install file://
localhost/<full path of elasticsearch-security-plugin*.zip file> --verbose
```

Quando viene richiesto di continuare l'installazione, immettere `y`.

4 (Condizionale) Se Elasticsearch non è in ascolto sulla porta HTTP di default (9200), è necessario aggiornare il numero di porta di Elasticsearch in tutte le voci del file `<directory_di_installazione_di_elasticsearch>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt`.

Per ulteriori informazioni, consultare “Accesso ai client Elasticsearch mediante white list” a pagina 82.

5 Riavviare Elasticsearch.

Accesso sicuro ai client Elasticsearch aggiuntivi

Di default, i client attendibili, quali il server SSDM (per il dashboard di visualizzazione degli eventi) e le istanze di YARN NodeManager, il server Sentinel (per il dashboard di visualizzazione degli eventi) ed RCM hanno accesso a Elasticsearch. Se si desidera utilizzare client Elasticsearch aggiuntivi, è necessario fornire un accesso sicuro a tali client aggiuntivi mediante token SAML o white list.

Accesso ai client REST di Elasticsearch mediante token SAML

Se si utilizza un client REST per accedere a Elasticsearch, è possibile includere un token SAML nell'intestazione della richiesta come segue:

1 Ottenere un token SAML dal server di autenticazione di Sentinel. Per ulteriori informazioni, vedere la documentazione delle API REST disponibile in Sentinel.

Fare clic su **Guida** > **API > Esercitazione > Sicurezza API > Ottenere un token SAML (login)**.

2 Utilizzare il token SAML nelle successive richieste REST: includere il token SAML nell'intestazione Authorization di ogni richiesta effettuata dal client REST. Specificare `Authorization` come nome dell'intestazione e utilizzare il *<token SAML>* ottenuto al passaggio 1 come valore dell'intestazione.

Accesso ai client Elasticsearch mediante white list

Di default, in Sentinel viene compilata automaticamente una white list con gli indirizzi IP dei client Elasticsearch attendibili, come il server SSDM (per il dashboard di visualizzazione degli eventi), le istanze di YARN NodeManager, il server Sentinel (per il dashboard di visualizzazione degli eventi) ed RCM. Il plug-in di sicurezza per Elasticsearch concede l'accesso a Elasticsearch a tutti i client elencati nella propria white list.

Per garantire l'accesso a client aggiuntivi che non inviano un token Sentinel valido, è necessario aggiungere l'indirizzo IP del client e il numero della porta HTTP del server Elasticsearch alla white list nel formato `indirizzo IP:porta`. È necessario accertarsi che i client esterni aggiunti alla white list siano legittimi e affidabili, al fine di impedire eventuali accessi non autorizzati.

Per aggiornare la white list:

1. Eseguire il login al server Sentinel o al nodo Elasticsearch come utente che sta eseguendo Elasticsearch.
2. Aggiungere la voce <IP_del_client_Elasticsearch>:<Porta_HTTP_di_destinazione_di_Elasticsearch> nel file:
   - `<percorso_di_installazione_di_Sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin//elasticsearch-ip-whitelist.txt` per il nodo Elasticsearch incluso in Sentinel.
   - `<directory_di_installazione_di_elasticsearch>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt` per i nodi Elasticsearch esterni.

   Se sono necessarie più voci, aggiungere ognuna di esse in una nuova riga e salvare il file.
3. Ripetere i passaggi precedenti in ciascun nodo del cluster Elasticsearch.

Aggiornamento della configurazione del plug-in di Elasticsearch

Nei casi in cui si modificano l'indirizzo IP/nome host e il numero di porta di componenti della memorizzazione scalabile o il numero di versione e il numero di porta di Elasticsearch, è necessario aggiornare i file di configurazione del plug-in di Elasticsearch di conseguenza.

Eseguire i passaggi seguenti in ciascun nodo del cluster Elasticsearch:

1. Eseguire il login al nodo Elasticsearch come l'utente che sta eseguendo Elasticsearch.
2. (Condizionale) Se si modificano gli indirizzi IP di YARN NodeManager, l'indirizzo IP di SSDM o del server Sentinel, gli indirizzi IP di RCM o il numero di porta di Elasticsearch, aggiornare la white list di conseguenza affinché il plug-in di sicurezza per Elasticsearch conceda l'accesso ai client Elasticsearch.

   Se si sta configurando SSDM o Sentinel nella modalità ad alta disponibilità, aggiungere le voci per l'indirizzo IP fisico di ciascun nodo attivo e passivo del cluster ad alta disponibilità.

   Se si modifica l'indirizzo IP fisico di uno qualsiasi dei nodi del cluster ad alta disponibilità o si aggiunge un nuovo nodo al cluster ad alta disponibilità, aggiornare la white list con gli indirizzi IP fisici dei nodi modificati o appena aggiunti.

   Per ulteriori informazioni, consultare “Accesso ai client Elasticsearch mediante white list” a pagina 82.

3 (Condizionale) Se si modifica l'indirizzo IP di SSDM, l'indirizzo IP del server Sentinel o il numero di porta del server Web, aggiornare le proprietà `authServer.host` e `authServer.port` nei file seguenti e riavviare Elasticsearch:

- `<percorso_di_installazione_di_Sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-configuration.properties` per il nodo Elasticsearch incluso in Sentinel.
- `<directory_di_installazione_di_elasticsearch>/plugins/elasticsearch-security-plugin/plugin-configuration.properties` per i nodi Elasticsearch esterni.

Se si sta configurando SSDM o Sentinel nella modalità ad alta disponibilità, impostare la proprietà `authServer.host` sull'indirizzo IP virtuale del cluster ad alta disponibilità.

Se si modifica l'indirizzo IP virtuale del cluster ad alta disponibilità, aggiornare la proprietà `authServer.host` impostando l'indirizzo IP virtuale modificato.

4 (Condizionale) Se si esegue l'upgrade di Elasticsearch a una versione più recente, aggiornare la proprietà `elasticsearch.version` nei file seguenti e riavviare Elasticsearch:

- `/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` per il nodo Elasticsearch incluso in Sentinel.
- `<directory_di_installazione_di_elasticsearch>/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` per i nodi Elasticsearch esterni.

Ottimizzazione delle prestazioni di Elasticsearch

In Sentinel viene eseguita automaticamente la configurazione delle impostazioni di Elasticsearch come riportato nella tabella seguente. È possibile personalizzare le impostazioni di Elasticsearch secondo necessità.

Per personalizzare le impostazioni di default:

Per la memorizzazione tradizionale: Aprire il file `/etc/opt/novell/sentinel/config/elasticsearch-index.properties` e aggiornare le proprietà elencate nella tabella secondo necessità.

Per la memorizzazione scalabile: Nella home page di SSDM, fare clic su **Memorizzazione** > **Storage scalabile** > **Proprietà avanzate** > **Elasticsearch**.

Tabella 12-1 *Proprietà di Elasticsearch*

Proprietà	Valore di default	Note
elasticsearch.Events.lucenefilter (facoltativo)		Specificare un filtro per inviare solo eventi specifici a Elasticsearch per l'indicizzazione. Ad esempio: se si specifica il valore sev:[3-5], vengono inviati a Elasticsearch solo gli eventi con valore di gravità compreso tra 3 e 5.

Proprietà	Valore di default	Note
index.fields	id,dt,rv171,msg,ei,evt,xdastaxname,xdasoutcomename,sev,vul,rv32,rv39,rv159,dhn,dip,rv98,dp,fn,rv199,dun,tufname,rv84,rv158,shn,sip,rv76,sun,iufname,sp,iudep,rv198,rv62,st,tid,srcgeo,destgeo,obsgeo,rv145,estz,estzmonth,estzdiy,estzdim,estzdiw,estzhour,estzmin,rv24,tudep,pn,xdasclass,xdasid,xdasreg,xdasprov,iuident,tuident	Indica i campi evento che si desidera indicizzare con Elasticsearch.
es.num.shards	5	Indica il numero di partizioni primarie per indice. È possibile aumentare questo valore di default quando le dimensioni della partizione sono superiori a 50 GB.
es.num.replicas	1	Indica il numero di partizioni di replica che ciascuna partizione primaria deve avere. Si consiglia di utilizzare un cluster con un minimo di 2 nodi considerando il failover e l'alta disponibilità.

Reinstallazione del plug-in di sicurezza per Elasticsearch

È necessario ripetere l'installazione, vale a dire disinstallare e reinstallare il plug-in di sicurezza per Elasticsearch nel nodo incluso in Sentinel e nei nodi esterni negli scenari seguenti:

- Aggiunta o modifica di indirizzi IP per istanze remote di Collector Manager.
- Disinstallazione di istanze remote di Collector Manager.
- Abilitazione della memorizzazione scalabile dopo l'installazione.

Per reinstallare il plug-in di sicurezza per Elasticsearch:

1. Eseguire il login al server Sentinel o al nodo Elasticsearch come utente che sta eseguendo Elasticsearch.
2. Disinstallare il plug-in utilizzando il seguente comando:
   - Per Elasticsearch incluso in Sentinel: `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin remove file://localhost/<percorso_di_installazione_di_Sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
   - Per Elasticsearch esterno: `<directory_di_installazione_di_elasticsearch> remove file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`

3 Reinstallare il plug-in:

- Per Elasticsearch incluso in Sentinel: `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin install file://localhost/<percorso_di_installazione_di_Sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
- Per Elasticsearch esterno: `<directory_di_installazione_di_elasticsearch>/bin/elasticsearch-plugin install file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`

4 Riavviare Elasticsearch utilizzando il comando seguente:

- Per il nodo Elasticsearch incluso in Sentinel:

  ```
  rcsentinel stopSIdb
  rcsentinel startSIdb
  ```

- Per i nodi Elasticsearch esterni:

  ```
  sudo systemctl restart elasticsearch.service
  ```

13 Installazione e configurazione della memorizzazione scalabile

Per configurare la memorizzazione scalabile come opzione di memorizzazione dati di Sentinel, eseguire le operazioni preliminari elencate nella tabella seguente:

Tabella 13-1 *Operazioni preliminari per abilitare la memorizzazione scalabile*

❒	Task	Vedere
❒	Stabilire il numero di nodi da configurare per il cluster della distribuzione Hadoop e il cluster Elasticsearch in base alla frequenza EPS e al numero di repliche necessarie. Scegliere la versione certificata di CDH ed Elasticsearch.	Informazioni tecniche su Sentinel.
❒	CDH, Elasticsearch e Sentinel dispongono di apposite matrici di supporto della piattaforma. Riesaminare la matrice di supporto di ciascuno di questi prodotti e stabilire quale piattaforma utilizzare. Per Elasticsearch, si consiglia di installare RPM poiché include lo script d'inizializzazione. Tale script installa Elasticsearch come servizio e ne abilita l'arresto e l'avvio automatici durante il riavvio e gli upgrade senza che vengano sovrascritti i file di configurazione. L'installazione dell'RPM per Elasticsearch non è supportata in SLES 11. In tal caso sarà quindi necessario scegliere una piattaforma appropriata per Elasticsearch.	Matrice di supporto di CDH nella documentazione di Cloudera. Matrice di supporto di Elasticsearch nella documentazione di Elasticsearch. Matrice di supporto di Sentinel.
❒	Installare e configurare CDH in modalità cluster.	“Installazione e configurazione di CDH” a pagina 88.
❒	Installare e configurare Elasticsearch in modalità cluster.	“Installazione e configurazione di Elasticsearch” a pagina 77.
❒	Abilitare la memorizzazione scalabile in Sentinel.	“Abilitazione della memorizzazione scalabile” a pagina 89

Installazione e configurazione di CDH

In questa sezione vengono fornite informazioni sulle impostazioni specifiche di Sentinel da eseguire durante l'installazione e la configurazione di CDH. Per informazioni dettagliate sull'installazione e la configurazione di CDH, fare riferimento alla versione certificata nella documentazione di Cloudera.

Sentinel funziona con Cloudera Express, la versione gratuita di CDH. Può essere utilizzato anche con Cloudera Enterprise, per il quale è necessario acquistare da Cloudera una licenza, che include numerose funzioni non disponibili nella versione Cloudera Express. Se si sceglie di iniziare con Cloudera Express e successivamente ci si rende conto che sono necessarie le funzionalità di Cloudera Enterprise, è possibile eseguire l'upgrade del cluster dopo aver acquistato la licenza da Cloudera.

- "Prerequisiti" a pagina 88
- "Installazione e configurazione di CDH" a pagina 89

Prerequisiti

Prima di installare CDH, è necessario configurare gli host conformemente ai prerequisiti seguenti:

- Effettuare le operazioni preliminari specificate nella documentazione di Cloudera.
- Per ottenere prestazioni migliori, si consiglia di utilizzare il file system ext4 o XFS.
- CDH necessita di alcuni pacchetti del sistema operativo che non vengono installati di default. È quindi necessario montare il DVD del rispettivo sistema operativo. Nelle istruzioni di installazione di Cloudera sono riportate le informazioni sui pacchetti da installare.
- Per i sistemi operativi SLES, è necessario il pacchetto `python-psycopg2`. Installare il pacchetto `python-psycopg2`. Per ulteriori informazioni, vedere la documentazione di openSUSE.
- Se si utilizzano macchine virtuali, quando si creano i relativi nodi, riservare lo spazio su disco necessario nel file system. Ad esempio, in VMware è possibile utilizzare il thick provisioning.
- Assicurarsi che i nodi del cluster Sentinel e CDH siano all'interno dello stesso fuso orario.
- Impostare la variabile Swappiness di tutti gli host su 1 nel file `/etc/sysctl.conf` aggiungendo la voce seguente:

  ```
  vm.swappiness=1
  ```

  Per applicare immediatamente l'impostazione, eseguire il comando seguente:

  ```
  sysctl -p
  ```

- La versione di JDK in CDH deve essere almeno uguale a quella usata in Sentinel. Se la versione di JDK disponibile in CDH è meno recente di quella di Sentinel, invece di installare il JDK disponibile nell'archivio CDH seguire le istruzioni di installazione manuale di JDK.

  Installare JDK utilizzando il file di archivio binario (`.tar.gz`), perché l'installazione dell'RPM di JDK causa problemi quando si utilizza lo script `manage_spark_jobs.sh` per inviare i lavori Spark su YARN.

  Per stabilire la versione di JDK utilizzata in Sentinel, vedere le Note di rilascio di Sentinel.

Installazione e configurazione di CDH

Installare la versione certificata di CDH. Per informazioni sulla versione certificata di CDH, consultare la pagina delle informazioni tecniche su Sentinel. Per le istruzioni di installazione, fare riferimento alla versione certificata nella documentazione di Cloudera.

Durante l'installazione di CDH, effettuare le operazioni seguenti:

- (Condizionale) Se l'installazione del database PostgreSQL incorporato ha esito negativo, effettuare i passaggi seguenti:

  ```
  mkdir -p /var/run/postgresql
  ```

  ```
  sudo chown cloudera-scm:cloudera-scm /var/run/postgresql
  ```

- Quando si sceglie il tipo di installazione del software nella finestra **Select Repository** (Selezione archivio), verificare che **Use Parcels** (Usa pacchetti) sia selezionato e scegliere Kafka in **Additional Parcels** (Pacchetti aggiuntivi).
- Quando si aggiungono nuovi servizi, assicurarsi di abilitare quelli specificati di seguito:
  - Cloudera Manager
  - ZooKeeper:
  - HDFS
  - HBase:
  - YARN
  - Spark
  - Kafka

  Nota: ai fini dell'affidabilità del sistema, il server Spark della cronologia e HDFS NameNode devono essere installati nello stesso nodo. Per informazioni sull'architettura di memorizzazione scalabile, vedere “Pianificazione per la memorizzazione scalabile” a pagina 44

  Quando si abilitano i servizi sopra menzionati, configurare l'alta disponibilità per:

  - HBase HMaster
  - HDFS NameNode
  - YARN ResourceManager
- (Condizionale) Se il programma di installazione non installa la configurazione client perché il percorso di Java è mancante, aprire una nuova sessione del browser e aggiornare manualmente il percorso di Java procedendo come segue:

  Fare clic su **Hosts** (Host) > **All Hosts** (Tutti gli host) > **Configuration** (Configurazione) e specificare il percorso corretto nel campo **Java Home Directory** (Home directory di Java).

Abilitazione della memorizzazione scalabile

È possibile abilitare la memorizzazione scalabile sia durante che dopo l'installazione di Sentinel. Quando si abilita la memorizzazione scalabile durante l'installazione, Sentinel configura i componenti di CDH con i valori di default. Alcune di queste configurazioni sono definitive e non possono essere modificate. Ad esempio, il numero di default delle partizioni per gli argomenti Kafka è 9 e non è modificabile.

Se si desidera modificare i valori di default, è necessario abilitare la memorizzazione scalabile dopo l'installazione di Sentinel per poi impostare le configurazioni dei componenti di CDH come desiderato.

Per le installazioni tradizionali, è possibile abilitare la memorizzazione scalabile sia durante che dopo l'installazione di Sentinel. Per le installazioni in modalità applicazione, è possibile abilitare la memorizzazione scalabile solo dopo l'installazione.

Nelle installazioni di upgrade, la memorizzazione scalabile può essere abilitata solo dopo aver eseguito l'upgrade di Sentinel.

Prima di abilitare la memorizzazione scalabile, tenere a portata di mano l'elenco degli indirizzi IP o dei nomi host e i numeri di porta dei nodi di Kafka, HDFS NameNode, YARN NodeManager, ZooKeeper ed Elasticsearch. Queste informazioni sono necessarie quando si abilita la memorizzazione scalabile.

Per abilitare la memorizzazione scalabile durante l'installazione di Sentinel, vedere la “Installazione personalizzata del server Sentinel” a pagina 92.

Per abilitare la memorizzazione scalabile dopo l'installazione o l'upgrade di Sentinel, vedere “Enabling Scalable Storage Post-Installation” (Abilitazione della memorizzazione scalabile dopo l'installazione) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

14 Installazione tradizionale

In questo capitolo sono riportate le informazioni relative alle varie modalità di installazione di Sentinel.

Installazione interattiva

In questa sezione sono riportate le informazioni sull'installazione standard e quella personalizzata.

Installazione standard del server Sentinel

Per effettuare un'installazione standard, utilizzare la procedura seguente:

1. Effettuare il download del file di installazione di Sentinel dal sito Web dei download di :
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 <directory_name>
   ```
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 della licenza di valutazione di default inclusa nel programma di installazione. In qualsiasi momento, durante o dopo il periodo di valutazione, è possibile sostituire la licenza di valutazione con la chiave di una 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 principale di Sentinel, specificare l'URL seguente nel browser Web:

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

Dove *IP_AddressOrDNS_Sentinel_server* è l'indirizzo IP o il nome DNS del server Sentinel e *8443* è la porta di default del server Sentinel.

Installazione personalizzata del server Sentinel

Se si esegue l'installazione di Sentinel con una configurazione personalizzata, è possibile personalizzare l'installazione specificando la propria chiave di licenza, impostando una password diversa, specificando altre porte e così via.

1 Se si desidera abilitare la memorizzazione scalabile, effettuare le operazioni preliminari specificate nel Capitolo 13, “Installazione e configurazione della memorizzazione scalabile”, a pagina 87.

2 Effettuare il download del file di installazione di Sentinel dal sito Web dei download di :

3 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.

4 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>`

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 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.

8 Specificare `2` per elaborare una configurazione personalizzata di Sentinel.

9 Immettere `1` per utilizzare la chiave della licenza di valutazione di default

oppure

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

10 Specificare la password dell'utente amministratore `admin` e confermarla nuovamente.

11 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.

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

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

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

15 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`.

16 ***Se si desidera abilitare Sentinel in modalità FIPS 140-2***, immettere `y`.

16a Specificare una password complessa per il database dell'archivio chiavi e confermarla.

Nota: la password deve essere di almeno sette caratteri. e deve contenere almeno tre dei tipi di carattere seguenti: cifre, lettere ASCII minuscole, lettere ASCII maiuscole, caratteri ASCII non alfanumerici e caratteri non ASCII.

Se si utilizza come primo carattere una lettera ASCII maiuscola o come ultimo una cifra, non vengono conteggiati.

16b Se si desidera inserire nel database dell'archivio chiavi dei certificati esterni per stabilire l'attendibilità, premere `s` e specificare il percorso del file del certificato. In caso contrario, premere `n`.

16c Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel Capitolo 24, “Esecuzione di Sentinel in modalità FIPS 140-2”, a pagina 133.

17 ***Se si desidera abilitare la memorizzazione scalabile***, immettere `yes` o `y` per abilitare la memorizzazione scalabile.

Importante: dopo aver abilitato la memorizzazione scalabile, è possibile ripristinare la configurazione solo reinstallando Sentinel.

17a Specificare gli indirizzi IP o i nomi host e i numeri di porta dei componenti della memorizzazione scalabile.

17b (Condizionale) Se si desidera uscire dalla configurazione della memorizzazione scalabile e continuare l'installazione di Sentinel, immettere `no` o `n`.

17c Al termine dell'installazione di Sentinel, eseguire la configurazione della memorizzazione scalabile come descritto nella sezione “Configurazione post-installazione per la memorizzazione scalabile” a pagina 94.

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 principale di Sentinel, specificare l'URL seguente nel browser Web:

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

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

Configurazione post-installazione per la memorizzazione scalabile

1. Eseguire il login al server SSDM.
2. Svuotare la cache del browser per visualizzare la versione di Sentinel installata.
3. Per visualizzare eventi e avvisi, aggiungere il nodo Elasticsearch incluso in SSDM al cluster Elasticsearch configurato per la memorizzazione scalabile:

   Nel nodo Elasticsearch locale, aprire il file `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` e aggiungere le seguenti informazioni:

   - cluster.name: <*nome_cluster_Elasticsearch*>
   - node.name: <*nome_nodo*>
   - discovery.zen.ping.unicast.hosts: ["<*FQDN di node1 di Elasticsearch*>", "<*FQDN di node2 di elasticsearch*>" e così via"]

   In tutti i nodi Elasticsearch esterni, aprire `/etc/elasticsearch/elasticsearch.yml` ed eseguire l'aggiornamento di

   discovery.zen.ping.unicast.hosts: ["<*FQDN di node1 di Elasticsearch*>", "<*FQDN di node2 di elasticsearch*>" e così via"]

   Nota: assicurarsi che i valori dei parametri nel file locale `elasticsearch.yml` e nel file `elasticsearch.yml` che risiede nei nodi Elasticsearch esterni siano i medesimi, fatta eccezione per `network.host` e `node.name` dato che questi valori sono univoci del nodo.

   ---

4. Riavviare i servizi di indicizzazione utilizzando il comando:

   ```
   rcsentinel stopSIdb
   rcsentinel startSIdb
   ```

5. Completare la configurazione della memorizzazione scalabile come indicato nelle sezioni seguenti:

   - “Sicurezza dei dati in Elasticsearch” a pagina 79
   - Performance Tuning Guidelines (Linee guida per l'ottimizzazione delle prestazioni) nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel)
   - Processing Data (Elaborazione dei dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel)

Installazione di Collector Manager e Correlation Engine

Per default viene eseguita l'istallazione di un'istanza di Collector Manager e di un'istanza di Correlation Engine. Per gli ambienti di produzione, configurare un'installazione distribuita poiché consente di raggruppare i componenti di raccolta dati in un computer separato, permettendo così di

gestire picchi e altre anomalie preservando la massima stabilità del sistema. Per informazioni sui vantaggi derivanti dall'installazione di componenti aggiuntivi, vedere la “Vantaggi delle installazioni distribuite” a pagina 46.

Importante: l'istanza aggiuntiva di Collector Manager o di Correlation Engine deve essere installata in sistemi separati. Tale istanza non deve risiedere nello stesso sistema in cui è installato il server Sentinel.

Elenco di controllo per l'installazione: Prima di iniziare l'installazione, verificare di aver completato i task seguenti.

- Assicurarsi che i requisiti hardware e software minimi siano soddisfatti. Per ulteriori informazioni, vedere il Capitolo 5, “Requisiti di sistema”, a pagina 37.
- Sincronizzare l'orario mediante il protocollo NTP (Network Time Protocol).
- Per un'istanza di Collector Manager è necessaria la connettività di rete alla porta bus messaggi (61616) nel server di Sentinel. Prima di iniziare il processo di installazione di Collector Manager, assicurarsi che a tutti i firewall e impostazioni di rete sia permesso comunicare su questa porta.

Per installare l'istanza di Collector Manager e di Correlation Engine, attenersi alla procedura seguente:

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

   `https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

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

   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. Fare clic su **Download del programma di installazione** in corrispondenza dell'installazione desiderata.
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.
7. Per installare l'istanza di Collector Manager o di Correlation Engine, specificare il comando seguente:

   Per Collector Manager:

   `./install-cm`

   Per Correlation Engine:

   `./install-ce`

   oppure

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

Per Collector Manager:

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

Per Correlation Engine:

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

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 Quando richiesto, specificare l'opzione appropriata per continuare con la configurazione standard o con quella personalizzata.

12 Immettere il nome host di default di Communication Server o l'indirizzo IP del computer in cui è installato Sentinel.

13 (Condizionale) Se si sceglie la configurazione personalizzata, specificare le informazioni seguenti:

13a Il numero di porta del canale di comunicazione del server Sentinel.

13b Il numero di porta del server Web Sentinel.

14 Quando richiesto, accettare il certificato ed eseguire il comando seguente nel server Sentinel per verificare il certificato:

Se in modalità FIPS:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.activemqkeystore.jks
```

Se non in modalità FIPS:

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/nonfips_backup/.activemqkeystore.jks
```

Confrontare l'output del certificato con quello del server Sentinel visualizzato mediante la procedura del Passo 12.

Nota: Se il certificato non corrisponde, l'installazione si interrompe. Configurare nuovamente l'installazione e verificare i certificati.

---

15 Se l'output del certificato corrisponde a quello del server Sentinel, accettarlo.

16 Specificare le credenziali di tutti gli utenti nel ruolo amministrativo. Immettere il nome utente e la password.

17 (Condizionale) Se si sceglie la configurazione personalizzata, immettere `yes` o `Y` per consentire la modalità FIPS 140-2 in Sentinel e continuare con la configurazione di tipo FIPS.

18 (Condizionale) Se nell'ambiente viene utilizzata l'autenticazione a più fattori o autenticazione forte, è necessario fornire l'ID del client Sentinel e il segreto del client Sentinel. Per ulteriori informazioni sui metodi di autenticazione, vedere "Authentication Methods" (Metodi di autenticazione) nella *Sentinel Administrator Guide* (Guida di amministrazione di Sentinel).

Per recuperare l'ID e il segreto client di Sentinel, visitare l'URL seguente:

`https://`*`Nomehost`*`:`*`porta`*`/SentinelAuthServices/oauth/clients`

Dove:

- *Nome host* è il nome host del server Sentinel.
- *Porta* è la porta utilizzata da Sentinel (in genere 8443).

L'URL specificato utilizza la sessione Sentinel corrente per recuperare l'ID e il segreto del client Sentinel.

19 (Condizionale) Se è stata abilitata la visualizzazione degli eventi, è necessario aggiungere alla white list di Elasticsearch l'istanza di Collector Manager. Per ulteriori informazioni, consultare "Accesso ai client Elasticsearch mediante white list" a pagina 82.

20 Continuare l'installazione seguendo le istruzioni visualizzate fino al termine della procedura.

Installazione in modalità automatica

L'installazione in modalità automatica può risultare pratica se è necessario installare più server Sentinel, istanze di Collector manager o di Correlation Engine. In uno scenario di questo tipo è possibile registrare i parametri di installazione durante l'installazione interattiva e, successivamente, eseguire il file registrato su tutti gli altri server.

Per eseguire un'installazione in modalità automatica, assicurarsi di aver registrato i parametri di installazione in un file. Per informazioni sulla creazione del file di risposta, consultare "Installazione standard del server Sentinel" a pagina 91 o "Installazione personalizzata del server Sentinel" a pagina 92 e "Installazione di Collector Manager e Correlation Engine" a pagina 94.

Per abilitare la modalità FIPS 140-2 in Sentinel, accertarsi che il file di risposta includa i parametri seguenti:

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

Per eseguire l'installazione in modalità automatica, utilizzare la procedura seguente:

1 Effettuare il download dei file di installazione dal sito Web dei download di .

2 Eseguire il login come utente `root` al server in cui si desidera installare Sentinel, l'istanza di Collector manager o di Correlation Engine.

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 eseguire l'installazione in modalità batch, specificare il comando seguente:

Per server Sentinel:

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

Per Collector Manager:

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

Per Correlation Engine:

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

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

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.

5 **(Condizionale) Se si sceglie di abilitare la modalità FIPS 140-2 per il server Sentinel,**

Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel Capitolo 24, “Esecuzione di Sentinel in modalità FIPS 140-2”, a pagina 133.

Installazione di Sentinel come utente non root

Se la policy della propria organizzazione non consente di eseguire l'installazione completa di Sentinel come utente `root`, l'installazione può essere effettuata come utente `non root`, vale a dire come utente `novell`. In questo tipo di installazione alcuni passaggi vengono eseguiti come utente `root` per poi continuare l'installazione di Sentinel come utente `novell` creato dall'utente `root`. L'utente `root`, alla fine, completa l'installazione.

Quando si installa Sentinel come utente `non root` è necessario eseguire l'installazione come utente novell. Le installazioni non root, eccetto l'utente novell, non sono supportate, sebbene la procedura abbia esito positivo.

Nota: Se si installa Sentinel in una directory esistente non di default, assicurarsi che l'utente novell disponga delle autorizzazioni necessarie su tale directory. Eseguire il comando seguente per assegnare le autorizzazioni di proprietà:

`chown novell:novell <non-default installation directory>`

---

1 Effettuare il download dei file di installazione dal sito Web dei download di .

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 passare all'utente non root appena creato, vale a dire `novell`:

```
su novell
```

7 (Condizionale) Per eseguire un'installazione interattiva:

7a Specificare il comando appropriato in base al componente che si sta installando:

Componente	Comando
Server Sentinel	**ubicazione di default:** `./install-sentinel`
	ubicazione diversa da quella di default: `./install-sentinel --location=/foo`
Collector Manager	**ubicazione di default:** `./install-cm`
	ubicazione diversa da quella di default: `./install-cm --location=/foo`
Correlation Engine	**ubicazione di default:** `./install-ce`
	ubicazione diversa da quella di default: `./install-cm --location=/foo`

7b Continuare con Passo 9.

8 (Condizionale) 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 “Installazione standard del server Sentinel” a pagina 91 o “Installazione personalizzata del server Sentinel” a pagina 92.

Per eseguire un'installazione in modalità automatica:

8a Specificare il comando appropriato in base al componente che si sta installando:

Componente	Comando
Server Sentinel	**ubicazione di default:** `./install-sentinel -u <file_risposta>`
	ubicazione diversa da quella di default: `./install-sentinel --location=/foo -u <file_risposta>`
Collector Manager	**ubicazione di default:** `./install-cm -u <file_risposta>`
	ubicazione diversa da quella di default: `./install-cm --location=/foo -u <file_risposta>`
Correlation Engine	**ubicazione di default:** `./install-ce -u <file_risposta>`
	ubicazione diversa da quella di default: `./install-ce --location=/foo -u <file_risposta>`

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 “Installazione standard del server Sentinel” a pagina 91.
- Se si sceglie di procedere con la configurazione personalizzata, continuare con Passo 8 mediante Passo 15 in “Installazione personalizzata del server Sentinel” a pagina 92.

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 principale di Sentinel, specificare l'URL seguente nel browser Web:

`https://`*`IP_AddressOrDNS_Sentinel_server`*`:`*`8443`*`/sentinel/views/main.html`

Dove *IP_AddressOrDNS_Sentinel_server* è l'indirizzo IP o il nome DNS del server Sentinel e *8443* è la porta di default per il server Sentinel.

15 Installazione in modalità applicazione

L'applicazione Sentinel è un'applicazione software pronta per l'esecuzione in base al framework dell'applicazione comune Micro Focus. L'applicazione unisce un sistema operativo SLES 12 SP 3 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 sfruttare gli investimenti realizzati dal cliente. L'applicazione Sentinel fornisce un'interfaccia utente basata sul Web per configurare e monitorare l'applicazione.

L'immagine dell'applicazione Sentinel è racchiusa in un pacchetto in formato ISO oppure OVF che può essere installato negli ambienti virtuali. Per ulteriori informazioni sulle piattaforme di virtualizzazione supportate, vedere il sito Web delle informazioni tecniche di Sentinel.

Prerequisiti

Verificare che l'ambiente in cui si intende installare Sentinel come applicazione ISO sia conforme ai requisiti seguenti:

- Prima d'installare l'applicazione Sentinel, esaminare le nuove funzionalità e i problemi noti illustrati nelle Note di rilascio del sistema SLES certificato.
- (Condizionale) Se si sta eseguendo l'installazione dell'applicazione Sentinel in formato ISO nell'hardware fisico, effettuare il download dell'immagine disco ISO dell'applicazione dal sito del supporto, decomprimere il file e creare un DVD.
- Affinché il programma d'installazione possa presentare la proposta di partizione automatica, verificare che lo spazio sul disco rigido sia di almeno 50 GB.
- Verificare che il sistema disponga di una memoria minima di 4 GB per il completamento dell'installazione. Se la quantità di memoria inferiore a 4 GB, l'installazione non riuscirà. Se la quantità di memoria disponibile è superiore a 4 GB ma inferiore a 24 GB, l?installazione visualizzerà un messaggio per notificare che la quantità di memoria a disposizione è inferiore a quella consigliata.

Installazione dell'applicazione Sentinel ISO

In questa sezione sono riportate le informazioni necessarie per l'installazione di Sentinel e delle istanze di Collector Manager e di Correlation Engine mediante l'immagine ISO dell'applicazione. Questo formato consente di generare un'immagine disco completa che può essere installata direttamente nell'hardware, sia fisico che virtuale (macchina virtuale non installata in un Hypervisor) utilizzando un'immagine DVD ISO avviabile.

Installazione di Sentinel

Per installare l'applicazione Sentinel ISO:

1. Effettuare il download dell'immagine ISO virtuale dell'applicazione dal sito Web dei download di .
2. (Condizionale) Se si utilizza un Hypervisor:

   Configurare la macchina virtuale utilizzando l'immagine ISO virtuale dell'applicazione e attivarla.

   oppure

   Copiare l'immagine ISO su un DVD, configurare la macchina virtuale utilizzando il DVD e attivarla.
3. (Condizionale) Se si sta eseguendo l'installazione dell'applicazione Sentinel nell'hardware fisico:
   - **3a** Inserire il DVD e avviare il computer fisico dall'unità DVD.
   - **3b** Seguire le istruzioni dell'installazione guidata visualizzate sullo schermo.
   - **3c** Selezionare **Installa server Sentinel < *versione* >**.
4. Selezionare la lingua desiderata.
5. Selezionare il layout della tastiera.
6. Fare clic su **Avanti**.
7. Leggere e accettare il contratto di licenza di SUSE Enterprise Server Software. Fare clic su **Avanti**
8. Leggere e accettare il contratto di licenza dell'applicazione server Sentinel. Fare clic su **Avanti**
9. Impostare le password dell'applicazione Sentinel, la configurazione NTP e il fuso orario.

   Impostare le credenziali utente `vaadmin` per eseguire il login alla console di gestione dell'applicazione Sentinel.

   Nota: Dopo l'installazione, è possibile modificare la configurazione NTP e il fuso orario nei seguenti modi:

   - Accedere al prompt dei comandi e immettere `yast -> Servizi di rete -> Configurazione NTP`
   - Accedere alla aonsole di gestione dell'applicazione Sentinel e fare clic su **Ora**.

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

   ```
   rcntp restart
   ```

   ---
10. Nella pagina Impostazioni di rete applicazione server Sentinel, specificare il nome host e il nome di dominio. Selezionare **Indirizzo IP statico** o **Indirizzo IP DHCP**.
11. Fare clic su **Avanti**.
12. (Condizionale) Se al passaggio 10 è stato selezionato **Indirizzo IP statico**, specificare le impostazioni della connessione di rete.
13. Fare clic su **Avanti**.
14. Impostare la password per l'utente Sentinel `admin`, quindi fare clic su **Avanti**.

    L'applicazione viene installata.
15. Annotare l'indirizzo IP dell'applicazione mostrato nella console.
16. Eseguire il login come `root` utente dalla console per eseguire il login all'applicazione.

Immettere il nome utente come `root` e immettere la password impostata in Passo 9.

17 Procedere con la “Configurazione dell'applicazione successiva all'installazione” a pagina 106.

Installazione di istanze di Collector Manager e di Correlation Engine

La procedura di installazione per un'istanza di Collector Manager o di Correlation Engine è uguale,tranne per il fatto che è necessario effettuare il download del file dell'applicazione ISO corrispondente dal sito Web dei download.

1 Eseguire i passaggi da 1 a 13 della “Installazione di Sentinel” a pagina 102.

   L'installazione controlla la quantità di memoria e spazio su disco disponibile. Se la quantità di memoria disponibile è inferiore a 1 GB, l'installazione non consente di continuare e il pulsante **Avanti** viene disattivato.

2 Per installare l'istanza di Collector Manager o di Correlation Manager, specificare la configurazione seguente:

   - **Nome host o indirizzo IP del server Sentinel:** specificare il nome host o l'indirizzo IP del server Sentinel al quale l'istanza di Collector Manager o di Correlation Engine deve connettersi.
   - **Porta del canale di comunicazione di Sentinel:** specificare il numero di porta del canale di comunicazione del server Sentinel. Il numero di porta di default è `61616`.
   - **Numero di porta del server Web Sentinel:** Specificare la porta del server Web Sentinel. La porta di default è la 8443.
   - **Nome utente con ruolo amministrativo:** Specificare il nome utente degli utenti che ricoprono un ruolo amministrativo.
   - **Password per utente con ruolo amministrativo:** specificare la password per il nome utente immesso nel campo precedente.

3 (Condizionale) Se nell'ambiente viene utilizzata l'autenticazione a più fattori o autenticazione forte, è necessario fornire l'ID del client Sentinel e il segreto del client Sentinel. Per ulteriori informazioni sui metodi di autenticazione, vedere “Authentication Methods” (Metodi di autenticazione) nella *Sentinel Administrator Guide* (Guida di amministrazione di Sentinel).

   Per recuperare l'ID e il segreto client di Sentinel, visitare l'URL seguente:

   `https://Nomehost:porta/SentinelAuthServices/oauth/clients`

   Dove:

   - *Nome host* è il nome host del server Sentinel.
   - *Porta* è la porta utilizzata da Sentinel (in genere 8443).

   L'URL specificato utilizza la sessione Sentinel corrente per recuperare l'ID e il segreto del client Sentinel.

4 Fare clic su **Avanti**.

5 Quando richiesto, accettare il certificato.

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

   Sulla console viene visualizzato un messaggio che include il tipo di applicazione (Collector Manager o Correlation Engine di Sentinel, a seconda del componente che si è scelto di installare) e l'indirizzo IP. Viene inoltre visualizzato l'indirizzo IP dell'interfaccia utente del server Sentinel.

7 Completare Passo 16 mediante Passo 17 in “Installazione di Sentinel” a pagina 102.

Installazione dell'applicazione Sentinel OVF

In questa sezione sono riportate le informazioni necessarie per installare Sentinel, Collector Manager e Correlation Engine come immagine dell'applicazione OVF.

Il formato OVF è un formato standard per macchine virtuali supportato dalla maggior parte degli Hypervisor, sia direttamente che tramite una semplice conversione. Sentinel supporta l'applicazione in formato OVF con due Hypervisor certificati, ma è possibile utilizzarla anche con altri Hypervisor.

- "Installazione di Sentinel" a pagina 104
- "Installazione di istanze di Collector Manager e di Correlation Engine" a pagina 105

Installazione di Sentinel

Per installare l'applicazione Sentinel OVF:

1. Effettuare il download dell'immagine virtuale dell'applicazione OVF dal sito Web dei download di .
2. Nella console di gestione dell'Hypervisor in uso, importare il file dell'immagine OVF come nuova macchina virtuale. Se viene visualizzato il messaggio di richiesta, consentire all'Hypervisor di convertire l'immagine OVF nel formato nativo.
3. Controllare le risorse hardware virtuali allocate alla nuova macchina virtuale per accertarsi che siano conformi ai requisiti di Sentinel.
4. Accendere la macchina virtuale.
5. Selezionare la lingua desiderata.
6. Selezionare il layout della tastiera.
7. Fare clic su **Avanti**.
8. Leggere e accettare il contratto di licenza di SUSE Enterprise Server Software. Fare clic su **Avanti**.
9. Leggere e accettare il contratto di licenza dell'applicazione server Sentinel. Fare clic su **Avanti**.
10. Impostare le password dell'applicazione Sentinel, della configurazione e il fuso orario.

    Impostare le credenziali utente `vaadmin` per eseguire il login alla console di gestione dell'applicazione Sentinel.

    Nota: Dopo l'installazione, è possibile modificare la configurazione NTP e il fuso orario nei seguenti modi:

    - Accedere al prompt dei comandi e immettere `yast -> Servizi di rete -> Configurazione NTP`
    - Accedere alla aonsole di gestione dell'applicazione Sentinel e fare clic su **Ora**.

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

    ```
    rcntp restart
    ```

    ---

11. Nella pagina Impostazioni di rete applicazione server Sentinel, specificare il nome host e il nome di dominio. Selezionare **Indirizzo IP statico** o **Indirizzo IP DHCP**.
12. Fare clic su **Avanti**.
13. (Condizionale) Se al passaggio 11 è stato selezionato **Indirizzo IP statico**, specificare le impostazioni della connessione di rete.

14 Fare clic su **Avanti**.

15 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.

16 Annotare l'indirizzo IP dell'applicazione mostrato nella console. Per accedere all'interfaccia principale di Sentinel, utilizzare lo stesso indirizzo IP.

Installazione di istanze di Collector Manager e di Correlation Engine

Per installare un'istanza di Collector Manager o di Correlation Engine in un server VMware ESX come immagine dell'applicazione OVF:

1 Eseguire i passaggi da 1 a 14 della “Installazione di Sentinel” a pagina 104.

L'installazione controlla la quantità di memoria e spazio su disco disponibile. Se la quantità di memoria disponibile è inferiore a 1 GB, l'installazione non consente di continuare e il pulsante **Avanti** viene disattivato.

2 Specificare il nome host/indirizzo IP del server Sentinel al quale l'istanza di Collector Manager deve connettersi.

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

4 Specificare le credenziali di tutti gli utenti nel ruolo amministrativo. Immettere il nome utente e la password.

5 (Condizionale) Se nell'ambiente viene utilizzata l'autenticazione a più fattori o autenticazione forte, è necessario fornire l'ID del client Sentinel e il segreto del client Sentinel. Per ulteriori informazioni sui metodi di autenticazione, vedere “Authentication Methods” (Metodi di autenticazione) nella *Sentinel Administrator Guide* (Guida di amministrazione di Sentinel).

Per recuperare l'ID e il segreto client di Sentinel, visitare l'URL seguente:

`https://`*`Nomehost`*`:`*`porta`*`/SentinelAuthServices/oauth/clients`

Dove:

- *Nome host* è il nome host del server Sentinel.
- *Porta* è la porta utilizzata da Sentinel (in genere 8443).

L'URL specificato utilizza la sessione Sentinel corrente per recuperare l'ID e il segreto del client Sentinel.

6 Fare clic su **Avanti**.

7 Accettare il certificato.

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

Al termine dell'installazione viene visualizzato un messaggio che include il tipo di applicazione (Collector Manager o Correlation Engine di Sentinel, a seconda del componente che si è scelto di installare) e l'indirizzo IP. Viene, inoltre, visualizzato l'indirizzo IP dell'interfaccia utente del server Sentinel.

Configurazione dell'applicazione successiva all'installazione

Dopo aver installato Sentinel è necessario effettuare ulteriori configurazioni affinché l'applicazione funzioni correttamente.

Registrazione degli aggiornamenti

È necessario registrare l'applicazione Sentinel con il canale di aggiornamento dell'applicazione alla ricezione di Sentinel e gli aggiornamenti più recenti del sistema operativo. Per registrare l'applicazione, ottenere prima di tutto il codice di registrazione o la chiave di attivazione dal servizio di assistenza clienti .

Registrazione tramite la console di gestione dell'applicazione Sentinel

Se si utilizza SLES 12 SP3, è possibile registrare gli aggiornamenti tramite la console di gestione dell'applicazione Sentinel.

1. Avviare l'applicazione Sentinel effettuando una delle seguenti operazioni:
   - Eseguire il login a fare clic su Sentinel **Sentinel principale** > **Applicazione**.
   - Specificare l'URL seguente nel browser Web: `https://<Indirizzo_IP>:9443`.
2. Eseguire il login come un utente `vaadmin` o `root`.
3. Fare clic su **Aggiornamento online** > **Registra ora**.
4. Nel campo **E-mail**, specificare l'ID e-mail al quale ricevere aggiornamenti,
5. Nel campo **Chiave di attivazione**, immettere il codice di registrazione.
6. Fare clic su **Registra** per completare la registrazione.

Registrazione mediante comandi

Se si utilizza SLES 11 SP4 o SLES 12 SP3, è possibile eseguire la registrazione mediante comandi.

Per registrarsi per gli aggiornamenti

1. Eseguire il login al server Sentinel come utente `root`.
2. Specificare i seguenti comandi:
   - Per registrare il server, specificare: `suse_register -a regcode-sentinel="<codice_di_registrazione>" -a email="<ID_email>"`
   - Per registrare Collector Manager, specificare: `suse_register -a regcode-sentinel-collector="<codice_di_registrazione>" -a email="<ID_emaIl>"`

- Per registrare Correlation Engine, specificare: `suse_register -a regcode-sentinel-correlation ="<codice_di_registrazione>" -a email="<ID_email>"`
- Per registrare Sentinel in configurazione ad alta disponibilità, specificare: `suse_register -a regcode-sentinel-ha ="<codice_di_registrazione>" -a email="<ID_email>"`

Per quanto riguarda il parametro e-mail, specificare l'ID e-mail al quale ricevere aggiornamenti,

Creazione di partizioni per la memorizzazione tradizionale

Utilizzare le informazioni contenute in questa sezione solo se come opzione di memorizzazione dati si desidera usare la memorizzazione tradizionale.

Come best practice, è opportuno creare partizioni separate per memorizzare i dati di Sentinel in una partizione diversa da quella utilizzata per file eseguibili, di configurazione e del sistema operativo. La memorizzazione in una partizione separata dei dati variabili facilita il backup di set di file e il recupero in caso di danneggiamento, oltre a garantire maggiore solidità in caso di riempimento di una partizione del disco. Per informazioni sulla pianificazione delle partizioni, vedere la “Pianificazione per la memorizzazione tradizionale” a pagina 41. È possibile aggiungere partizioni nell'applicazione e spostarvi una directory mediante lo strumento YaST.

La procedura seguente consente di creare una nuova partizione e di 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.

   Per informazioni sulla creazione delle partizioni, vedere Using the YaST Partitioner (Utilizzo della modalità di partizionamento di YaST) nella *documentazione di SLES 11*.
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. Per riavviare l'applicazione Sentinel, eseguire il comando seguente:

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

Configurazione della memorizzazione scalabile

Per abilitare e configurare la memorizzazione scalabile come opzione di memorizzazione dati, vedere “Configuring Scalable Storage” (Configurazione della memorizzazione scalabile) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

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 Customer Center che offre importanti funzionalità.

Prerequisiti

Prima di configurare l'applicazione con SMT, verificare di aver soddisfatto i prerequisiti seguenti:

- Ottenere le credenziali di Customer Center per ricevere gli aggiornamenti di Sentinel. Per ulteriori informazioni su come ottenere le credenziali, rivolgersi al supporto tecnico.
- Assicurarsi che nel computer in cui si desidera installare SMT, SLES 11 SP3 sia installato con i pacchetti seguenti:
  - htmldoc
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - perl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - yum-metadata-parser
  - createrepo
  - 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 nella documentazione di SMT:
    - 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` nel computer in cui risiede l'applicazione.

Configurazione dell'applicazione

Per configurare l'applicazione con SMT, effettuare i passaggi seguenti:

1. Abilitare gli archivi dell'applicazione eseguendo i comandi seguenti nel server SMT:

   ```
   smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64
   smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64
   smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64
   ```

2. Configurare l'applicazione con SMT eseguendo i passaggi descritti nella sezione “Configuring Clients to Use SMT” (Configurazione del client per utilizzare SMT) nella documentazione di SMT.

Esecuzione dell'upgrade dell'applicazione

Per informazioni sull'upgrade dell'applicazione, vedere la “Esecuzione dell'upgrade di Sentinel” a pagina 159.

16 Installazione di servizi di raccolta e connettori aggiuntivi

Per default, tutti i servizi di raccolta e connettori rilasciati vengono installati al momento dell'installazione di Sentinel. Se si desidera installare un nuovo servizio di raccolta o un connettore rilasciato successivamente alla versione di Sentinel in uso, utilizzare le informazioni riportate nelle sezioni seguenti.

Installazione di un servizio di raccolta

Per installare un servizio di raccolta, utilizzare la procedura seguente:

1. Effettuare il download del servizio di raccolta desiderato dal sito Web dei plug-in di Sentinel.
2. Da **Sentinel Main**, fare clic sul menu a discesa **admin** e successivamente su **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**, quindi scegliere **Strumenti** > **Importa plug-in**.
5. 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**.
6. Rispondere alle richieste rimanenti, quindi fare clic su **Fine**.

Per configurare il servizio di raccolta, consultare la relativa documentazione specifica disponibile sul sito Web dei plug-in di Sentinel.

Installazione di un connettore

Per installare un connettore, utilizzare la procedura seguente:

1. Effettuare il download del connettore desiderato dal sito Web dei plug-in di Sentinel.
2. Da **Sentinel Main**, fare clic sul menu a discesa **admin** e successivamente su **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**, quindi scegliere **Strumenti** > **Importa plug-in**.
5. Individuare e selezionare il file relativo al connettore di cui è stato effettuato il download in Passo 1, quindi fare clic su **Avanti**.
6. Rispondere alle richieste rimanenti, quindi fare clic su **Fine**.

Per configurare il connettore, consultare la relativa documentazione specifica disponibile sul sito Web dei plug-in di Sentinel.

17 Verifica dell'installazione

È possibile verificare se l'installazione è stata eseguita correttamente effettuando una delle operazioni seguenti:

- Verifica della versione di Sentinel:

  ```
  /etc/init.d/sentinel version
  ```

- Verificare se i servizi Sentinel sono attivi, in esecuzione e se funzionano in modalità FIPS o meno:

  ```
  /etc/init.d/sentinel status
  ```

- Verifica dell'attivazione ed esecuzione dei servizi Web:

  ```
  netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  Il numero di porta di default è 8443.

- Avviare Sentinel:

  1. Avviare un browser Web supportato.
  2. Specificare l'URL di Sentinel:

     ```
     https://IP_AddressOrDNS_Sentinel_server:8443
     ```

     Dove *IP_AddressOrDNS_Sentinel_server* è l'indirizzo IP o il nome DNS del server Sentinel e *8443* è la porta di default per il server Sentinel.
  3. Eseguire il login con il nome utente e la password dell'amministratore specificati durante l'installazione. Il nome utente di default è admin.

IV Configurazione di Sentinel

In questa sezione sono riportate le informazioni necessarie per configurare Sentinel e i plug-in pronti all'uso.

18 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. In questa sezione sono riportate le informazioni relative all'orario, su come eseguire la configurazione e su come gestire i fusi orario in Sentinel.

L'orario in Sentinel

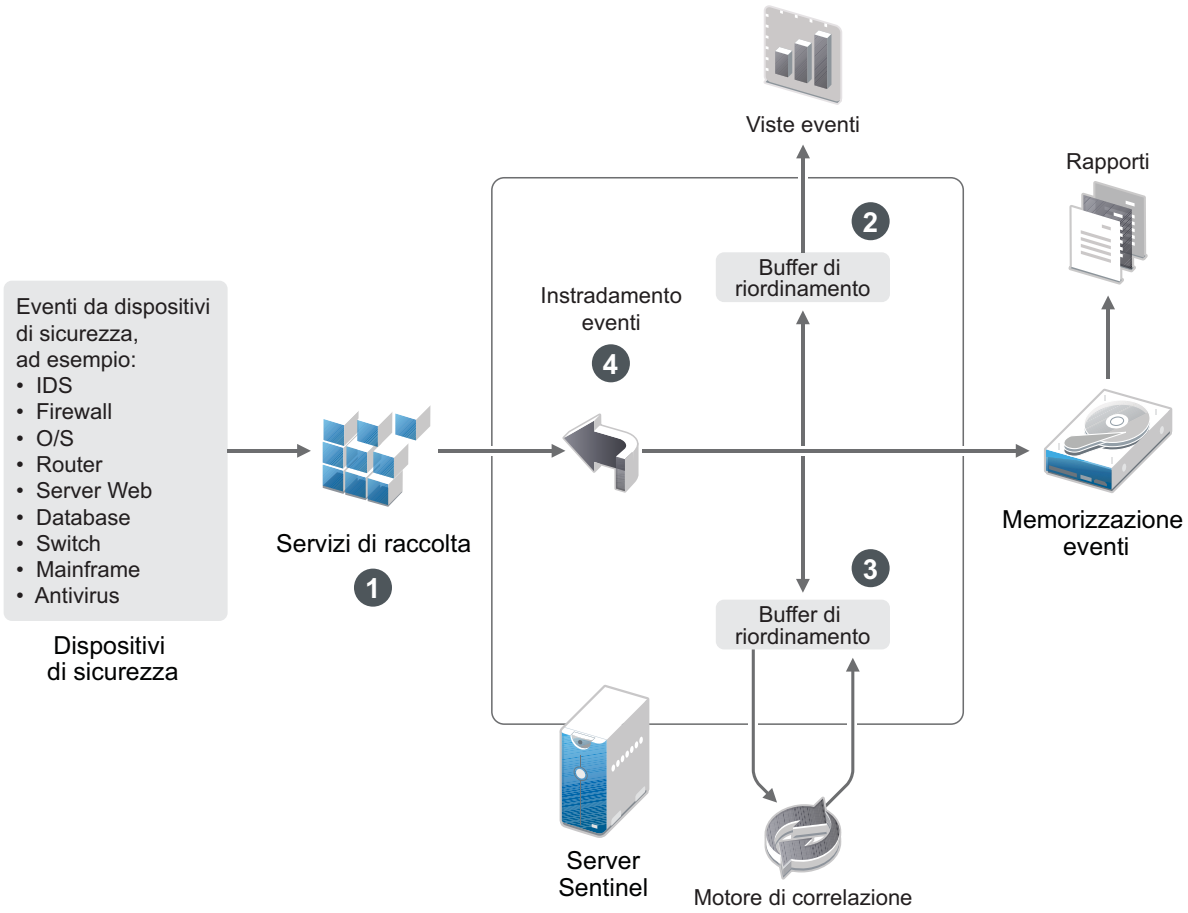
Sentinel è un sistema distribuito e consiste in diversi processi che possono essere realizzati in varie parti della rete. L'origine eventi potrebbe inoltre indurre alcuni ritardi. Per gestire al meglio tale situazione, prima dell'elaborazione i processi di Sentinel riordinano gli eventi in un flusso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

Per ogni evento sono disponibili tre campi:

- **Orario evento:** orario dell'evento utilizzato da tutti i motori di analisi, le ricerche, i rapporti e così via.
- **SentinelProcessTime:** orario in cui Sentinel ha acquisito i dati dal dispositivo e derivante dall'orario di sistema di Collector Manager.
- **ObserverEventTime:** registrazione dell'orario che il dispositivo inserisce nei dati. Non sempre i dati contengono una registrazione dell'orario affidabile ed essa potrebbe essere notevolmente diversa dall'orario di SentinelProcessTime, ad esempio quando il dispositivo fornisce i dati in batch.

Nell'illustrazione seguente si descrive come Sentinel esegue questa operazione in una configurazione con memorizzazione tradizionale:

Figura 18-1 *Orario Sentinel*



1. Per default, il campo EventTime è impostato sul valore di SentinelProcessTime. La condizione ideale è quella in cui EventTime corrisponde a ObserverEventTime, qualora esso sia disponibile e affidabile. È consigliabile configurare la raccolta dati su **Ora origine evento di fiducia**, qualora l'orario del dispositivo sia disponibile, accurato e analizzato sintatticamente nel modo adeguato dal servizio di raccolta. Il servizio di raccolta imposta EventTime affinché corrisponda a ObserverEventTime.
2. Gli eventi con EventTime compreso entro un intervallo di 5 minuti precedenti o successivi all'orario del server vengono elaborati normalmente dalle viste eventi. Gli eventi con EventTime oltre i 5 minuti successivi non vengono visualizzati nelle viste eventi, ma inseriti nella memorizzazione eventi. Gli eventi con EventTime oltre i 5 minuti successivi e meno di 24 ore precedenti vengono comunque mostrati nei grafici, ma non sono visualizzati nei dati degli eventi di tali grafici. Per recuperare quegli eventi dalla memorizzazione eventi, è necessario eseguire il drill-down.
3. Gli eventi vengono ordinati in intervalli di 30 secondi, affinché possano essere elaborati dall'istanza di Correlation Engine in ordine cronologico. Se EventTime è anteriore a 30 secondi rispetto all'orario del server, l'istanza di Correlation Engine non elabora gli eventi.
4. Se EventTime è anteriore a 5 minuti rispetto all'orario di sistema di Collector Manager, gli eventi vengono direttamente instradati alla relativa memorizzazione, ignorando i sistemi in tempo reale quali Correlation Engine e Security Intelligence.

Configurazione dell'orario in Sentinel

L'istanza di Correlation Engine 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 nell'istanza di Collector Manager e deselezionare **Ora origine evento elemento attendibile** nell'origine evento presente in Gestione origini eventi. L'istanza di Collector Manager 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 *Sentinel 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.

Configurazione della soglia di ritardo degli eventi

Quando Sentinel riceve gli eventi dalle origini eventi, è possibile che si verifichi un ritardo fra il momento in cui l'evento viene generato e quello in cui Sentinel lo elabora. In Sentinel gli eventi con ritardi prolungati vengono memorizzati in partizioni separate. La presenza di numerosi eventi con ritardi prolungati può essere un'indicazione di configurazione errata dell'origine eventi. Tale condizione potrebbe inoltre ridurre le prestazioni di Sentinel, in quanto sarà occupato a tentare di gestire gli eventi ritardati. Poiché gli eventi ritardati potrebbero essere la conseguenza di un errore di configurazione e, in tal caso, non sarebbe opportuno memorizzarli, in Sentinel è possibile configurare la soglia di ritardo accettabile per gli eventi in entrata. Il router degli eventi rimuoverà quelli che superano la soglia di ritardo. La soglia di ritardo deve essere specificata nella proprietà seguente del file `configuration.properties`:

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

È inoltre possibile registrare periodicamente nel file di log del server Sentinel un elenco delle origini eventi da cui sono stati ricevuti eventi con un ritardo superiore alla soglia specificata. Per registrare queste informazioni, specificare la soglia nella proprietà seguente del file `configuration.properties`:

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

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, l'istanza di Collector Manager 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.

Nel secondo scenario, se vengono utilizzati ID di fuso orario in formato lungo oppure offset, è possibile passare al formato UTC per recuperare l'orario UTC assoluto canonico (memorizzato in DeviceEventTime), ma anche calcolare i campi ObserverTZ dell'ora locale. Se viene utilizzato l'ID del fuso orario in formato abbreviato, potrebbero generarsi dei conflitti potenziali.

Il terzo scenario richiede che l'amministratore imposti manualmente il fuso orario dell'origine eventi per tutte le origini interessate, affinché Sentinel sia in grado di calcolare correttamente 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 nell'istanza di Collector Manager. 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 dall'istanza di Collector Manager al server Sentinel e memorizzate nella memorizzazione eventi. Il fuso orario in cui si trova l'istanza di Collector Manager 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, UTC EventTime viene convertito nell'ora locale del browser, affinché tutti gli eventi vengano 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.

19 Sicurezza dei dati in Elasticsearch

Sentinel utilizza Kibana, un dashboard di ricerca e analisi basato su browser che facilita la visualizzazione di eventi e avvisi nei dashboard. Sentinel memorizza e indicizza gli avvisi in Elasticsearch. È possibile configurare Sentinel affinché memorizzi e indicizzi gli eventi anche in Elasticsearch, così da sfruttarne le funzionalità di visualizzazione degli eventi. I dashboard di Sentinel accedono ai dati provenienti da Elasticsearch per presentare avvisi ed eventi. Per garantire che i dashboard visualizzino solo i dati che il ruolo dell'utente è autorizzato a visualizzare e per impedire l'accesso non autorizzato ai dati in Elasticsearch, è necessario installare il plug-in di sicurezza per Elasticsearch. Per ulteriori informazioni, consultare “Sicurezza dei dati in Elasticsearch” a pagina 79.

20 Abilitazione della visualizzazione degli eventi

Nelle configurazioni con memorizzazione scalabile, le visualizzazioni degli eventi sono disponibili di default. Nelle configurazioni con memorizzazione tradizionale, le visualizzazioni degli eventi sono disponibili solo se è abilitato l'archivio dati di visualizzazione (Elasticsearch) per memorizzare e indicizzare i dati.

Prerequisito

Per l'indicizzazione scalabile e distribuita degli eventi in ambienti di produzione, è necessario configurare ulteriori nodi Elasticsearch in modalità cluster. Per installare e configurare Elasticsearch in modalità cluster, vedere “Installazione e configurazione di Elasticsearch” a pagina 77.

Abilitazione della visualizzazione degli eventi

Per abilitare la visualizzazione degli eventi:

1. Eseguire il login al server Sentinel come utente novell.
2. Aprire il file `/etc/opt/novell/sentinel/config/configuration.properties`.
3. Impostare `eventvisualization.traditionalstorage.enabled` su `true`.
4. Aggiornare l'interfaccia utente dopo alcuni minuti per visualizzare le visualizzazioni degli eventi.

   Nell'interfaccia utente **Mio Sentinel** tutti i dashboard dovrebbero apparire abilitati. Avviare un dashboard, ad esempio Ricerca minacce, e fare clic su **Cerca**. Il dashboard visualizza tutti gli eventi generati nell'ultima ora.
5. (Facoltativo) I dashboard di visualizzazione degli eventi visualizzano solo gli eventi elaborati dopo aver abilitato la visualizzazione degli eventi. Per visualizzare gli eventi esistenti presenti nella memorizzazione basata su file, è necessario eseguire la migrazione dei dati dalla memorizzazione basata su file a Elasticsearch. Per ulteriori informazioni, consultare Capitolo 33, “Migrazione dei dati in Elasticsearch”, a pagina 183.

Nota: l'abilitazione o la disabilitazione della visualizzazione degli eventi genera un'eccezione, poiché riavvia i servizi d'indicizzazione di Sentinel. L'eccezione è prevista e può essere ignorata.

---

21 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 è disponibile nella cartella `\opt\novell\sentinel\setup`.

1. Chiudere Sentinel utilizzando il comando seguente:

   ```
   rcsentinel stop
   ```

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

   ```
   ./configure.sh
   ```

3. Immettere `1` per eseguire una configurazione di Sentinel standard oppure `2` per eseguirne una personalizzata.
4. Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.
5. 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.
6. Immettere `1` per utilizzare la chiave della licenza di valutazione di default

   oppure

   Immettere `2` per inserire una chiave di licenza di Sentinel acquistata.
7. 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 8.
   - Se si desidera cambiare la password esistente, immettere `2`, specificare la nuova password, confermarla, quindi continuare con Passo 8.

     L'utente `admin` rappresenta l'identità utilizzata per eseguire i task di amministrazione mediante l'interfaccia principale di Sentinel, inclusa la creazione di altri account utente.
8. 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 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. 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 10.

- Se si desidera cambiare la password esistente, immettere `2`, specificare la nuova password, confermarla, quindi continuare con Passo 10.

  L'account `appuser` rappresenta l'identità interna che il processo Java di Sentinel utilizza per stabilire la connessione e interagire con il database. La password che si immette in questa posizione viene utilizzata per eseguire i task del database.

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

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

12 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`.

22 Configurazione dei plug-in pronti all'uso

In Sentinel sono preinstallati i plug-in di default disponibili al momento del rilascio.

In questo capitolo sono riportate le informazioni necessarie per la configurazione dei plug-in pronti all'uso.

Visualizzazione dei plug-in preinstallati

È possibile visualizzare l'elenco dei plug-in preinstallati in Sentinel, oltre alle relative versioni e altri metadati, utili per stabilire se si dispone della versione più recente di un plug-in.

Per visualizzare i plug-in installati nel server Sentinel:

1. Eseguire il login all'interfaccia principale di Sentinel come amministratore all'indirizzo `https://<Indirizzo IP>:8443`, in cui 8443 è la porta di default del server Sentinel.
2. Fare clic su **Plug-in** > **Catalogo**.

Configurazione della raccolta di dati

Per informazioni sulla configurazione di Sentinel per la raccolta dati, vedere “Collecting and Routing Event Data” (Raccolta e instradamento dei dati degli eventi) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Configurazione dei pacchetti soluzione

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. La maggior parte di questi contenuti proviene dal pacchetto soluzione principale di Sentinel e dal pacchetto soluzione per la serie ISO 27000 preinstallati. Per ulteriori informazioni, consultare “Using Solution Packs (Utilizzo dei pacchetti soluzione)” nella *Sentinel User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

I pacchetti soluzione consentono di organizzare in categorie e raggruppare i contenuti in vari set di controlli o policy che vengono gestiti come una sola unità. I controlli inclusi nei pacchetti soluzione vengono preinstallati affinché i contenuti pronti all'uso siano immediatamente disponibili. Tuttavia, tali controlli devono essere formalmente implementati o provati mediante l'interfaccia principale 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 dei pacchetti soluzione 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 *Sentinel User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

Configurazione di azioni e integratori

Per informazioni sulla configurazione dei plug-in pronti all'uso, vedere la documentazione specifica del plug-in disponibile sul sito Web dei plug-in di Sentinel.

23 Abilitazione della modalità FIPS 140-2 in un'installazione esistente di Sentinel

In questo capitolo sono riportate le informazioni relative all'abilitazione della modalità FIPS 140-2 in un'installazione esistente di Sentinel.

Nota: le istruzioni seguenti presuppongono che Sentinel sia installato nella directory `/opt/novell/sentinel`. I comandi devono essere eseguiti come utente `novell`.

Abilitazione dell'esecuzione in modalità FIPS 140-2 nel server Sentinel

Per abilitare l'esecuzione in modalità FIPS 140-2 del server Sentinel:

1. Eseguire il login al server Sentinel.
2. Passare all'utente `novell` (`su novell`).
3. Passare alla directory bin di Sentinel.
4. Eseguire lo script `convert_to_fips.sh` e seguire le istruzioni visualizzate.
5. (Condizionale) Se nell'ambiente viene utilizzata l'autenticazione a più fattori o l'autenticazione forte, è necessario eseguire lo script `create_mfa_fips_keys.sh` e seguire le istruzioni visualizzate.

   Nota: Quando viene eseguito, lo script richiede la password per il database nns.

   ---
6. (Condizionale) Se nell'ambiente viene utilizzata l'autenticazione a più fattori o autenticazione forte, è necessario fornire l'ID del client Sentinel e il segreto del client Sentinel. Per ulteriori informazioni sui metodi di autenticazione, vedere "Authentication Methods" (Metodi di autenticazione) nella *Sentinel Administrator Guide* (Guida di amministrazione di Sentinel).

   Per recuperare l'ID e il segreto client di Sentinel, visitare l'URL seguente:

   `https://Nomehost:porta/SentinelAuthServices/oauth/clients`

   Dove:

   - *Nome host* è il nome host del server Sentinel.
   - *Porta* è la porta utilizzata da Sentinel (in genere 8443).

   L'URL specificato utilizza la sessione Sentinel corrente per recuperare l'ID e il segreto del client Sentinel.
7. Riavviare il server Sentinel.
8. Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel Capitolo 24, "Esecuzione di Sentinel in modalità FIPS 140-2", a pagina 133.

Abilitazione della modalità FIPS 140-2 in istanze remote di Collector Manager e di Correlation Engine

Se con il server Sentinel eseguito in modalità FIPS 140-2 si desidera utilizzare comunicazioni conformi agli standard FIPS, è necessario abilitare la modalità FIPS 140-2 nell'istanza remota di Collector Manager e di Correlation Engine.

Per abilitare l'esecuzione in modalità FIPS 140-2 di un'istanza remota di Collector Manager o di Correlation Engine:

1. Eseguire il login al sistema remoto di Collector Manager o di Correlation Engine.
2. Passare all'utente `novell` (`su novell`).
3. Passare alla directory bin. L'ubicazione di default è `/opt/novell/sentinel/bin`.
4. Eseguire lo script `convert_to_fips.sh` e seguire le istruzioni visualizzate.
5. Riavviare Collector Manager oppure Correlation Engine.
6. Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel Capitolo 24, “Esecuzione di Sentinel in modalità FIPS 140-2”, a pagina 133.

24 Esecuzione di Sentinel in modalità FIPS 140-2

In questo capitolo sono riportate le informazioni relative alla configurazione e all'utilizzo di Sentinel in modalità FIPS 140-2.

Configurazione del servizio Advisor in modalità FIPS 140-2

Per effettuare il download del proprio feed dal server Advisor, il servizio Advisor utilizza una connessione HTTPS sicura. Il certificato utilizzato dal server per le comunicazioni sicure deve essere aggiunto al database dell'archivio chiavi FIPS di Sentinel.

Per verificare che la registrazione nel database di gestione risorse sia avvenuta correttamente:

1. Effettuare il download del certificato dal server Advisor e salvare il file con il nome `advisor.cer`.
2. Importare il certificato del server Advisor nell'archivio chiavi FIPS di Sentinel.

   Per ulteriori informazioni sull'importazione del certificato, vedere “Importazione di certificati nel database di archivio chiavi FIPS” a pagina 143.

Configurazione della ricerca distribuita in modalità FIPS 140-2

In questa sezione sono riportate informazioni sulla configurazione della ricerca distribuita in modalità FIPS 140-2.

Scenario 1: i server di origine e destinazione di Sentinel sono in modalità FIPS 140-2

Per le ricerche distribuite su più server Sentinel eseguiti in modalità FIPS 140-2, è necessario aggiungere nell'archivio chiavi FIPS i certificati utilizzati per la comunicazione sicura.

1. Eseguire il login al computer di origine della ricerca distribuita.
2. Passare alla directory del certificato:

   ```
   cd <sentinel_install_directory>/config
   ```

3. Copiare il certificato dell'origine (`sentinel.cer`) in un'ubicazione temporanea nel computer di destinazione.
4. Importare il certificato dell'origine nell'archivio chiavi FIPS di destinazione di Sentinel.

   Per ulteriori informazioni sull'importazione del certificato, vedere “Importazione di certificati nel database di archivio chiavi FIPS” a pagina 143.
5. Eseguire il login al computer di destinazione della ricerca distribuita.
6. Passare alla directory del certificato:

   ```
   cd /etc/opt/novell/sentinel/config
   ```
7. Copiare il certificato della destinazione (`sentinel.cer`) in un'ubicazione temporanea nel computer di origine.
8. Importare il certificato del sistema di destinazione nell'archivio chiavi FIPS di origine di Sentinel.
9. Riavviare i servizi Sentinel nei computer di origine e di destinazione.

Scenario 2: il server Sentinel di origine è in modalità non FIPS e il server di destinazione è in modalità FIPS 140-2

È necessario convertire l'archivio chiavi del server Web del computer di origine al formato del certificato ed esportare il certificato nel computer di destinazione.

1. Eseguire il login al computer di origine della ricerca distribuita.
2. Creare l'archivio chiavi del server Web nel formato del certificato (`.cer`):

   ```
   <sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -
   keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
   password -file <certificate_name.cer>
   ```
3. Copiare il certificato di origine della ricerca distribuita (`Sentinel.cer`) in un'ubicazione temporanea nel computer di destinazione della ricerca distribuita.
4. Eseguire il login al computer di destinazione della ricerca distribuita.
5. Importare il certificato dell'origine nell'archivio chiavi FIPS di destinazione di Sentinel.

   Per ulteriori informazioni sull'importazione del certificato, vedere “Importazione di certificati nel database di archivio chiavi FIPS” a pagina 143.
6. Riavviare i servizi Sentinel nel computer di destinazione.

Scenario 3: il server Sentinel di origine è in modalità FIPS e il server di destinazione è in modalità non FIPS

1. Eseguire il login al computer di destinazione della ricerca distribuita.
2. Creare l'archivio chiavi del server Web nel formato del certificato (.cer):

   ```
   <sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -
   keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
   password -file <certificate_name.cer>
   ```
3. Copiare il certificato in un'ubicazione temporanea nel computer di origine della ricerca distribuita.
4. Importare il certificato della destinazione nell'archivio chiavi FIPS di origine di Sentinel.

   Per ulteriori informazioni sull'importazione del certificato, vedere “Importazione di certificati nel database di archivio chiavi FIPS” a pagina 143.
5. Riavviare i servizi Sentinel nel computer di origine.

Configurazione dell'autenticazione LDAP in modalità FIPS 140-2

Per configurare l'autenticazione LDAP per server Sentinel eseguiti in modalità FIPS 140-2:

1. Ottenere il certificato del server LDAP dall'amministratore LDAP oppure utilizzare un comando. Ad esempio,

   ```
   openssl s_client -connect <LDAP server IP>:636
   ```

   e copiare il testo restituito in un file senza includere le righe BEGIN ed END.
2. Importare il certificato del server LDAP nell'archivio chiavi FIPS di Sentinel.

   Per ulteriori informazioni sull'importazione del certificato, vedere “Importazione di certificati nel database di archivio chiavi FIPS” a pagina 143.
3. Andare all'interfaccia di **Sentinel Main** come utente con il ruolo amministrativo e continuare con la configurazione dell'autenticazione LDAP.

   Per ulteriori informazioni, vedere “LDAP Authentication Against a Single LDAP Server Or Domain” (Autenticazione LDAP a un solo server o dominio LDAP) nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel).

Nota: è inoltre possibile configurare l'autenticazione LDAP per un server Sentinel in modalità FIPS 140-2 eseguendo lo script `ldap_auth_config.sh` disponibile nella directory `/opt/novell/sentinel/setup`.

Aggiornamento dei certificati del server nelle istanze remote di Collector Manager e di Correlation Engine

Per configurare le istanze remote esistenti di Collector Manager e di Correlation Engine affinché comunichino con un server Sentinel eseguito in modalità FIPS 140-2, è possibile convertire il sistema remoto in modalità FIPS 140-2 oppure aggiornare il certificato del server Sentinel nel sistema remoto e lasciare l'istanza di Collector Manager o di Correlation Engine in modalità non FIPS. Le istanze remote di Collector Manager eseguite in modalità FIPS potrebbero non funzionare correttamente con le origini eventi che non supportano FIPS o che richiedono uno dei connettori Sentinel non ancora abilitati per FIPS.

Se non si prevede di abilitare la modalità FIPS 140-2 nelle istanze remote di Collector Manager o di Correlation Engine, è necessario copiare nel sistema remoto il certificato del server Sentinel più recente, affinché le istanze di Collector Manager o di Correlation Engine possano comunicare con il server Sentinel.

Per aggiornare il certificato del server Sentinel nell'istanza remota di Collector Manager o di Correlation Engine:

1. Eseguire il login al computer remoto in cui è installata l'istanza remota di Collector Manager o di Correlation Engine.
2. Passare all'utente `novell` (`su novell`).
3. Passare alla directory bin. L'ubicazione di default è `/opt/novell/sentinel/bin`.
4. Eseguire lo script `updateServerCert.sh` e seguire le istruzioni visualizzate.

Configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2

In questa sezione vengono fornite informazioni sulla configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2.

Nota: queste istruzioni si basano sul presupposto che Sentinel sia stato installato nella directory `/opt/novell/sentinel`. Eseguire tutti i comandi come utente `novell`.

Connettore di Agent Manager

Eseguire la procedura seguente soltanto se durante la configurazione delle impostazioni di rete del server di origine eventi di Agent Manager è stata selezionata l'opzione **Cifrato (HTTPS)**.

Per configurare il connettore di Agent Manager affinché venga eseguito in modalità FIPS 140-2:

1. Aggiungere o modificare il server di origine eventi di Agent Manager. Eseguire le operazioni indicate nelle schermate di configurazione fino a quando non appare la finestra Sicurezza. Per ulteriori informazioni, vedere *Agent Manager Connector Guide* (Guida del connettore di Agent Manager).
2. Selezionare una delle opzioni nel campo *Tipo di autenticazione client*. Il tipo di autenticazione del client determina il livello di rigorosità adottato dal server di origine eventi SSL di Agent Manager per la verifica dell'identità delle origini eventi di Agent Manager che tentano di inviare dati.
   - **Aperta:** consente le connessioni SSL provenienti da agenti di Agent Manager. Non viene eseguita alcuna convalida o autenticazione del certificato del client.
   - **Chiusa:** esegue la convalida del certificato affinché sia un certificato X.509 valido e verifica inoltre che il certificato del client sia considerato attendibile dal server di origine eventi. Affinché origini illecite non possano inviare dati non autorizzati, sarà necessario aggiungere esplicitamente al server Sentinel nuove origini.

     Per l'opzione **Rigida** è necessario importare nell'archivio chiavi FIPS di Sentinel il certificato di ciascun nuovo client di Agent Manager. Quando Sentinel viene eseguito in modalità FIPS 140-2, non è possibile importare il certificato del client utilizzando l'interfaccia Gestione origini eventi (ESM).

     Per ulteriori informazioni sull'importazione del certificato, vedere “Importazione di certificati nel database di archivio chiavi FIPS” a pagina 143.

Nota: in modalità FIPS 140-2, il server di origine eventi di Agent Manager utilizza la coppia di chiavi del server Sentinel e non è quindi necessario importare la coppia di chiavi del server.

3 Se l'autenticazione del server è abilitata negli agenti, è necessario configurarli affinché considerino attendibile il certificato del server Sentinel o dell'istanza remota di Collector Manager, a seconda dell'ubicazione di installazione del connettore.

Ubicazione del certificato del server Sentinel: `/etc/opt/novell/sentinel/config/sentinel.cer`

Ubicazione del certificato dell'istanza remota di Collector Manager: `/etc/opt/novell/sentinel/config/rcm.cer`

Nota: quando si utilizzano certificati personalizzati con firma digitale apposta da un'autorità di certificazione (CA), è necessario che l'agente di Agent Manager consideri attendibile il file del relativo certificato.

Connettore del database (JDBC)

Eseguire la procedura seguente soltanto se durante la configurazione della connessione al database è stata selezionata l'opzione *SSL*.

Per configurare il connettore del database affinché venga eseguito in modalità FIPS 140-2:

1 Prima di configurare il connettore, effettuare il download del certificato dal server del database e salvarlo come file denominato `database.cert` nella directory `/etc/opt/novell/sentinel/config` del server Sentinel.

Per ulteriori informazioni, consultare la documentazione del rispettivo database.

2 Importare il certificato nell'archivio chiavi FIPS di Sentinel.

Per ulteriori informazioni sull'importazione del certificato, vedere “Importazione di certificati nel database di archivio chiavi FIPS” a pagina 143.

3 Continuare la configurazione del connettore.

Connettore di collegamento Sentinel

Eseguire la procedura seguente soltanto se durante la configurazione delle impostazioni di rete del server di origine eventi di Collegamento Sentinel è stata selezionata l'opzione **Cifrato (HTTPS)**.

Per configurare il connettore di Collegamento Sentinel affinché venga eseguito in modalità FIPS 140-2:

1 Aggiungere o modificare il server di origine eventi di Collegamento Sentinel. Eseguire le operazioni indicate nelle schermate di configurazione fino a quando non appare la finestra Sicurezza. Per ulteriori informazioni, vedere la *Sentinel Link Connector Guide* (Guida del connettore di Collegamento Sentinel).

2 Selezionare una delle opzioni nel campo *Tipo di autenticazione client*. Il tipo di autenticazione del client determina il livello di rigorosità adottato dal server di origine eventi SSL di Collegamento Sentinel per la verifica dell'identità delle origini eventi di Collegamento Sentinel (integratori di Collegamento Sentinel) che tentano di inviare dati.

- **Aperta:** consente le connessioni SSL provenienti dai client (integratori di Collegamento Sentinel). Non viene eseguita alcuna convalida o autenticazione del certificato dell'integratore.

- **Chiusa:** esegue la convalida del certificato dell'integratore affinché sia un certificato X.509 valido e verifica inoltre che il certificato dell'integratore sia considerato attendibile dal server di origine eventi. Per ulteriori informazioni, consultare la documentazione del rispettivo database.

  Per l'opzione **Rigida**:

  - Se l'integratore di Collegamento Sentinel è in modalità FIPS 140-2, è necessario copiare il file `/etc/opt/novell/sentinel/config/sentinel.cer` dal computer Sentinel mittente al computer Sentinel destinatario. Importare il certificato nell'archivio chiavi FIPS del computer Sentinel destinatario.

    Nota: quando si utilizzano certificati personalizzati con firma digitale apposta da un'autorità di certificazione (CA), è necessario importare il file corretto del certificato personalizzato.

  - Se l'integratore di Collegamento Sentinel è in modalità non FIPS, è necessario importare il certificato personalizzato dell'integratore nell'archivio chiavi FIPS del computer Sentinel destinatario.

    Nota: se il mittente è Sentinel Log Manager (in modalità non FIPS) e il destinatario è Sentinel in modalità FIPS 140-2, il certificato del server da importare nel mittente dal computer Sentinel destinatario è il file `/etc/opt/novell/sentinel/config/sentinel.cer`.

  Quando Sentinel viene eseguito in modalità FIPS 140-2, non è possibile importare il certificato del client utilizzando l'interfaccia Gestione origini eventi (ESM). Per ulteriori informazioni sull'importazione del certificato, vedere "Importazione di certificati nel database di archivio chiavi FIPS" a pagina 143.

Nota: in modalità FIPS 140-2, il server di origine eventi di Collegamento Sentinel utilizza la coppia di chiavi del server Sentinel. Non è quindi necessario importare la coppia di chiavi del server.

Connettore Syslog

Eseguire la procedura seguente soltanto se durante la configurazione delle impostazioni di rete del server di origine eventi Syslog è stato selezionato il protocollo **SSL**.

Per configurare il connettore Syslog affinché venga eseguito in modalità FIPS 140-2:

1. Aggiungere o modificare il server di origine eventi Syslog. Eseguire le operazioni indicate nelle schermate di configurazione fino a quando non appare la finestra Rete. Per ulteriori informazioni, vedere la *Syslog Connector Guide* (Guida del connettore Syslog).
2. Fare clic su **Impostazioni**.
3. Selezionare una delle opzioni nel campo *Tipo di autenticazione client*. Il tipo di autenticazione del client determina il livello di rigorosità adottato dal server SSL di origine eventi Syslog per la verifica dell'identità delle origini eventi di Syslog che tentano di inviare dati.
   - **Aperta:** consente le connessioni SSL provenienti dai client (origini eventi). Non viene eseguita alcuna convalida o autenticazione del certificato del client.
   - **Chiusa:** esegue la convalida del certificato affinché sia un certificato X.509 valido e verifica inoltre che il certificato del client sia considerato attendibile dal server di origine eventi. Affinché origini illecite non possano inviare dati a Sentinel, sarà necessario aggiungere esplicitamente a Sentinel le nuove origini.

Per l'opzione **Rigida** è necessario importare nell'archivio chiavi FIPS di Sentinel il certificato del client Syslog.

Quando Sentinel viene eseguito in modalità FIPS 140-2, non è possibile importare il certificato del client utilizzando l'interfaccia Gestione origini eventi (ESM).

Per ulteriori informazioni sull'importazione del certificato, vedere "Importazione di certificati nel database di archivio chiavi FIPS" a pagina 143.

Nota: in modalità FIPS 140-2, il server di origine eventi Syslog utilizza la coppia di chiavi del server Sentinel. Non è quindi necessario importare la coppia di chiavi del server.

4 Se l'autenticazione del server è abilitata nel client Syslog, è necessario configurarlo affinché consideri attendibile il certificato del server Sentinel o dell'istanza remota di Collector Manager, a seconda dell'ubicazione di installazione del connettore.

Il file del certificato del server Sentinel si trova in `/etc/opt/novell/sentinel/config/sentinel.cer`.

Il file del certificato dell'istanza remota di Collector Manager si trova in `/etc/opt/novell/sentinel/config/rcm.cer`.

Nota: quando si utilizzano certificati personalizzati con firma digitale apposta da un'autorità di certificazione (CA), è necessario che il client consideri attendibile il file del relativo certificato.

Connettore degli eventi di Windows (WMI)

Per configurare il connettore degli eventi di Windows (WMI) affinché venga eseguito in modalità FIPS 140-2:

1 Aggiungere o modificare il connettore degli eventi di Windows. Eseguire le operazioni indicate nelle schermate di configurazione fino a quando non appare la finestra Sicurezza. Per ulteriori informazioni, vedere la *Windows Event (WMI) Connector Guide* (Guida del connettore degli eventi di Windows).

2 Fare clic su **Impostazioni**.

3 Selezionare una delle opzioni nel campo *Tipo di autenticazione client*. Il tipo di autenticazione del client determina il livello di rigorosità adottato dal connettore degli eventi di Windows per la verifica dell'identità dei servizi di raccolta eventi di Windows (WECS) del client che tentano di inviare dati.

- **Aperta:** consente le connessioni SSL provenienti dai WECS del client. Non viene eseguita alcuna convalida o autenticazione del certificato del client.
- **Chiusa:** esegue la convalida del certificato affinché sia un certificato X.509 valido e verifica inoltre che il certificato del WECS del client sia firmato da un'autorità di certificazione. Affinché origini illecite non possano inviare dati a Sentinel, sarà necessario aggiungere esplicitamente a Sentinel le nuove origini.

  Per l'opzione **Rigida** è necessario importare nell'archivio chiavi FIPS di Sentinel il certificato del WECS del client. Quando Sentinel viene eseguito in modalità FIPS 140-2, non è possibile importare il certificato del client utilizzando l'interfaccia Gestione origini eventi (ESM).

  Per ulteriori informazioni sull'importazione del certificato, vedere "Importazione di certificati nel database di archivio chiavi FIPS" a pagina 143.

Nota: in modalità FIPS 140-2, il server di origine eventi di Windows utilizza la coppia di chiavi del server Sentinel. Non è quindi necessario importare la coppia di chiavi del server.

4 Se l'autenticazione del server è abilitata nel client Windows, è necessario configurarlo affinché consideri attendibile il certificato del server Sentinel o dell'istanza remota di Collector Manager, a seconda dell'ubicazione di installazione del connettore.

Il file del certificato del server Sentinel si trova in `/etc/opt/novell/sentinel/config/sentinel.cer`.

Il file del certificato dell'istanza remota di Collector Manager si trova in `/etc/opt/novell/sentinel/config/rcm.cer`.

Nota: quando si utilizzano certificati personalizzati con firma digitale apposta da un'autorità di certificazione (CA), è necessario che il client consideri attendibile il file del relativo certificato.

---

5 Se si desidera sincronizzare automaticamente le origini eventi o popolare l'elenco delle origini eventi utilizzando una connessione ad Active Directory, è necessario importare il certificato del server di Active Directory nell'archivio chiavi FIPS di Sentinel.

Per ulteriori informazioni sull'importazione del certificato, vedere “Importazione di certificati nel database di archivio chiavi FIPS” a pagina 143.

Integratore di Collegamento Sentinel

Eseguire la procedura seguente soltanto se durante la configurazione delle impostazioni di rete dell'integratore di Collegamento Sentinel è stata selezionata l'opzione **Cifrato (HTTPS)**.

Per configurare l'integratore di Collegamento Sentinel affinché venga eseguito in modalità FIPS 140-2:

1 Quando l'integratore di Collegamento Sentinel è in modalità FIPS 140-2, l'autenticazione del server è obbligatoria. Prima di configurare l'istanza dell'integratore, importare il certificato del server di Collegamento Sentinel nell'archivio chiavi FIPS di Sentinel:

- **Se il connettore di Collegamento Sentinel è in modalità FIPS 140-2**:

  Se il connettore di Collegamento Sentinel è installato nel server Sentinel, è necessario copiare il file `/etc/opt/novell/sentinel/config/sentinel.cer` dal computer Sentinel destinatario al computer Sentinel mittente.

  Se il connettore è installato in un'istanza remota di Collector Manager, è necessario copiare il file `/etc/opt/novell/sentinel/config/rcm.cer` dal computer destinatario dell'istanza remota di Collector Manager al computer Sentinel destinatario.

  Importare il certificato nell'archivio chiavi FIPS del computer Sentinel mittente.

  Nota: quando si utilizzano certificati personalizzati con firma digitale apposta da un'autorità di certificazione (CA), è necessario importare il file corretto del certificato personalizzato.

- Se il connettore di Collegamento Sentinel non è in modalità FIPS:

  Importare il certificato personalizzato del server di Collegamento Sentinel nell'archivio chiavi FIPS del computer Sentinel mittente.

  Nota: quando l'integratore di Collegamento Sentinel è in modalità FIPS 140-2 e il connettore di Collegamento Sentinel non è in modalità FIPS, utilizzare la coppia di chiavi personalizzata del server nel connettore. Non utilizzare la coppia di chiavi interna del server.

Per ulteriori informazioni sull'importazione del certificato, vedere “Importazione di certificati nel database di archivio chiavi FIPS” a pagina 143.

2 Continuare la configurazione dell'istanza dell'integratore.

Nota: in modalità FIPS 140-2, l'integratore di Collegamento Sentinel utilizza la coppia di chiavi del server Sentinel. Non è necessario importare la coppia di chiavi dell'integratore.

Integratore LDAP

Per configurare l'integratore LDAP affinché venga eseguito in modalità FIPS 140-2:

1. Prima di configurare l'istanza dell'integratore, effettuare il download del certificato dal server LDAP e salvarlo come file denominato `ldap.cert` nella directory `/etc/opt/novell/sentinel/config` del server Sentinel.

   Utilizzare ad esempio

   ```
   openssl s_client -connect <LDAP server IP>:636
   ```

   e copiare il testo restituito in un file senza includere le righe BEGIN ed END.
2. Importare il certificato nell'archivio chiavi FIPS di Sentinel.

   Per ulteriori informazioni sull'importazione del certificato, vedere "Importazione di certificati nel database di archivio chiavi FIPS" a pagina 143.
3. Continuare la configurazione dell'istanza dell'integratore.

Integratore SMTP

L'integratore SMTP supporta la modalità FIPS 140-2 a partire dalla versione 2011.1r2. Non è necessario apportare alcuna modifica alla configurazione.

Integratore syslog

Eseguire la procedura seguente soltanto se durante la configurazione delle impostazioni di rete dell'integratore Syslog è stata selezionata l'opzione Cifrato (SSL).

Per configurare l'integratore Syslog affinché venga eseguito in modalità FIPS 140-2:

1. Quando l'integratore Syslog è in modalità FIPS 140-2, l'autenticazione del server è obbligatoria. Prima di configurare l'istanza dell'integratore, importare il certificato del server Syslog nell'archivio chiavi FIPS di Sentinel:
   - **Quando il connettore Syslog è in modalità FIPS 140-2:** se il connettore è installato nel server Sentinel, è necessario copiare il file `/etc/opt/novell/sentinel/config/sentinel.cer` dal server Sentinel destinatario al server Sentinel mittente.

     Quando il connettore è installato in un'istanza remota di Collector Manager, è necessario copiare il file `/etc/opt/novell/sentinel/config/rcm.cer` dal computer destinatario dell'istanza remota di Collector Manager al computer Sentinel destinatario.

     Importare il certificato nell'archivio chiavi FIPS del computer Sentinel mittente.

     Nota: quando si utilizzano certificati personalizzati con firma digitale apposta da un'autorità di certificazione (CA), è necessario importare il file corretto del certificato personalizzato.
   - **Quando il connettore Syslog non è in modalità FIPS:** importare il certificato personalizzato del server Syslog nell'archivio chiavi FIPS mittente di Sentinel.

Nota: quando l'integratore Syslog è in modalità FIPS 140-2 e il connettore Syslog non è in modalità FIPS, utilizzare la coppia di chiavi personalizzata del server nel connettore. Non utilizzare la coppia di chiavi interna del server.

Per importare i certificati nel database dell'archivio chiavi FIPS:

1. Copiare il file del certificato in un'ubicazione temporanea a scelta nel server Sentinel o nell'istanza remota di Collector Manager.
2. Passare alla directory `/opt/novell/sentinel/bin`.
3. Per importare il certificato nel database dell'archivio chiavi FIPS, eseguire il comando seguente e seguire le istruzioni visualizzate.

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

4. Quando viene richiesto di riavviare il server Sentinel o l'istanza remota di Collector Manager, immettere `sì` o `s`.

2 Continuare la configurazione dell'istanza dell'integratore.

Nota: in modalità FIPS 140-2, l'integratore Syslog utilizza la coppia di chiavi del server Sentinel. Non è necessario importare la coppia di chiavi dell'integratore.

Utilizzo di connettori non FIPS con Sentinel in modalità FIPS 140-2

In questa sezione si descrive come utilizzare i connettori non abilitati per FIPS con un server Sentinel in modalità FIPS 140-2. Se si utilizzano origini che non supportano FIPS o se si desidera raccogliere gli eventi da connettori non FIPS presenti nell'ambiente, si consiglia di utilizzare questo approccio.

Per utilizzare connettori non FIPS con Sentinel in modalità FIPS 140-2:

1 Installare un'istanza remota di Collector Manager in modalità non FIPS per eseguire la connessione al server Sentinel in modalità FIPS 140-2.

Per ulteriori informazioni, vedere il Parte III, “Installazione di Sentinel,” a pagina 71.

2 Installare i connettori non FIPS nell'istanza remota di Collector Manager specifica.

Nota: sono stati riscontrati alcuni problemi noti in caso di installazione di connettori non FIPS, come ad esempio il connettore di revisione e il connettore file, in un'istanza remota di Collector Manager connessa a un server Sentinel in modalità FIPS 140-2. Per ulteriori informazioni sui problemi noti, vedere le note di rilascio di Sentinel .

Importazione di certificati nel database di archivio chiavi FIPS

Per stabilire una comunicazione sicura (SSL) dai componenti proprietari di certificati a Sentinel, è necessario inserire i relativi certificati nel database dell'archivio chiavi FIPS di Sentinel. Non è possibile effettuare l'upload dei certificati mediante l'interfaccia utente di Sentinel quando è stata abilitata la modalità FIPS 140-2, importare manualmente i certificati nel database dell'archivio chiavi FIPS.

Per le origini eventi che utilizzano connettori installati in un'istanza remota di Collector Manager, è necessario importare i certificati nel database dell'archivio chiavi FIPS dell'istanza remota di Collector Manager invece che nel server Sentinel centrale.

Per importare i certificati nel database dell'archivio chiavi FIPS:

1. Copiare il file del certificato in un'ubicazione temporanea a scelta nel server Sentinel o nell'istanza remota di Collector Manager.
2. Passare alla directory bin di Sentinel. L'ubicazione di default è `/opt/novell/sentinel/bin`.
3. Per importare il certificato nel database dell'archivio chiavi FIPS, eseguire il comando seguente e seguire le istruzioni visualizzate.

   `./convert_to_fips.sh -i <certificate file path>`
4. Quando viene richiesto di riavviare il server Sentinel o l'istanza remota di Collector Manager, immettere `sì` o `s`.

Ripristino di Sentinel nella modalità non FIPS

In questa sezione sono riportate le informazioni necessarie per ripristinare Sentinel e i relativi componenti nella modalità non FIPS.

- "Ripristino del server Sentinel nella modalità non FIPS" a pagina 143
- "Ripristino della modalità non FIPS in istanze remote di Collector Manager o di Correlation Engine" a pagina 144

Ripristino del server Sentinel nella modalità non FIPS

Per ripristinare in modalità non FIPS un server Sentinel eseguito in modalità FIPS 140-2 è necessario disporre di una copia di backup del server Sentinel effettuata prima del passaggio alla modalità FIPS 140-2.

Nota: quando si ripristina un server Sentinel in modalità non FIPS, gli eventi, i dati dei casi e le modifiche di configurazione successivi al passaggio alla modalità FIPS 140-2 vengono cancellati. Il sistema Sentinel viene ripristinato utilizzando l'ultimo punto di ripristino della modalità non FIPS. È necessario effettuare un backup del sistema prima del ripristino alla modalità non FIPS, da utilizzare per eventuali esigenze future.

Per ripristinare la modalità non FIPS nel server Sentinel:

1. Eseguire il login al server Sentinel come utente `root`.
2. Passare all'utente `novell`.
3. Passare alla directory bin di Sentinel. L'ubicazione di default è `/opt/novell/sentinel/bin`.

4 Per ripristinare la modalità non FIPS nel server Sentinel, eseguire il comando seguente e seguire le istruzioni visualizzate:

   `./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'`

   Ad esempio, se `non-fips20130124191111359034887.tar.gz` è il file di backup, eseguire il comando seguente:

   `./backup_util.sh -f non-fips20130124191111359034887.tar.gz -m 'restore'`

5 Riavviare il server Sentinel.

Ripristino della modalità non FIPS in istanze remote di Collector Manager o di Correlation Engine

È possibile ripristinare la modalità non FIPS in istanze remote di Collector Manager o di Correlation Engine.

Per ripristinare la modalità non FIPS in istanze remote di Collector Manager o di Correlation Engine:

1 Eseguire il login al sistema remoto di Collector Manager o di Correlation Engine.

2 Passare all'utente `novell` (`su novell`).

3 Passare alla directory bin. L'ubicazione di default è `/opt/novell/sentinel/bin`.

4 Eseguire lo script `revert_to_nonfips.sh` e seguire le istruzioni visualizzate.

5 Riavviare l'istanza remota di Collector Manager o di Correlation Engine.

25 Aggiunta di un'intestazione di consenso

In Sentinel è possibile visualizzare un'intestazione di consenso prima del login. L'utente può specificare il contenuto dell'intestazione secondo necessità. Dopo aver aggiunto l'intestazione di consenso, è necessario accettare i termini dell'intestazione stessa ogni volta che si esegue il login a Sentinel.

Per aggiungere un'intestazione di consenso:

1. Eseguire il login al server Sentinel come utente `novell`.
2. Accedere a `<percorso_di_installazione_di_Sentinel>/var/opt/novell/sentinel/3rdparty/jetty/webapps/ROOT/siemdownloads`.
3. Aggiungere un file di testo denominato `USER_AGREEMENT.txt`.
4. Immettere il testo del contratto con l'utente.
5. Salvare il file.
6. Avviare Sentinel per visualizzare l'intestazione di consenso.

L'intestazione di consenso viene ora visualizzata nella schermata di login di Sentinel.

Nota: è necessario eseguire manualmente il backup del file `USER_AGREEMENT.txt` prima di eseguire l'upgrade di Sentinel.

V Esecuzione dell'upgrade di Sentinel

In questa sezione sono riportate le informazioni necessarie per eseguire l'upgrade di Sentinel e di altri componenti.

26 Elenco di controllo per l'implementazione

Prima di eseguire l'upgrade di Sentinel, esaminare il seguente elenco di controllo:

Tabella 26-1 *Elenco di controllo per l'implementazione*

❒	Task	Vedere
❒	Accertarsi che i computer in cui si installano Sentinel e i relativi componenti siano conformi ai requisiti specificati.	Sito Web delle informazioni tecniche di Sentinel
❒	Per informazioni sui problemi noti, esaminare le note di rilascio relative al sistema operativo supportato.	Note di rilascio di SUSE
❒	Esaminare le note di rilascio di Sentinel per informazioni sulle nuove funzionalità e i problemi noti.	Note di rilascio di Sentinel
❒	Completare i task menzionati nei prerequisiti.	Capitolo 27, “Prerequisiti”, a pagina 151

27 Prerequisiti

Salvataggio delle informazioni sulla configurazione personalizzata

Salvataggio delle impostazioni del file server.conf

Se sono stati configurati dei valori dei parametri della configurazione personalizzata nel file `server.conf`, salvare tali valori in un file separato prima di eseguire l'upgrade.

Per salvare le informazioni sulla configurazione personalizzata:

1. Eseguire il login al server Sentinel come utente `novell` e passare alla directory `/etc/opt/novell/sentinel/config/`.
2. Creare un file di configurazione denominato `server-custom.conf` e aggiungere in tale file i parametri personalizzati di configurazione.

Durante l'upgrade, in questi file viene applicata la configurazione personalizzata che è stata salvata.

Salvataggio delle impostazioni del file jetty-ssl

Sentinel 8.1 include una versione aggiornata di Jetty. La versione aggiornata di Jetty include modifiche alla relativa struttura di file.

Se il file `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml` è stato modificato nelle precedenti versioni di Sentinel, ad esempio escludendo delle cifrature, salvare tali modifiche in un file distinto prima dell'upgrade di Sentinel.

Una volta completato l'upgrade di Sentinel, copiare tali modifiche nel file `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl-context.xml` e riavviare Sentinel.

Estensione del periodo di permanenza per i dati delle associazioni dell'evento

A partire da Sentinel 7.4.4, il periodo di permanenza di default per i dati delle associazioni dell'evento è di 14 giorni. Se si esegue l'upgrade da una versione di Sentinel precedente alla 7.4.4, il periodo di permanenza fissato per i dati delle associazioni dell'evento sarà riportato a 14 giorni dopo l'upgrade. Per evitarlo, è possibile impostare il periodo di permanenza su un valore desiderato aggiungendo una proprietà nel file `configuration.properties`. Per ulteriori informazioni, vedere “Configuring the

Retention Period for the Event Associations Data" (Configurazione del periodo di permanenza per i dati delle associazioni dell'evento) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Configurazione pre-upgrade per SSDM

Il processo di upgrade consentirà l'aggiornamento dei file correlati alle applicazioni Spark. Per utilizzare i file aggiornati, è necessario riavviare il lavoro Spark e reimpostare tutti i punti di controllo Spark sugli argomenti Kafka. Per evitare la perdita di dati dovuta alla reimpostazione del punto di controllo dell'argomento Kafka, è necessario sospendere l'inoltro dei dati dalle istanze di Collector Manager a Kafka prima di eseguire l'upgrade di SSDM. Durante la sospensione dell'inoltro dei dati, questi ultimi saranno memorizzati in Collector Manager finché l'inoltro non viene ripreso. Nel momento in cui l'applicazione Spark ha terminato l'elaborazione dei dati che erano stati inoltrati a Kafka prima della sospensione dell'inoltro, è possibile reimpostare il punto di controllo in sicurezza, senza perdita dei dati.

Per sospendere l'inoltro di eventi da Collector Manager a Kafka:

1. In Sentinel Main, fare clic su **Memorizzazione** > **Memorizzazione scalabile** > **Configurazione avanzata** > **Kafka**.
2. Aggiungere la seguente proprietà e impostarla su true:

   ```
   pause.events.tokafka
   ```
3. Fare clic su **Salva**.

Integrazione di Change Guardian

Sentinel è compatibile con Change Guardian 4.2 e versioni successive. Per ricevere gli eventi da Change Guardian, è necessario eseguire prima l'upgrade del server Change Guardian, degli agenti e dell'editor delle policy alla versione 4.2 o successive affinché Sentinel continui a ricevere gli eventi da Change Guardian dopo l'upgrade.

28 Upgrade dell'installazione tradizionale di Sentinel

Esecuzione dell'upgrade di Sentinel

Per eseguire l'upgrade del server Sentinel, utilizzare la procedura seguente:

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

   Per ulteriori informazioni, vedere “Backing Up and Restoring Data” (Backup e ripristino dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.1) .
2. (Condizionale) Se nei file `server.xml`, `collector_mgr.xml` o `correlation_engine.xml` le impostazioni di configurazione sono state personalizzate, accertarsi di aver creato i rispettivi file delle proprietà denominati con l'ID del componente dell'oggetto affinché le personalizzazioni non vadano perse con l'upgrade. Per ulteriori informazioni, vedere “Maintaining Custom Settings in XML Files” (Conservazione delle impostazioni personalizzate nei file XML) nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel NetIQ).
3. Effettuare il download della versione più recente del programma di installazione dal sito Web dei download.
4. Effettuare il login come utente `root` al server in cui si desidera eseguire l'upgrade di Sentinel.
5. Specificare il seguente comando per estrarre i file di installazione dal file .tar:

   ```
   tar xfz <install_filename>
   ```

   Sostituire *<nomefile_installazione>* con il nome attuale del file di installazione.
6. Passare alla directory in cui è stato estratto il file d'installazione.
7. Per eseguire l'upgrade di Sentinel, specificare il comando seguente:

   ```
   ./install-sentinel
   ```
8. 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.
9. Leggere il contratto di licenza con l'utente finale, immettere `sì` o `s` per accettarlo, quindi continuare con il processo di installazione.
10. 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. Per continuare con l'upgrade, premere s.

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

11 Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.

12 Svuotare la cache di Java Web Start nei computer client, affinché venga utilizzata la versione più recente delle applicazioni Sentinel.

   Per svuotare la cache di Java Web Start è possibile utilizzare il comando `avaws -clearcache` o Java Control Center. Per ulteriori informazioni, vedere http://www.java.com/en/download/help/plugin_cache.xml.

13 (Condizionale) Nel caso in cui sia stato eseguito un upgrade sostanziale del database PostgreSQL (ad esempio da 8.0 a 9.0 o da 9.0 a 9.1) eliminare i file della versione precedente dal database PostgreSQL. Per informazioni sull'esecuzione dell'upgrade del database PostgreSQL, vedere le note di rilascio di Sentinel.

   13a Passare all'utente novell.

   ```
   su novell
   ```

   13b Passare alla cartella `bin`:

   ```
   cd /opt/novell/sentinel/3rdparty/postgresql/bin
   ```

   13c Cancellare i vecchi file PostgreSQL utilizzando il comando seguente:

   ```
   ./delete_old_cluster.sh
   ```

14 Per eseguire l'upgrade dei sistemi di Collector Manager e di Correlation Engine, vedere la “Upgrade di Collector Manager o di Correlation Engine” a pagina 156.

15 (Condizionale) Se si utilizza l'autenticazione Kerberos, abilitare AES256 in Java Runtime Environment poiché la cartella `java` viene sostituita con i file di default durante l'upgrade. Per abilitare AES256 in Java Runtime Environment, eseguire i passaggi seguenti:

   15a Effettuare il download di Java Cryptography Extension (JCE) 8 dall'ubicazione seguente: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`.

   15b Estrarre i due file `*.jar` e copiarli nella directory `/opt/novell/sentinel/jdk/jre/lib/security`.

   15c (Condizionale) Se si esegue Sentinel in un ambiente ad alta disponibilità, ripetere questi passaggi in tutti i nodi del cluster.

   15d Riavviare Sentinel.

Upgrade di Sentinel come utente non root

Se per motivi di policy dell'organizzazione non è possibile eseguire l'upgrade completo di Sentinel come utente `root`, l'upgrade può essere eseguito come utente di diverso tipo. In questo caso, alcuni passaggi vengono eseguiti come utente `root` per poi procedere con un altro tipo di utente creato dall'utente `root`.

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

   Per ulteriori informazioni sul backup dei dati, vedere “Backing Up and Restoring Data” (Backup e ripristino dei dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

2 (Condizionale) Se nei file `server.xml`, `collector_mgr.xml` o `correlation_engine.xml` le impostazioni di configurazione sono state personalizzate, accertarsi di aver creato i rispettivi file delle proprietà denominati con l'ID del componente dell'oggetto affinché le personalizzazioni non

vadano perse con l'upgrade. Per ulteriori informazioni, consultare “Backing Up and Restoring Data” (Backup e ripristino dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).

3. Effettuare il download dei file di installazione dal sito Web dei download di .
4. 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.
5. Effettuare il login come utente `root` al server in cui si desidera eseguire l'upgrade di Sentinel.
6. Estrarre l'RPM `squashfs` dai file di installazione di Sentinel.
7. Installare `squashfs` nel server Sentinel.

   ```
   rpm -Uvh <install_filename>
   ```
8. Specificare il comando seguente per modificare l'utente `novell` non root appena creato: `novell`:

   ```
   su novell
   ```
9. (Condizionale) Per eseguire un upgrade interattivo:

   9a Immettere il comando seguente:

   ```
   ./install-sentinel
   ```

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

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

   9b Continuare con la Passo 11.
10. (Condizionale) Per eseguire un upgrade automatico, specificare il comando seguente:

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

    L'installazione continua con i valori memorizzati nel file di risposta. L'upgrade di Sentinel è terminato.
11. Immettere il numero corrispondente alla lingua che si desidera utilizzare per l'upgrade.

    Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.
12. Leggere la licenza con l'utente finale e immettere `sì` o `s` per accettarla e continuare l'upgrade.

    L'upgrade inizia a installare tutti i pacchetti RPM. Il completamento dell'installazione potrebbe richiedere alcuni secondi.
13. Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.
14. Svuotare la cache di Java Web Start nei computer client, affinché venga utilizzata la versione più recente delle applicazioni Sentinel.

    Per svuotare la cache di Java Web Start è possibile utilizzare il comando `avaws -clearcache` o Java Control Center. Per ulteriori informazioni, vedere http://www.java.com/en/download/help/plugin_cache.xml.
15. (Condizionale) Nel caso in cui sia stato eseguito un upgrade sostanziale del database PostgreSQL (ad esempio da 8.0 a 9.0 o da 9.0 a 9.1) eliminare i file della versione precedente dal database PostgreSQL. Per informazioni sull'esecuzione dell'upgrade del database PostgreSQL, vedere le note di rilascio di Sentinel.

    15a Passare all'utente Novell.

```
su novell
```

15b Passare alla cartella `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

15c Cancellare i vecchi file PostgreSQL utilizzando il comando seguente:

```
./delete_old_cluster.sh
```

16 (Condizionale) Se si utilizza l'autenticazione Kerberos, abilitare AES256 in Java Runtime Environment poiché la cartella `java` viene sostituita con i file di default durante l'upgrade. Per abilitare AES256 in Java Runtime Environment, eseguire i passaggi seguenti:

16a Effettuare il download di Java Cryptography Extension (JCE) 8 dall'ubicazione seguente: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`.

16b Estrarre i due file `*.jar` e copiarli nella directory `/opt/novell/sentinel/jdk/jre/lib/security`.

16c (Condizionale) Se si esegue Sentinel in un ambiente ad alta disponibilità, ripetere questi passaggi in tutti i nodi del cluster.

16d Riavviare Sentinel.

Upgrade di Collector Manager o di Correlation Engine

Per eseguire l'upgrade di Collector Manager o di Correlation Engine, effettuare le operazioni seguenti:

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

   Per ulteriori informazioni, consultare “Backing Up and Restoring Data” (Backup e ripristino dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).
2. Andare all'interfaccia di **Sentinel Main** come utente con ruolo di amministratore.
3. Selezionare **Download**.
4. Fare clic su **Download del programma di installazione** nella sezione Programma di installazione di Collector Manager.
5. Salvare il file di installazione sul rispettivo server in cui risiede Collector Manager o Correlation Engine.
6. Copiare il file in un'ubicazione temporanea.
7. Estrarre i contenuti del file.
8. Eseguire lo script seguente:

   Per Collector Manager:

   ```
   ./install-cm
   ```

   Per Correlation Engine:

   ```
   ./install-ce
   ```
9. Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo.
10. (Condizionale) Nelle installazioni personalizzate, eseguire il comando seguente per sincronizzare le configurazioni tra il server Sentinel, Collector Manager e Correlation Engine:

    ```
    /opt/novell/sentinel/setup/configure.sh
    ```

Upgrade del sistema operativo

Questa versione di Sentinel include un set di comandi da utilizzare durante la procedura di upgrade del sistema operativo. Tali comandi garantiscono il corretto funzionamento di Sentinel dopo l'upgrade del sistema operativo.

Nota: eseguire l'upgrade di Sentinel prima dell'upgrade del sistema operativo.

Per eseguire l'upgrade del sistema operativo, effettuare i passaggi seguenti:

1. Nel server Sentinel in cui si desidera eseguire l'upgrade del sistema operativo, eseguire il login come uno degli utenti seguenti:
   - Utente `root`
   - Utente non root
2. Aprire un prompt dei comandi e passare alla directory in cui è stato estratto il file di installazione di Sentinel.
3. Interrompere i servizi Sentinel:

   ```
   rcsentinel stop
   ```
4. (Condizionale) Se Sentinel era in modalità FIPS prima dell'upgrade del sistema operativo, è necessario eseguire l'upgrade manuale dei file di database NSS mediante il seguente comando:

   ```
   certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
   ```

   Per eseguire l'upgrade del database NSS, seguire le istruzioni visualizzate.

   Fornire all'utente `novell` le autorizzazioni compete per i seguenti file:

   ```
   cert9.db
   key4.db
   pkcs11.txt
   ```
5. Eseguire l'upgrade del sistema operativo.
6. (Condizionale) Se si utilizza Mozilla Network Security Services (NSS) 3.29, due file RPM dipendenti, `libfreebl3 hmac` e `libsoftokn3 hmac`, non vengono installati. Installare manualmente i seguenti file RPM: `libfreebl3 hmac` e `libsoftokn3 hmac`.
7. (Condizionale) Per RHEL 7.*x*, eseguire il comando seguente per verificare che non siano presenti errori nel database RPM:

   `rpm -qa --dbpath <`*`ubicazione_installazione`*`>/rpm | grep novell`

   Esempio: `# rpm -qa --dbpath /custom/rpm | grep novell`

   7a Se vengono rilevati errori, eseguire il comando seguente per risolverli:

   `rpm --rebuilddb --dbpath <`*`ubicazione_installazione`*`>/rpm`

   Esempio: `# rpm --rebuilddb --dbpath /custom/rpm`

   7b Eseguire il comando indicato al passaggio 7 per verificare che non siano presenti errori.
8. Ripetere la procedura per i componenti seguenti:
   - Istanze di Collector Manager
   - Istanze di Correlation Engine
   - Istanze di NetFlow Collector Manager
9. Riavviare il servizio Sentinel:

`rcsentinel restart`

Questo passaggio non è valido per Sentinel ad alta disponibilità.

29 Esecuzione dell'upgrade dell'applicazione Sentinel

Le procedure descritte in questo capitolo illustrano come eseguire l'upgrade dell'applicazione Sentinel. È possibile scegliere di eseguire l'upgrade di Sentinel senza eseguire l'upgrade del sistema operativo SLES oppure eseguire l'upgrade sia di Sentinel che del sistema operativo SLES. Poiché l'applicazione Sentinel 8.2 include SLES 12 SP 3, il canale degli aggiornamenti di SLES 11 è ora obsoleto e verrà rimosso quando SUSE cesserà il supporto generale per SLES 11. Pertanto, per continuare a ricevere gli aggiornamenti del sistema operativo, è consigliabile eseguire l'upgrade all'applicazione Sentinel 8.2 che include il sistema operativo SLES 12 SP3. È necessario eseguire l'upgrade di Sentinel prima dell'upgrade del sistema operativo.

Esecuzione dell'upgrade di Sentinel

Upgrade di Sentinel mediante il canale degli aggiornamenti dell'applicazione

È possibile eseguire l'upgrade di Sentinel mediante Zypper. Zypper è uno strumento di gestione dei pacchetti della riga di comando che consente di eseguire un upgrade interattivo dell'applicazione. Nei casi in cui per completare l'upgrade è necessaria l'interazione dell'utente, ad esempio un aggiornamento del contratto di licenza con l'utente finale, l'upgrade dell'applicazione Sentinel deve essere eseguito tramite Zypper.

Per eseguire l'upgrade dell'applicazione mediante il canale degli aggiornamenti dell'applicazione:

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

   Per ulteriori informazioni, consultare “Backing Up and Restoring Data” (Backup e ripristino dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).
2. (Condizionale) Se nei file `server.xml`, `collector_mgr.xml` o `correlation_engine.xml` le impostazioni di configurazione sono state personalizzate, accertarsi di aver creato i rispettivi file delle proprietà denominati con l'ID del componente dell'oggetto affinché le personalizzazioni non vadano perse con l'upgrade. Per ulteriori informazioni, vedere “Maintaining Custom Settings in XML Files” (Conservazione delle impostazioni personalizzate nei file XML) nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel NetIQ).
3. Eseguire il login alla console dell'applicazione come utente `root`.
4. Eseguire il comando seguente:

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

5. (Condizionale) Se nel programma di installazione viene visualizzato un messaggio che richiede di risolvere la dipendenza per il pacchetto OpenSSH, immettere l'opzione appropriata per eseguire il downgrade del pacchetto OpenSSH.
6. (Condizionale) Se nel programma di installazione viene visualizzato un messaggio che indica una modifica nell'architettura ncgOverlay, immettere l'opzione appropriata per accettare la modifica dell'architettura.
7. (Condizionale) Se nel programma di installazione viene visualizzato un messaggio che richiede di risolvere la dipendenza di alcuni pacchetti dell'applicazione, immettere l'opzione appropriata per disinstallare i pacchetti dipendenti.
8. Immettere `Y` per continuare.
9. Per accettare il contratto di licenza, immettere `yes`.
10. Riavviare l'applicazione Sentinel.
11. (Condizionale) Se Sentinel è installato su una porta personalizzata oppure se l'istanza di Collector Manager o di Correlation Engine è in modalità FIPS, eseguire il comando seguente:

    ```
    /opt/novell/sentinel/setup/configure.sh
    ```
12. Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.
13. Svuotare la cache di Java Web Start nei computer client, affinché venga utilizzata la versione più recente delle applicazioni Sentinel.

    Per svuotare la cache di Java Web Start è possibile utilizzare il comando `avaws -clearcache` o Java Control Center. Per ulteriori informazioni, vedere http://www.java.com/en/download/help/plugin_cache.xml.
14. (Condizionale) Nel caso in cui sia stato eseguito un upgrade sostanziale del database PostgreSQL (ad esempio da 8.0 a 9.0 o da 9.0 a 9.1) eliminare i file della versione precedente dal database PostgreSQL. Per informazioni sull'esecuzione dell'upgrade del database PostgreSQL, vedere le note di rilascio di Sentinel.

    14a Passare all'utente Novell.

    ```
    su novell
    ```

    14b Passare alla cartella `bin`:

    ```
    cd /opt/novell/sentinel/3rdparty/postgresql/bin
    ```

    14c Cancellare i vecchi file PostgreSQL utilizzando il comando seguente:

    ```
    ./delete_old_cluster.sh
    ```
15. (Condizionale) Per eseguire l'upgrade dell'istanza di di Collector Manager o di Correlation Engine, procedere come descritto nel Passo 3 fino al Passo 11.
16. (Condizionale) Se si utilizza l'autenticazione Kerberos, abilitare AES256 in Java Runtime Environment poiché la cartella `java` viene sostituita con i file di default durante l'upgrade. Per abilitare AES256 in Java Runtime Environment, eseguire i passaggi seguenti:

    16a Effettuare il download di Java Cryptography Extension (JCE) 8 dall'ubicazione seguente: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`.

    16b Estrarre i due file `*.jar` e copiarli nella directory `/opt/novell/sentinel/jdk/jre/lib/security`.

    16c Riavviare Sentinel.
17. (Condizionale) Se si esegue Sentinel in un ambiente ad alta disponibilità, ripetere questi passaggi in tutti i nodi del cluster.

18 (Condizionale) Per eseguire l'upgrade del sistema operativo, vedere “Upgrade del sistema operativo” a pagina 162.

19 Riavviare Sentinel.

Upgrade di Sentinel mediante SMT

Negli ambienti protetti in cui l'applicazione deve essere eseguita senza un accesso diretto a Internet, è possibile configurarla con Subscription Management Tool (SMT), che consente di eseguire l'upgrade alle versioni più recenti disponibili.

1 Assicurarsi che l'applicazione sia configurata con SMT.

   Per ulteriori informazioni, vedere il “Configurazione dell'applicazione con SMT” a pagina 108.

2 eseguire il backup della configurazione, quindi creare un'esportazione ESM.

   Per ulteriori informazioni, consultare “Backing Up and Restoring Data” (Backup e ripristino dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).

3 (Condizionale) Se nei file `server.xml`, `collector_mgr.xml` o `correlation_engine.xml` le impostazioni di configurazione sono state personalizzate, accertarsi di aver creato i rispettivi file delle proprietà denominati con l'ID del componente dell'oggetto affinché le personalizzazioni non vadano perse con l'upgrade. Per ulteriori informazioni, vedere “Maintaining Custom Settings in XML Files” (Conservazione delle impostazioni personalizzate nei file XML) nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel NetIQ).

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

5 Aggiornare l'archivio per l'upgrade:

```
zypper ref -s
```

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

```
zypper lr
```

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

```
zypper lu
```

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

```
zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
```

9 Aggiornare l'applicazione:

```
zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
```

10 Riavviare l'applicazione.

```
rcsentinel restart
```

11 (Condizionale) Se Sentinel è installato su una porta personalizzata oppure se l'istanza di Collector Manager o di Correlation Engine è in modalità FIPS, eseguire il comando seguente:

```
/opt/novell/sentinel/setup/configure.sh
```

12 (Condizionale) Per eseguire l'upgrade dell'istanza di di Collector Manager o di Correlation Engine, procedere come descritto nel Passo 4 fino al Passo 11.

13 (Condizionale) Se si utilizza l'autenticazione Kerberos, abilitare AES256 in Java Runtime Environment poiché la cartella `java` viene sostituita con i file di default durante l'upgrade. Per abilitare AES256 in Java Runtime Environment, eseguire i passaggi seguenti:

13a Effettuare il download di Java Cryptography Extension (JCE) 8 dall'ubicazione seguente: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`.

13b Estrarre i due file `*.jar` e copiarli nella directory `/opt/novell/sentinel/jdk/jre/lib/security`.

13c Riavviare Sentinel.

14 (Condizionale) Se si esegue Sentinel in un ambiente ad alta disponibilità, ripetere questi passaggi in tutti i nodi del cluster.

15 (Condizionale) Per eseguire l'upgrade del sistema operativo, vedere “Upgrade del sistema operativo” a pagina 162.

16 Riavviare Sentinel.

Upgrade del sistema operativo

Dopo l'upgrade di Sentinel è necessario eseguire l'upgrade del sistema operativo. Dopo l'upgrade del sistema operativo, è necessario configurare l'applicazione per sfruttare le nuove funzionalità di gestione dell'applicazione Sentinel. La funzione di gestione dell'applicazione di Sentinel fornisce un'interfaccia utente basata sul Web semplice che consente di configurare e gestire l'applicazione. Questa sostituisce la funzionalità WebYast esistente.

Per eseguire l'upgrade del sistema operativo e configurare l'applicazione:

1 Eseguire l'upgrade di Sentinel. Per ulteriori informazioni, consultare “Esecuzione dell'upgrade di Sentinel” a pagina 159.

2 Interrompere i servizi Sentinel:

```
rcsentinel stop
```

3 (Condizionale) Se Sentinel era in modalità FIPS prima dell'upgrade del sistema operativo, è necessario eseguire l'upgrade manuale dei file di database NSS mediante il seguente comando:

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Per eseguire l'upgrade del database NSS, seguire le istruzioni visualizzate.

Fornire all'utente `novell` le autorizzazioni compete per i seguenti file:

```
cert9.db
key4.db
pkcs11.txt
```

4 (Condizionale) Se si utilizza Mozilla Network Security Services (NSS) 3.29, due file RPM dipendenti, `libfreebl3 hmac` e `libsoftokn3 hmac`, non vengono installati. Installare manualmente i seguenti file RPM: `libfreebl3 hmac` e `libsoftokn3 hmac`.

5 Effettuare il download del programma di installazione di SLES 12 SP3 e della utility post-upgrade dal sito Web Micro Focus Patch Finder. Per Sentinel ad alta disponibilità, effettuare anche il download del file SLES 12 SP3 HA.

6 Attenersi alle istruzioni di installazione per eseguire l'upgrade del sistema operativo. Per Sentinel ad alta disponibilità, quando viene richiesto di installare ulteriori prodotti aggiuntivi, selezionare l'ubicazione in cui è stato effettuato il download del file SLES 12 SP3 HA e procedere con l'upgrade.

Per ulteriori informazioni sull'upgrade a SLES 12 SP3, consultare la documentazione di SLES.

7 Durante il processo di upgrade, SLES rinomina il file `/etc/sysctl.conf` in `/etc/sysctl.conf.rpmsave` come backup e crea un file`new /etc/sysctl.conf`. Dopo l'upgrade, copiare il contenuto del file `/etc/sysctl.conf.rpmsave` nel file`etc/sysctl.conf`. Aprire il file `sysctl.conf` e ricercare la stringa `# Added by sentinel vm.max_map_count`. Spostare questa impostazione nella riga successiva come indicato di seguito:

Modifica

```
net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count : 65530
vm.max_map_count = 262144
```

In

```
net.core.wmem_max = 67108864
# Added by sentinel vm.max_map_count : 65530
vm.max_map_count = 262144
```

8 (Condizionale) Per Sentinel ad alta disponibilità, completare i passaggi descritti nelle seguenti sezioni:

- “Configurazione delle destinazioni iSCSI” a pagina 216
- “Configurazione degli iniziatori iSCSI” a pagina 217
- “Configurazione del cluster ad alta disponibilità” a pagina 218

9 Per configurare l'applicazione, eseguire la utility post-upgrade dal prompt dei comandi:

9a Decomprimere il file:

`tar - xvf < nome file del programma di installazione della utility post-upgrade>. tar. gz`

9b Passare alla directory in cui è stato estratta la utility:

`cd < nome file del programma di installazione della utility post-upgrade>`

9c Per configurare l'applicazione, eseguire il seguente script:

`./appliance_SLESISO_post_upgrade.sh`

Nota: Non eseguire questo script in remoto poiché comporta la riconfigurazione della rete.

9d Per completare la configurazione, seguire le istruzioni visualizzate sullo schermo.

I pacchetti installati verranno riconfigurati dallo scritp che eseguirà anche la configurazione dei pacchetti per la gestione dell'applicazione.

10 Utilizzando il codice di registrazione esistente, registrarsi nuovamente per gli aggiornamenti per ricevere aggiornamenti di Sentinel e del sistema operativo. Per ulteriori informazioni, consultare “Registrazione degli aggiornamenti” a pagina 106.

30 Configurazioni di post-upgrade

In questo capitolo sono descritte le configurazioni di post-upgrade.

Sicurezza dei dati in Elasticsearch

Sentinel utilizza Kibana, un dashboard di ricerca e analisi basato su browser che facilita la visualizzazione di eventi e avvisi nei dashboard. Sentinel memorizza e indicizza gli avvisi in Elasticsearch. È possibile configurare Sentinel affinché memorizzi e indicizzi gli eventi anche in Elasticsearch, così da sfruttarne le funzionalità di visualizzazione degli eventi. I dashboard di Sentinel accedono ai dati provenienti da Elasticsearch per presentare avvisi ed eventi. Per garantire che i dashboard visualizzino solo i dati che il ruolo dell'utente è autorizzato a visualizzare e per impedire l'accesso non autorizzato ai dati in Elasticsearch, è necessario installare il plug-in di sicurezza per Elasticsearch. Per ulteriori informazioni, consultare “Sicurezza dei dati in Elasticsearch” a pagina 79.

Configurazione delle visualizzazioni degli eventi

In Sentinel sono ora disponibili visualizzazioni degli eventi che presentano i dati sotto forma di grafici, tabelle e mappe, per facilitare la visualizzazione e l'analisi di grandi volumi di dati, quali eventi, eventi dei flussi IP e avvisi. È inoltre possibile creare visualizzazioni e dashboard personalizzati.

Sentinel utilizza Kibana, un dashboard di ricerca e analisi basato su browser che consente di cercare e visualizzare gli eventi. Kibana accede ai dati dall'archivio dati di visualizzazione (Elasticsearch) per presentare gli eventi nei dashboard. Sentinel include di default un nodo Elasticsearch. Per memorizzare e indicizzare gli eventi in Elasticsearch è necessario abilitare la visualizzazione degli eventi. Per ulteriori informazioni, consultare “Configurazione dell'archivio dati di visualizzazione” a pagina 43.

Nota: alcuni dei dashboard di Sentinel che utilizzano Kibana non vengono caricati dopo l'upgrade a Sentinel 8.2. Questo problema si verifica in quanto è stato eseguito l'upgrade delle versioni di Elasticsearch e Kibana in Sentinel 8.2 e il file di indice di Kibana esistente non è compatibile con tali versioni di Elasticsearch e Kibana. Per risolvere questo problema, è necessario eliminare manualmente il file di indice di Kibana esistente e ricrearne uno nuovo. Per ulteriori informazioni, vedere l'articolo 7022736 della knowledgebase.

Configurazione della raccolta dati del flusso IP

Sentinel utilizza ora ArcSight SmartConnectors, che permette di controllare la rete aziendale mediante la raccolta dati del flusso IP in aggiunta ai dati NetFlow. SmartConnectors raccoglie i dati del flusso IP come eventi, per consentire di:

- Utilizzare le istanze esistenti di Collector Manager per raccogliere i dati del flusso IP. Non è più necessario utilizzare istanze di NetFlow Collector Manager per raccogliere i dati NetFlow.
- Utilizzare i dati del flusso IP in svariate aree di Sentinel, quali visualizzazioni, instradamento degli eventi, federazione di dati, rapporti e correlazione.
- Applicare policy di permanenza ai dati del flusso IP, così da memorizzarli per il periodo di tempo desiderato.

Dopo aver eseguito l'upgrade di Sentinel, è possibile continuare a utilizzare le funzionalità NetFlow o scegliere di configurare la raccolta dati del flusso IP. Tuttavia, grazie alla disponibilità della raccolta dati del flusso IP e alla funzionalità di visualizzazione, le funzionalità NetFlow precedentemente disponibili, incluse le viste NetFlow, sono ora obsolete e verranno rimosse in futuro al fine di migliorare l'esperienza dell'utente.

Dopo aver abilitato la raccolta dati del flusso IP:

- I dati del flusso IP vengono raccolti come eventi e quindi conteggiati nel totale di EPS.
- I dati NetFlow raccolti prima di abilitare il flusso IP andranno persi. Il sistema NetFlow obsoleto aveva un periodo massimo di permanenza di 3 giorni. È possibile conservare gli eventi del flusso IP per tutto il tempo desiderato.
- Non è possibile eseguire la migrazione dei dati NetFlow raccolti prima di abilitare il flusso IP nella funzionalità Flusso IP.
- Non è possibile ripristinare la configurazione a meno che non si reinstalli Sentinel.
- Verrà eseguito il logout da Sentinel principale e si dovrà ripetere il login.

Per configurare la raccolta dati del flusso IP:

1. Installare e configurare ArcSight SmartConnector. Durante la configurazione, assicurarsi di configurare le istanze appropriate di SmartConnectors che raccolgono i dati del flusso IP.

   Per informazioni sulla configurazione di SmartConnectors, consultare la documentazione di Generic Universal CEF Collector sul sito Web dei plug-in di Sentinel.
2. In **Sentinel principale** > **Raccolta** > **Flusso IP**, selezionare **Raccogli dati flusso IP** e fare clic su **Abilita**.

Nota: poiché gli eventi del flusso IP vengono ora inviati a Collector Manager, non è più necessario utilizzare istanze di NetFlow Collector Manager. Pertanto, è possibile disinstallare eventuali istanze esistenti di NetFlow Collector Manager. Per ulteriori informazioni, consultare “Disinstallazione dell'istanza di NetFlow Collector Manager” a pagina 233.

Configurazione di post-upgrade per la gestione scalabile dei dati di Sentinel

- “Installazione del plug-in di sicurezza per Elasticsearch” a pagina 167
- “Aggiornamento della applicazioni Spark su YARN” a pagina 167

- “Abilitazione delle funzionalità di Sentinel” a pagina 168
- “Aggiornamento di dashboard e visualizzazioni in Sentinel Scalable Data Manager” a pagina 168

Installazione del plug-in di sicurezza per Elasticsearch

Oltre ai nodi Elasticsearch esterni, Sentinel include ora di default un nodo Elasticsearch locale per la visualizzazione dei dati. È pertanto necessario installare un plug-in per l'istanza locale di Elasticsearch. Per ulteriori informazioni, consultare “Installazione del plug-in di sicurezza per Elasticsearch” a pagina 80.

Poiché viene eseguito l'upgrade di Elasticsearch e Kibana utilizzati in Sentinel, è necessario ripetere l'installazione di tutti i plug-in di sicurezza per Elasticsearch nei nodi Elasticsearch esistenti. Per ulteriori informazioni sulla reinstallazione del plug-in di sicurezza per Elasticsearch, vedere “Reinstallazione del plug-in di sicurezza per Elasticsearch” a pagina 84.

Aggiornamento della applicazioni Spark su YARN

Durante l'upgrade di Sentinel, vengono aggiornati anche alcuni file dell'applicazione Spark. È necessario inviare nuovamente le applicazioni Spark con questi file aggiornati effettuando i seguenti passaggi:

1. Accedere al server SSDM come utente `novell` e copiare i file nel server della cronologia Spark in cui è installato HDFS NameNode:

   ```
   cd /etc/opt/novell/sentinel/scalablestore
   ```

   ```
   scp SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties log4j.properties manage_spark_jobs.sh root@<nodo_hdfs>:<directory_di destinazione>
   ```

   dove <*directory_di destinazione*> è una directory qualsiasi in cui si desidera collocare i file copiati. Inoltre, assicurarsi che l'utente `hdfs` disponga delle autorizzazioni complete per questa directory.
2. Eseguire il login al server <*nodo_hdfs*> come utente root e modificare la proprietà dei file copiati in utente `hdfs`:

   ```
   cd <directory_di destinazione>
   ```

   ```
   chown hdfs SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties log4j.properties manage_spark_jobs.sh
   ```

   Assegnare l'autorizzazione eseguibile allo script `manage_spark_jobs.sh`.
3. Assicurarsi che i lavori Spark abbiano completato l'elaborazione di tutti i dati:

   Passare all'interfaccia Web ResourceManager di YARN e visualizzare ciascuna applicazione Spark di Sentinel. I dati dell'applicazione Spark Streaming mostreranno l'azzeramento della frequenza di input quando tutti i dati sono stati elaborati da Kafka.
4. Eseguire il seguente comando per interrompere l'elaborazione dei dati:

   ```
   ./manage_spark_jobs.sh stop
   ```
5. Annullare il punto di controllo dell'elaborazione dei dati:

   ```
   sudo -u hdfs hadoop fs -rm -R -skipTrash  /spark/checkpoint
   ```

   dove `/spark/checkpoint` è la directory del punto di controllo.
6. Eseguire lo script seguente per inviare nuovamente i lavori Spark:

   ```
   ./manage_spark_jobs.sh start
   ```

Il comando precedente impiega qualche istante per completare il processo di invio.

7 (Facoltativo) Eseguire il seguente comando per verificare lo stato dei lavori Spark inviati:

```
./manage_spark_jobs.sh status
```

8 Riprendere l'inoltro degli eventi a Kafka per consentire a Spark di iniziare a elaborare gli eventi:

8a In Sentinel Main, fare clic su **Memorizzazione** > **Memorizzazione scalabile** > **Configurazione avanzata** > **Kafka**.

8b Impostare la seguente proprietà su false:

```
pause.events.tokafka
```

8c Fare clic su **Salva**.

Abilitazione delle funzionalità di Sentinel

Quando si esegue l'upgrade da SSDM 8.0.*x.x*, alcune delle funzionalità di Sentinel aggiunte in Sentinel 8.1 e versioni successive non sono disponibili per default. Tali funzionalità devono essere abilitate manualmente nel file `/etc/opt/novell/sentinel/config/ui-configuration.properties`.

1 Eseguire il login al server Sentinel come utente `novell`.

2 Aprire il file `/etc/opt/novell/sentinel/config/ui-configuration.properties`.

3 Modificare le seguenti proprietà su false:

```
alerts.hideUI
solutionDesigner.launcher.hideUI
correlation.hideUI
scc.configurations.solutionPacks.hideUI
people.hideUI
permission.knowledgeBase.hideUI
scc.menuBarItem.toolsMenu.hideUI
scc.toolBarItem.peopleBrowser.hideUI
integration.hideUI
```

4 Aggiornare il browser di Sentinel.

Aggiornamento di dashboard e visualizzazioni in Sentinel Scalable Data Manager

Dopo aver eseguito l'upgrade di SSDM, è necessario aggiornare i dashboard e le visualizzazioni affinché vengano applicati i miglioramenti inclusi nella versione più recente di dashboard e visualizzazioni.

Quando si esegue l'upgrade di SSDM, dashboard e visualizzazioni non vengono aggiornati per default. È comunque possibile eseguire l'aggiornamento manualmente dopo l'upgrade. Per effettuare l'aggiornamento, eliminare i dashboard e le visualizzazioni esistenti ed eseguire lo script `load_kibana_data.sh`, che installa i dashboard e le visualizzazioni più recenti.

Importante: quando si esegue l'aggiornamento di dashboard e visualizzazioni, le personalizzazioni eventualmente eseguite vanno perse.

Per aggiornare dashboard e visualizzazioni:

1. Eseguire il login all'interfaccia Web di SSDM e passare alla visualizzazione degli eventi.
2. Nella visualizzazione degli eventi, scegliere **Settings** (Impostazioni) > **Objects** (Oggetti) > **Dashboards** (Dashboard).
3. Selezionare i dashboard che si desidera aggiornare, quindi fare clic su **Delete** (Elimina).
4. Fare clic su **Visualizations**(Visualizzazioni). Selezionare le visualizzazioni che si desidera aggiornare, quindi fare clic su **Delete** (Elimina).
5. Eseguire il logout dall'interfaccia Web di SSDM.
6. Eseguire il login al server SSDM come utente `novell`.
7. Passare alla directory `/opt/novell/sentinel/bin`.
8. Eseguire `load_kibana_data.sh` utilizzando il comando seguente:

   ```
   ./load_kibana_data.sh http://<indirizzo ip>:<porta>> <avvisi/eventi/varie>
   ```

   Ad esempio:

   ```
   ./load_kibana_data.sh http://127.0.0.1:9200 avvisi
   ```

   ```
   ./load_kibana_data.sh http://127.0.0.1:9200 eventi
   ```
9. Eseguire il login all'interfaccia Web di SSDM e passare alla visualizzazione degli eventi per visualizzare i dashboard e le visualizzazioni aggiornati.

Aggiunta del driver JDBC DB2

Dopo aver eseguito l'upgrade a Sentinel, aggiungere il driver JDBC corretto e configurarlo per la raccolta e la sincronizzazione dei dati eseguendo le operazioni seguenti:

1. Copiare nella cartella `/opt/novell/sentinel/lib` la versione corretta del driver IBM DB2 JDBC (`db2jcc-*.jar`) per la versione del database DB2 in uso.
2. Assicurarsi che vengano impostate la proprietà e le autorizzazioni necessarie per il file del driver.
3. Configurare il driver per la raccolta dati. Per ulteriori informazioni, vedere la documentazione del connettore del database.

Configurazione delle proprietà della federazione dati nell'applicazione Sentinel

Elaborare la procedura seguente dopo aver eseguito l'upgrade dell'applicazione Sentinel, in modo tale che la federazione dati non riporti alcun errore nell'ambiente in cui sono stati configurati due o più NIC:

1. Nel server del richiedente autorizzato, aggiungere la proprietà seguente nel file `/etc/opt/novell/sentinel/config/configuration.properties` come illustrato di seguito:

   ```
   sentinel.distsearch.console.ip=<uno degli indirizzi IP del richiedente autorizzato>
   ```
2. Nel server dell'origine dati, aggiungere la proprietà seguente nel file `/etc/opt/novell/sentinel/config/configuration.properties` come illustrato di seguito:

   ```
   sentinel.distsearch.target.ip=<uno degli indirizzi IP dell'origine dati>
   ```
3. Riavviare Sentinel:

   ```
   rcsentinel restart
   ```

4 Eseguire il login al server del richiedente autorizzato e fare clic su Integrazione. Se l'origine dati che si desidera aggiungere è già presente, eliminarla e aggiungerla nuovamente utilizzando uno degli indirizzi IP specificati nel passaggio 2.

   Utilizzare la stessa procedura per aggiungere richiedenti autorizzati usando gli indirizzi IP specificati al passaggio 1.

Registrazione dell'applicazione Sentinel per gli aggiornamenti

Se è stato eseguito l'upgrade del sistema operativo, è necessario registrare di nuovo l'applicazione Sentinel per ricevere aggiornamenti del sistema operativo e di Sentinel. È possibile utilizzare la chiave di registrazione esistente per registrare di nuovo gli aggiornamenti. Per registrare l'applicazione, vedere “Registrazione degli aggiornamenti” a pagina 106.

Aggiornamento dei database esterni per la sincronizzazione dei dati

A partire da Sentinel 8.x, la dimensione del campo evento `Message (msg)` è stata portata da 4000 a 8000 caratteri per consentire di immettere maggiori informazioni nel campo.

Se nelle versioni precedenti di Sentinel era stata creata una policy per la sincronizzazione dei dati del campo evento Message (msg) con un database esterno, è necessario aumentare di conseguenza la dimensione della colonna mappata corrispondente nel database esterno.

Nota: il passaggio precedente è valido solo se si esegue l'upgrade da versioni precedenti di Sentinel alla versione 8.x.

Riautenticazione di Sentinel in modalità di autenticazione multifattori

Quando si esegue l'upgrade del server Sentinel in modalità MFA, le istanze esistenti di NetFlow Collector Manager non rieseguono automaticamente l'autenticazione al server Sentinel. Per ripetere manualmente l'autenticazione delle istanze di NetFlow Collector Manager al server Sentinel è necessario eseguire i passaggi seguenti.

Per ripetere l'autenticazione a Sentinel in modalità MFA:

1 Eseguire il login al computer in cui risiede l'istanza di NetFlow Collector Manager.

2 Spostarsi in `/opt/novell/sentinel/setup`.

3 Eseguire lo script `configure.sh`.

   Viene richiesto di eseguire il login al server Sentinel.

4 Specificare il nome utente e la password LDAP

5 Fornire l'ID e il segreto del client Sentinel.

   Per recuperare l'ID e il segreto client di Sentinel, visitare l'URL seguente:

   `https://FQDN_di_Sentinel:porta/SentinelAuthServices/oauth/clients`

Dove:

- `FQDN_di_Sentinel` è il nome di dominio completo del server Sentinel.

  Ad esempio, `abc.netiq.com`

  in cui `abc` è il nome host del server Sentinel, `netiq.com` è il nome del dominio.
- `Porta` è la porta utilizzata da Sentinel (in genere 8443).

L'URL specificato utilizza la sessione Sentinel corrente per recuperare l'ID e il segreto del client Sentinel.

31 Esecuzione dell'upgrade dei plug-in di Sentinel

Le installazioni di upgrade di Sentinel non eseguono l'upgrade dei plug-in non compatibili con l'ultima versione di Sentinel.

Sul sito Web dei plug-in di Sentinel vengono costantemente resi disponibili plug-in nuovi e aggiornati, inclusi i Pacchetti soluzione. Effettuando il download e installando la versione più recente dei plug-in è possibile ottenere le correzioni dei bug, gli aggiornamenti della documentazione e i miglioramenti più recenti. Per informazioni sull'installazione dei plug-in, vedere la relativa documentazione specifica.

VI Migrazione dei dati dalla memorizzazione tradizionale

La migrazione dei dati da Sentinel con la memorizzazione tradizionale consente di sfruttare i dati di Sentinel esistenti e il tempo investito. Per eseguire la migrazione dei dati da Sentinel con la memorizzazione tradizionale, la versione di Sentinel sui server Sentinel di origine e destinazione deve essere la stessa. Se, ad esempio, si desidera eseguire la migrazione dei dati da Sentinel 8.1 (origine) a Sentinel 8.2 (destinazione), è necessario innanzitutto eseguire l'upgrade di Sentinel 8.1 a Sentinel 8.2 e quindi iniziare il processo di migrazione dei dati.

In questa sezione si forniscono informazioni sulla migrazione dei dati esistenti verso il componente di memorizzazione desiderato.

32 Migrazione dei dati nella memorizzazione scalabile

È possibile disporre di un singolo server Sentinel o di più server Sentinel con la memorizzazione tradizionale. Il processo di migrazione dei dati che è necessario eseguire dipende da come si desidera configurare e mantenere l'installazione di Sentinel.

Tabella 32-1 *Processo di migrazione dei dati per la distribuzione di Sentinel*

Distribuzione di Sentinel	Processo di migrazione
Si dispone di un singolo server Sentinel e si pianifica di eseguire l'upgrade del server Sentinel esistente alla memorizzazione scalabile.	Una volta eseguito l'upgrade del server Sentinel e abilitata la memorizzazione scalabile, eseguire la migrazione dei dati degli eventi e dei dati non elaborati dalla memorizzazione tradizionale a quella scalabile. Per ulteriori informazioni, consultare la Capitolo 34, “Migrazione dei dati”, a pagina 185.
Si dispone di un singolo server Sentinel con la memorizzazione tradizionale e si desidera configurare un altro server Sentinel per la memorizzazione scalabile in modo da poter utilizzare tutte le funzionalità in Sentinel.	Ricorrere all'utility di backup e ripristino per eseguire la migrazione dei dati da Sentinel con la memorizzazione tradizionale a Sentinel con la memorizzazione scalabile. Per informazioni sull'utilizzo dell'utility di backup e ripristino, vedere “Backing Up and Restoring Data” (Backup e ripristino dei dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Distribuzione di Sentinel	Processo di migrazione
Si dispone di una configurazione a più livelli con più server Sentinel e si pianifica di configurare un nuovo server Sentinel o di utilizzare uno dei server esistenti per la memorizzazione scalabile. È necessario eseguire la migrazione dei dati di configurazione oltre ai dati evento e a quelli non elaborati.	In una configurazione a più livelli, è possibile identificare uno dei server Sentinel tradizionali contenente la maggior parte dei dati e utilizzare l'utility di backup e ripristino per eseguire la migrazione dei dati. Se è necessario eseguire il backup della parte restante dei server Sentinel, i dati di configurazione, i dati evento e i dati non elaborati devono essere migrati da tali server utilizzando un approccio diverso, descritto più avanti in questa sezione. È inoltre necessario ricreare manualmente una parte delle configurazioni. Non è possibile ricorrere all'utility di backup e ripristino per eseguire la migrazione dei dati da più server, in quanto l'utility sostituisce i dati esistenti al momento del ripristino. Se, ad esempio, è già stato eseguito il ripristino dei dati dal Server A e si cerca di ripristinare i dati dal Server B, questa utility sostituisce i dati già ripristinati nel Server A. Pertanto, per comprendere il processo di migrazione dei dati interessato, attenersi alle istruzioni fornite nelle sezioni successive nello stesso ordine: ◆ Dati di cui è possibile eseguire la migrazione ◆ Migrazione dei dati di configurazione ◆ Migrazione dei dati ◆ Migrazione dei dati degli avvisi e di NetFlow ◆ Aggiornamento dei client Sentinel ◆ Importazione della configurazione ESM

Dati di cui è possibile eseguire la migrazione

È possibile eseguire la migrazione di dati evento, dati non elaborati e alcuni dei dati di configurazione. È necessario ricreare manualmente il resto della configurazione, per la quale non è possibile eseguire la migrazione.

Tabella 32-2 Configurazioni di cui è possibile eseguire la migrazione e configurazioni che è necessario ricreare

Configurazioni di cui è possibile eseguire la migrazione	Configurazione che è necessario ricreare
◆ Regole di correlazione ◆ Azioni ◆ Mappe ◆ Filtri ◆ Feed minacce ◆ Configurazione ESM ◆ Avvisi eccetto dati Knowledge Base ◆ NetFlow	◆ Tenant, ruoli, utenti e configurazione LDAP ◆ Regole di instradamento di eventi e avvisi ◆ Policy di permanenza di dati e avvisi ◆ Dashboard ◆ Viste in tempo reale ◆ Informazioni sull'identità ◆ Configurazione feed ◆ Configurazione plug-in azione e integratore ◆ Configurazione della sicurezza

Migrazione dei dati di configurazione

Prima di eseguire la migrazione dei dati evento, è necessario innanzitutto eseguire la migrazione dei dati di configurazione al server di destinazione Sentinel. È possibile eseguire il backup di una parte della configurazione utilizzando Solution Designer e le opzioni Esporta e Importa in Gestione origine eventi (ESM). È necessario ricreare manualmente la parte restante dei dati di configurazione per i quali non è possibile eseguire il backup o l'esportazione.

- “Backup dei dati sul server di origine” a pagina 179
- “Ripristino dei dati sul server di destinazione” a pagina 180

Backup dei dati sul server di origine

È necessario eseguire il backup dei dati necessari utilizzando varie opzioni in Sentinel.

- “Utilizzo dei pacchetti di soluzioni” a pagina 180
- “Utilizzo dell'opzione Esporta configurazione in ESM” a pagina 180

Utilizzo dei pacchetti di soluzioni

Eseguire il backup della configurazione seguente sul server di origine mediante Solution Designer:

Tabella 32-3 *Dati di configurazione*

	Dati	Note
❒	Regole di correlazione	Creare controlli distinti per ciascun Correlation Engine in modo da poter eseguire la migrazione delle regole separatamente per gli specifici Correlation Engine.
❒	Azioni	È possibile eseguire il backup solo delle azioni JavaScript e non delle azioni legacy, ad esempio un elenco dinamico e la creazione di un incidente.
❒	Arricchimento dell'evento	Sentinel esegue anche il backup delle mappe associate ai campi evento. Pertanto, non è necessario ricreare le mappe associate dopo il ripristino dei dati di arricchimento dell'evento.
❒	Filtri	Backup di tutti i filtri personalizzati.
❒	Feed	Il pacchetto di soluzioni esegue il backup unicamente dei plug-in dei feed ma non quello della configurazione dei plug-in.

Per informazioni sul backup dei dati in Solution Designer, vedere “Creating Solution Packs” (Creazione di pacchetti di soluzioni) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Utilizzo dell'opzione Esporta configurazione in ESM

Eseguire il backup della raccolta dati utilizzando l'opzione Esporta configurazione in Gestione origine eventi (ESM). Per ulteriori informazioni, vedere “Exporting Configurations” (Esportazione delle configurazioni) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Ripristino dei dati sul server di destinazione

- “Installazione dei dati di configurazione dal pacchetto di soluzioni” a pagina 180
- “Ricreazione manuale della configurazione” a pagina 181

Installazione dei dati di configurazione dal pacchetto di soluzioni

Importare i dati di configurazione di cui è stato eseguito il backup sul server utilizzando Solution Designer. Per ulteriori informazioni, vedere “Installing Content from Solution Packs” (Installazione del contenuto dai pacchetti di soluzioni) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Rinominare i nomi duplicati degli oggetti quali filtri, azioni e regole di correlazione. Di default, tutti i filtri sono pubblici quando vengono importati sul server di destinazione. Assegnare di nuovo l'autorizzazione per ogni filtro manualmente.

Ricreazione manuale della configurazione

Oltre ai dati di configurazione importati dal pacchetto di soluzioni, è necessario ricreare manualmente tutte le altre configurazioni. Per ulteriori informazioni sulle configurazioni che è necessario ricreare manualmente, vedere Tabella 32-2, “Configurazioni di cui è possibile eseguire la migrazione e configurazioni che è necessario ricreare”, a pagina 179.

Migrazione di dati evento e dati non elaborati

Per eseguire la migrazione di dati degli eventi e dati non elaborati, vedere Migrazione dei dati.

Migrazione dei dati degli avvisi e di NetFlow

È possibile utilizzare l'utility di backup e ripristino per eseguire la migrazione dei dati degli avvisi e di NetFlow dal server di origine al server di destinazione. Per gli avvisi, questa utility ripristina gli eventi che hanno attivato l'avviso. Tuttavia, non ripristina le informazioni sulla regola di correlazione e la knowledge base associate.

Utilizzare i seguenti comandi per eseguire il backup e il ripristino dei dati degli avvisi e di NetFlow:

```
For backing up:
./backup_util.sh -i

For restore:
./backup_util.sh -m restore -f <backup_file_path>
```

Per i dati degli avvisi e di NetFlow, si dispone di un'opzione per sostituire o aggiungere ai dati esistenti. Scegliere l'opzione desiderata.

Sebbene il comando precedente consenta di eseguire il backup e il ripristino dei dati di Security Intelligence, non è possibile utilizzare tali dati perché Security Intelligence non è disponibile in SSDM.

Per informazioni dettagliate sull'utilizzo dell'utility di backup e ripristino, vedere “Backing Up and Restoring Data” (Backup e ripristino dei dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Aggiornamento dei client Sentinel

È necessario eseguire l'aggiornamento della configurazione delle istanze di Collector Manager, Correlation Engine e NetFlow Collector Manager in modo che venga avviata la comunicazione con il server Sentinel di destinazione. Per ulteriori informazioni, vedere “Updating Sentinel Clients” (Aggiornamento dei client Sentinel) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Nota: sebbene sia già stata eseguita la migrazione dei dati degli eventi dal server di origine, è necessario eseguire nuovamente lo script per eseguire la migrazione dei dati degli eventi che potrebbero essere arrivati durante o dopo tale processo di migrazione. Per ulteriori informazioni, consultare la Capitolo 34, “Migrazione dei dati”, a pagina 185.

Importazione della configurazione ESM

Importare la configurazione della raccolta dati utilizzata sul server di origine utilizzando l'opzione Importa configurazione nell'interfaccia utente di ESM. Per ulteriori informazioni, vedere “Importing Configurations” (Importazione delle configurazioni) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

33 Migrazione dei dati in Elasticsearch

Sentinel memorizza i dati nella memorizzazione tradizionale basata su file e, di default, li indicizza in locale nel server Sentinel. Quando si abilita la visualizzazione degli eventi, Sentinel memorizza e indicizza i dati in Elasticsearch oltre che nella memorizzazione tradizionale basata su file. I dashboard visualizzano solo gli eventi elaborati dopo aver abilitato la visualizzazione degli eventi. Per visualizzare gli eventi esistenti presenti nella memorizzazione basata su file, è necessario eseguire la migrazione dei dati dalla memorizzazione basata su file a Elasticsearch. Per eseguire la migrazione dei dati in Elasticsearch, vedere Capitolo 34, “Migrazione dei dati”, a pagina 185.

34 Migrazione dei dati

Per eseguire la migrazione dei dati in uno dei componenti di memorizzazione dati seguenti, è possibile utilizzare lo script `data_uploader.sh`:

- **Kafka:** è possibile eseguire la migrazione in Kafka sia degli eventi che dei dati non elaborati. Eseguire lo script singolarmente per i dati evento e per i dati non elaborati. Lo script esegue la migrazione dei dati negli argomenti Kafka.

  È possibile specificare personalizzazioni come la compressione dei dati durante la migrazione, l'invio dei dati in batch e così via. Per specificare queste personalizzazioni, creare un file di proprietà e aggiungere le proprietà richieste nel formato chiave-valore. Ad esempio, è possibile aggiungere proprietà nel modo indicato di seguito:

  ```
  compression.type=lz4
  ```

  ```
  batch.size=20000
  ```

  Per informazioni sulle proprietà Kafka, vedere la documentazione Kafka. Impostare le proprietà e i relativi valori a propria discrezione in quanto lo script non convalida queste proprietà.

  Nota: verificare che il server Sentinel sia in grado di risolvere tutti i nomi host del broker Kafka in indirizzi IP validi per tutto il cluster Kafka. Se il DNS non è configurato per consentire questa operazione, aggiungere i nomi host del broker Kafka nel file `/etc/hosts` del server Sentinel.

- **Elasticsearch:** è possibile eseguire la migrazione in Elasticsearch solo dei dati degli eventi. Prima di eseguire la migrazione dei dati, verificare che sia stata abilitata la visualizzazione degli eventi. Per ulteriori informazioni, consultare “Abilitazione della visualizzazione degli eventi” a pagina 125.

Lo script trasferisce i dati per l'intervallo di date (da e a) specificato. Quando si esegue lo script, vengono visualizzati i parametri obbligatori e opzionali che è necessario specificare per avviare la migrazione dei dati e anche le informazioni relative alle proprietà pertinenti da utilizzare per il componente di memorizzazione dati desiderato.

Lo script deve essere eseguito come utente novell. Pertanto, assicurarsi che le directory dei dati e i file specificati dispongano delle autorizzazioni appropriate per l'utente novell. Di default, lo script esegue la migrazione dei dati dalla memorizzazione primaria. Se si desidera eseguire la migrazione dei dati dalla memorizzazione secondaria, specificare il percorso appropriato della memorizzazione secondaria quando si esegue lo script.

Per eseguire la migrazione dei dati:

1. Eseguire il login al server Sentinel come utente novell.
2. Eseguire lo script seguente:

   ```
   /opt/novell/sentinel/bin/data_uploader.sh
   ```

3. Seguire le istruzioni visualizzate ed eseguire nuovamente lo script con i parametri richiesti.

Il periodo di permanenza dei dati di cui è stata eseguita la migrazione è quello impostato nel server di destinazione.

Una volta eseguita la migrazione dei dati, lo script registra lo stato, ad esempio partizioni di cui è stata completata la migrazione, partizioni per le quali la migrazione ha avuto esito negativo, numero di eventi per i quali è stata eseguita la migrazione e così via. Per le partizioni con la data del giorno precedente e del giorno corrente, lo stato di trasferimento dei dati verrà mostrato IN_PROGRESS considerando gli eventi che potrebbero verificarsi in ritardo.

Negli scenari in cui la migrazione dei dati non è stata completata correttamente o in cui lo stato di migrazione dei dati per le partizioni continua a indicare IN_PROGRESS, eseguire nuovamente lo script. Quando si esegue nuovamente lo script, viene prima verificato il file di stato per individuare le partizioni di cui è già stata eseguita la migrazione, quindi viene eseguita la migrazione solo di quelle rimanenti. Lo script conserva i log nella directory /`var/opt/novell/sentinel/log/data_uploader.log` ai fini della risoluzione dei problemi.

VII Installazione di Sentinel per alta disponibilità

In questa sezione si descrive come installare Sentinel in una modalità ad alta disponibilità attiva-passiva che consenta il failover di Sentinel in un nodo ridondante del cluster in caso di errore hardware o software. Per ulteriori informazioni sull'implementazione dell'alta disponibilità e il disaster recovery nell'ambiente Sentinel, rivolgersi al supporto tecnico .

Nota: la configurazione per alta disponibilità è supportata solo nel server Sentinel. Le istanze di Collector Manager e di Correlation Engine possono comunque comunicare con il server Sentinel ad alta disponibilità.

---

35 Concetti

Per alta disponibilità si intende una metodologia di progettazione che mira a mantenere un sistema disponibile all'uso per il maggior tempo possibile. L'obiettivo è quello di ridurre al minimo il tempo di fermo, ad esempio i guasti di sistema e la manutenzione, e di minimizzare il tempo necessario per rilevare e risolvere gli eventi di guasto che si verificano. In pratica, sono necessari meccanismi automatizzati in grado di rilevare e risolvere i guasti, poiché si devono raggiungere livelli di disponibilità superiori.

Per ulteriori informazioni sull'alta disponibilità, consultare la SUSE High Availability Guide (Guida all'alta disponibilità SUSE).

Sistemi esterni

Sentinel è un'applicazione complessa e articolata su più livelli, che utilizza e fornisce una vasta gamma di servizi, oltre a integrare numerosi sistemi esterni di terze parti per la raccolta e la condivisione dei dati, nonché per la risoluzione dei casi. La maggior parte delle soluzioni ad alta disponibilità permette a chi le implementa di dichiarare le dipendenze fra i servizi che devono garantire un'elevata disponibilità, ma tale possibilità si applica solo ai servizi eseguiti nel cluster stesso. I sistemi esterni a Sentinel, quali ad esempio le origini eventi, devono essere configurati separatamente affinché la loro disponibilità soddisfi le esigenze dell'organizzazione e in modo che possano gestire correttamente le situazioni in cui Sentinel non è disponibile per un certo periodo di tempo, ad esempio in caso di failover. Se i diritti di accesso prevedono limitazioni rigide, ad esempio se si utilizzano sessioni autenticate per l'invio e/o la ricezione dei dati fra un sistema di terze parti e Sentinel, il sistema terzo deve essere configurato affinché accetti le sessioni o le avvii in qualsiasi nodo del cluster (in questo caso Sentinel deve essere configurato con un indirizzo IP virtuale).

Memorizzazione condivisa

Tutti i cluster ad alta disponibilità necessitano di un qualche tipo di memorizzazione condivisa, affinché sia possibile spostare rapidamente i dati dell'applicazione da un nodo del cluster a un altro in caso di errore nel nodo di origine. Anche la memorizzazione deve essere ad alta disponibilità e in genere questo requisito si soddisfa utilizzando la tecnologia SAN (Storage Area Network) connessa ai nodi del cluster mediante una rete Fibre Channel. Altri sistemi utilizzano tecnologie NAS (Network Attached Storage), iSCSI o altre tecnologie che consentono il montaggio in remoto della memorizzazione condivisa. Il requisito fondamentale della memorizzazione condivisa consiste nella possibilità di spostare con precisione la memorizzazione da un nodo guasto a un nuovo nodo dello stesso cluster.

Per la memorizzazione condivisa, in Sentinel è possibile utilizzare due approcci di base. Il primo prevede l'ubicazione di tutti i componenti (file binari dell'applicazione, file di configurazione e dati degli eventi) nella memorizzazione condivisa. In caso di failover, la memorizzazione viene smontata dal nodo primario e spostata nel nodo di backup, che carica l'intera applicazione e la configurazione

dalla memorizzazione condivisa. Il secondo approccio prevede invece la memorizzazione dei dati degli eventi nella memorizzazione condivisa, mentre i file binari dell'applicazione e i file di configurazione risiedono nel rispettivo nodo del cluster. In caso di failover, viene eseguito lo spostamento nel nodo di backup dei soli dati degli eventi.

Ciascuno di questi due approcci presenta vantaggi e svantaggi, ma il secondo consente di utilizzare i percorsi di installazione standard conformi a FHS, di effettuare la verifica dei pacchetti RPM, di applicare a caldo le patch e di eseguire la riconfigurazione per ridurre al minimo i tempi di fermo.

Questa soluzione illustra una procedura dettagliata mediante un esempio di installazione in un cluster che utilizza la memorizzazione condivisa iSCSI e colloca i file binari dell'applicazione e di configurazione nel rispettivo nodo del cluster.

Monitoraggio dei servizi

Uno dei fattori essenziali di un ambiente ad alta disponibilità è l'utilizzo di un metodo affidabile e coerente per monitorare le risorse che devono avere una disponibilità elevata e le eventuali risorse da cui esse dipendono. SLE HAE utilizza un componente denominato Resource Agent che esegue questo monitoraggio. La funzione di Resource Agent consiste nel comunicare lo stato di ciascuna risorsa e, quando richiesto, nell'avviare e arrestare la risorsa stessa.

Al fine di evitare tempi di fermo non necessari, i componenti Resource Agent devono comunicare lo stato delle risorse monitorate in modo affidabile. I falsi positivi (cioè i casi in cui una risorsa viene giudicata in condizione di guasto ma in realtà è in grado di ripristinarsi autonomamente) possono causare la migrazione non necessaria di servizi (con relativi tempi di fermo), mentre i falsi negativi (cioè i casi in cui Resource Agent segnala che una risorsa è in funzione anche se non sta operando correttamente) possono impedire l'uso corretto del servizio. D'altro canto, il monitoraggio esterno di un servizio può risultare alquanto difficoltoso: la porta di un servizio Web potrebbe rispondere ad un semplice ping, ad esempio, ma non essere in grado di fornire dati corretti in risposta a una vera e propria interrogazione. In molti casi le funzionalità di autodiagnosi devono essere integrate nel servizio stesso affinché forniscano valori precisi.

Questa soluzione integra in Sentinel un Resource Agent di tipo OCF, in grado di monitorare gli errori principali di hardware, sistema operativo o sistema Sentinel. Al momento le funzionalità esterne di monitoraggio per Sentinel sono basate sui controlli delle porte IP ed esiste la possibilità che si verifichino falsi positivi e falsi negativi. Per migliorare la precisione di questo componente è stata pianificata per il futuro l'ottimizzazione sia di Sentinel che del Resource Agent.

Fencing

In un cluster ad alta disponibilità, i servizi critici vengono costantemente monitorati e riavviati automaticamente in altri nodi in caso di errore. Questo tipo di automazione può, però, creare dei problemi, in caso di difficoltà di comunicazione con il nodo primario; nonostante il servizio eseguito nel nodo appaia in stato di errore, in effetti continua a funzionare e a scrivere i dati nella memorizzazione condivisa. In questo caso l'avvio di un nuovo set di servizi in un nodo di backup potrebbe con tutta probabilità danneggiare i dati.

Per evitare che si verifichi questa situazione, i cluster utilizzano numerose tecniche, generalmente definite fencing, fra le quali Split Brain Detection (SBD) e Shoot The Other Node In The Head (STONITH). L'obiettivo principale è quello di evitare il danneggiamento dei dati nella memorizzazione condivisa.

36 Requisiti di sistema

In caso di allocazione di risorse del cluster a supporto di un'installazione ad alta disponibilità, valutare i requisiti seguenti:

- ❒ (Condizionale) Per le installazioni in modalità applicazione ad alta disponibilità, verificare che sia disponibile l'applicazione Sentinel ad alta disponibilità con una licenza valida. L'applicazione Sentinel ad alta disponibilità è un'applicazione ISO che include i pacchetti seguenti:
  - Sistema operativo: SLES 12 SP3
  - Pacchetto SLES High Availability Extension (SLES HAE)
  - Il software Sentinel (incluso l'RPM per l'alta disponibilità)
- ❒ (Condizionale) Per le installazioni tradizionali ad alta disponibilità, verificare che i requisiti seguenti siano stati soddisfatti:
  - Sistema operativo: SLES 11 SP4 o SLES 12 SP1 o versione successiva
  - Immagine ISO di SLES HAE con licenze valide
  - Programma di installazione di Sentinel (file TAR)
- ❒ (Condizionale) Se si utilizza il sistema operativo SLES con il kernel versione 3.0.101 o successive, è necessario caricare manualmente nel computer il driver del processo Watchdog. Per individuare il driver del processo Watchdog appropriato per l'hardware del computer in uso, rivolgersi al fornitore dell'hardware. Per caricare il driver del processo Watchdog, eseguire le operazioni seguenti:
  1. Al prompt dei comandi, eseguire il comando seguente per caricare il driver del processo Watchdog nella sessione attuale:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. Nel file `/etc/init.d/boot.local`, aggiungere la riga seguente affinché il computer carichi automaticamente il driver del processo Watchdog a ogni avvio:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```
- ❒ Accertarsi che i nodi del cluster in cui risiedono i servizi Sentinel siano conformi ai requisiti specificati nel Capitolo 5, “Requisiti di sistema”, a pagina 37.
- ❒ Memorizzazione condivisa sufficiente per i dati di Sentinel e per quelli dell'applicazione.
- ❒ Accertarsi di utilizzare un indirizzo IP virtuale che consenta la migrazione dei servizi da un nodo a un altro in caso di failover.
- ❒ Accertarsi che il dispositivo di memorizzazione condivisa soddisfi i requisiti di prestazioni e dimensioni specificate nel Capitolo 5, “Requisiti di sistema”, a pagina 37. Utilizzare una macchina virtuale SLES standard, configurata con le destinazioni iSCSI come memorizzazione condivisa.

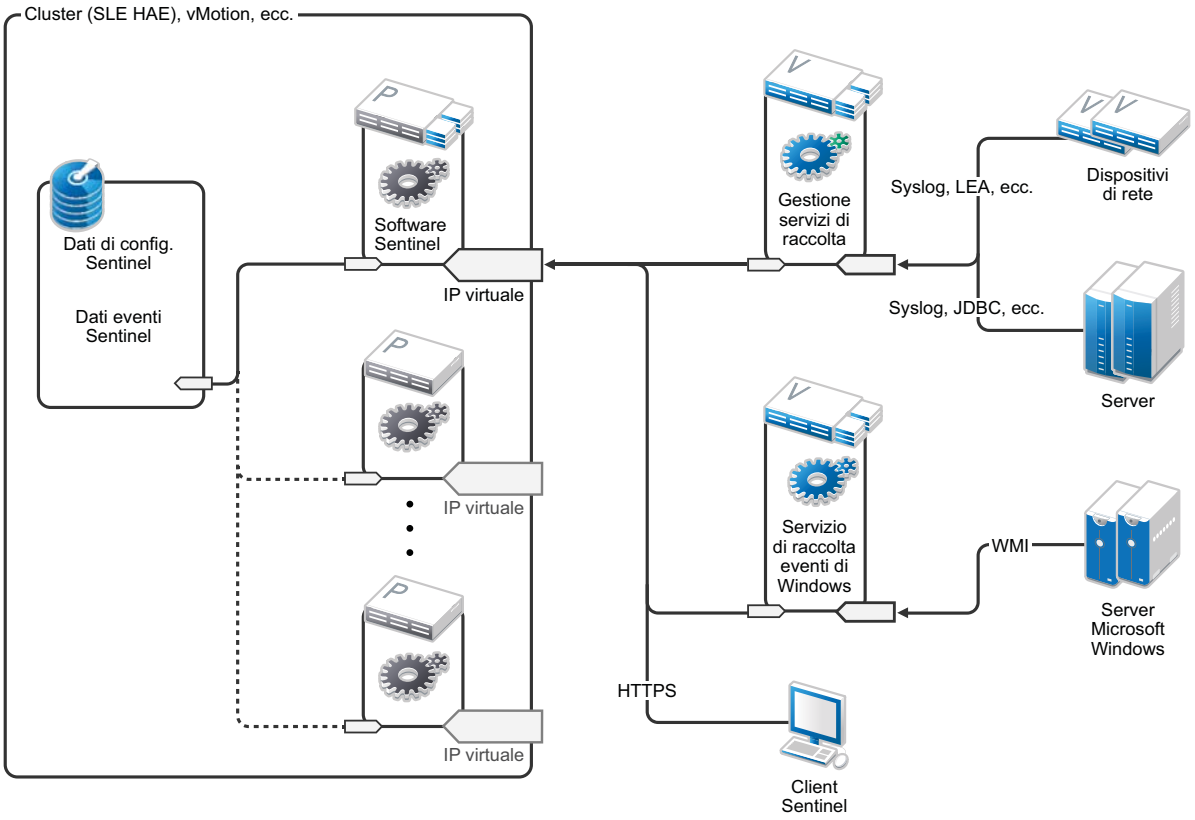
  per iSCSI si deve utilizzare l'unità MTU (Message Transfer Unit) più grande supportata dall'hardware in uso. L'uso di unità MTU di grandi dimensioni migliora le prestazioni di memorizzazione. Nel caso in cui la latenza e la larghezza di banda verso l'unità di memorizzazione siano più lente dei valori consigliati, si potrebbero verificare dei problemi in Sentinel.

- ❒ Accertarsi di disporre di un minimo di due nodi nel cluster che soddisfino i requisiti delle risorse per l'esecuzione di Sentinel nell'ambiente del cliente. È consigliabile utilizzare due macchine virtuali SLES.
- ❒ Accertarsi di aver creato un metodo che consenta ai nodi del cluster di comunicare con la memorizzazione condivisa, ad esempio Fibre Channel per un SAN. Utilizzare un indirizzo IP dedicato per eseguire la connessione alla destinazione iSCSI.
- ❒ Accertarsi di disporre di un indirizzo IP virtuale che consenta la migrazione da un nodo del cluster a un altro da utilizzare come indirizzo IP esterno per Sentinel.
- ❒ Accertarsi di disporre di almeno un indirizzo IP per nodo del cluster da utilizzare per le comunicazioni all'interno del cluster stesso. È possibile utilizzare un semplice indirizzo IP unicast, ma per gli ambienti di produzione è preferibile il multicast.

37 Installazione e configurazione

In questo capitolo è illustrata la procedura di installazione e configurazione di Sentinel in un ambiente ad alta disponibilità.

Nello schema seguente è rappresentata un'architettura ad alta disponibilità attiva-passiva.



Configurazione iniziale

Configurare l'hardware di computer, rete e memorizzazione, i sistemi operativi, gli account utente e altre risorse di base del sistema in funzione dei requisiti specificati per Sentinel e di quelli locali del cliente. Sottoporre i sistemi a prova per verificare che funzionino correttamente e siano stabili.

Per la configurazione e l'impostazione iniziale utilizzare l'elenco di controllo seguente.

	Voci dell'elenco di controllo
❑	Le caratteristiche di CPU, RAM e spazio su disco di ciascun nodo del cluster devono essere conformi ai requisiti di sistema indicati nel Capitolo 5, “Requisiti di sistema”, a pagina 37 e basati sulla frequenza eventi prevista.
❑	Le caratteristiche di spazio su disco e I/O per i nodi di memorizzazione devono essere conformi ai requisiti di sistema indicati nel Capitolo 5, “Requisiti di sistema”, a pagina 37 e basati sulla frequenza eventi prevista e sulle policy di conservazione dei dati per la memorizzazione primaria e/o secondaria.
❑	Se si desidera configurare i firewall del sistema operativo affinché limitino l'accesso a Sentinel e al cluster, vedere il Capitolo 8, “Porte utilizzate”, a pagina 63, in cui sono riportati i dettagli relativi alle porte che devono essere disponibili a seconda della configurazione locale e delle origini che invieranno i dati degli eventi.
❑	Accertarsi che l'orario di tutti i nodi del cluster sia sincronizzato. A tale scopo è possibile utilizzare NTP o una tecnologia analoga.
❑	◆ Per il cluster è necessario che la risoluzione dei nomi host sia affidabile. Per garantire la continuità del cluster in caso di errore DNS, immettere tutti i nomi degli host all'interno del cluster nel file `/etc/hosts`. ◆ Accertarsi di non aver assegnato un nome host a un indirizzo IP di loopback. ◆ Quando si configurano il nome host e il nome di dominio durante l'installazione del sistema operativo, deselezionare **Assegnare il nome host all'IP di loopback**.

È possibile utilizzare la configurazione seguente:

- (Condizionale) Per le installazioni tradizionali ad alta disponibilità:
  - Due macchine virtuali nodo cluster con SLES 11 SP4 o SLES 12 SP1 o versione successiva.
  - (Condizionale) Se è necessario configurare l'interfaccia grafica, è possibile installare X Windows. Impostare gli script di avvio in modo che si avviino senza X (livello di esecuzione 3), affinché sia possibile avviarli solo quando necessario.
- (Condizionale) Per installazioni in modalità applicazione ad alta disponibilità: due macchine virtuali basate sull'applicazione ISO ad alta disponibilità nel nodo del cluster. Per informazioni sull'installazione in modalità applicazione ISO ad alta disponibilità, vedere la “Installazione di Sentinel” a pagina 102.
- I nodi utilizzeranno una NIC per l'accesso esterno e una per le comunicazioni iSCSI.
- Configurare le NIC esterne con indirizzi IP che consentano l'accesso in remoto mediante il protocollo SSH o simili. In questo esempio sono stati utilizzati gli indirizzi 172.16.0.1 (node01) e 172.16.0.2 (node02).
- Ciascun nodo deve disporre di uno spazio su disco sufficiente per il sistema operativo, i file binari e di configurazione di Sentinel, il software del cluster, i file temporanei e così via. Vedere i requisiti di sistema di SLES e SLE HAE, nonché i requisiti dell'applicazione Sentinel.

- Una macchina virtuale SLES 11 SP4 o SLES 12 SP1 o versione successiva configurata con iSCSI Targets per la memorizzazione condivisa
  - (Condizionale) Se è necessario configurare l'interfaccia grafica, è possibile installare X Windows. Impostare gli script di avvio in modo che si avviino senza X (livello di esecuzione 3), affinché sia possibile avviarli solo quando necessario.
  - Il sistema utilizzerà due NIC, una per l'accesso esterno e una per le comunicazioni iSCSI.
  - Configurare la NIC esterna con un indirizzo IP che consenta l'accesso remoto mediante il protocollo SSH o simili. Ad esempio, 172.16.0.3 (memorizzazione 03).
  - Il sistema deve disporre di uno spazio sufficiente su disco per il sistema operativo, i file temporanei, un volume di grande dimensioni per la memorizzazione condivisa dei dati di Sentinel e uno spazio limitato per una partizione SBD. Vedere i requisiti di sistema di SLES, nonché i requisiti per la memorizzazione dei dati degli eventi di Sentinel.

Nota: per le comunicazioni all'interno di un cluster di produzione è possibile utilizzare IP interni non instradabili in NIC separate (possibilmente un paio per la ridondanza).

Configurazione della memorizzazione condivisa

Configurare la memorizzazione condivisa e verificare che sia possibile montarla in ciascun nodo del cluster. Se si utilizza Fibre Channel e un SAN, potrebbe essere necessario predisporre dei collegamenti fisici ed effettuare ulteriori operazioni di configurazione. Sentinel utilizza la memorizzazione condivisa per i database e i dati degli eventi. Verificare che la memorizzazione condivisa sia di dimensioni appropriate in base alla frequenza eventi prevista e alle policy di permanenza dei dati.

Si consideri il seguente esempio di configurazione della memorizzazione condivisa:

Un'implementazione tipica potrebbe includere un SAN veloce collegato mediante Fibre Channel a tutti i nodi del cluster e un RAID di grande capacità per la memorizzazione dei dati locali degli eventi. Per la memorizzazione secondaria più lenta si potrebbe utilizzare un nodo NAS o iSCSI separato. Se il nodo del cluster consente di montare la memorizzazione primaria come dispositivo di blocco normale, è possibile utilizzarlo per la soluzione. La memorizzazione secondaria può essere montata anche come dispositivo di blocco, oppure può essere un volume NFS o CIFS.

Nota: configurare la memorizzazione condivisa e provarla montandola in ciascun nodo del cluster. Tuttavia, sarà la configurazione del cluster a gestire il montaggio vero e proprio della memorizzazione.

Per creare le destinazioni iSCSI residenti in una macchina virtuale SLES, effettuare le operazioni seguenti:

1. Eseguire la connessione a `storage03`, vale a dire la macchina virtuale creata durante la Configurazione iniziale, e avviare una sessione della console.
2. Per creare un file vuoto dalle dimensioni desiderate per la memorizzazione primaria di Sentinel, eseguire il comando seguente:

   `dd if=/dev/zero of=/localdata count=<dimensione file> bs=<dimensione bit>`

   Ad esempio, per creare un file di 20 GB contenente gli zeri copiati dallo pseudo dispositivo `/dev/zero`, eseguire il comando seguente:

   ```
   dd if=/dev/zero of=/localdata count=20480000 bs=1024
   ```
3. Ripetere i passaggi 1 e 2 per creare allo stesso modo un file per la memorizzazione secondaria.

Ad esempio, eseguire il comando seguente per la memorizzazione secondaria:

```
dd if=/dev/zero of=/networkdata count=20480000 bs=1024
```

Nota: in questo esempio sono stati creati due file delle stesse dimensioni e caratteristiche prestazionali che rappresentano due dischi. Per l'installazione in un ambiente di produzione, la memorizzazione primaria può essere creata in un SAN veloce, mentre quella secondaria in un volume iSCSI, NFS o CIFS più lento.

Per configurare i dispositivi iniziatore e destinazione iSCSI, effettuare i passaggi descritti nelle sezioni seguenti:

- “Configurazione delle destinazioni iSCSI” a pagina 196
- “Configurazione degli iniziatori iSCSI” a pagina 198

Configurazione delle destinazioni iSCSI

Per configurare i file `localdata` e `networkdata` come destinazioni iSCSI, eseguire la procedura seguente.

Per ulteriori informazioni sulla configurazione delle destinazioni iSCSI, vedere Creating iSCSI Targets with YaST (Creazione di destinazioni iSCSI con YaST) nella documentazione di SUSE.

1. Eseguire YaST dalla riga di comando (o utilizzare l'interfaccia grafica utente): `/sbin/yast`
2. Selezionare **Dispositivi di rete** > **Impostazioni di rete**.
3. Verificare che la scheda **Panoramica** sia selezionata.
4. Selezionare la NIC secondaria nell'elenco visualizzato e spostarsi con il tasto TAB su Modifica, quindi premere `Invio`.
5. Nella scheda **Address** (Indirizzo), assegnare l'indirizzo IP statico 10.0.0.3, che sarà l'indirizzo IP per le comunicazioni iSCSI interne.
6. Fare clic su **Avanti** e successivamente su **OK**.
7. (Condizionale) Nella schermata principale:
   - Se si utilizza SLES 11 SP4, selezionare **Network Services** (Servizi di rete) > **iSCSI Target** (Destinazione iSCSI).
   - Se si utilizza SLES 12 SP1 o versione successiva, selezionare **Servizi di rete** > **iSCSI LIO Target**.

   Nota: se non è possibile trovare l'opzione, scegliere **Software** > **Software Management** (Gestione software) > **iSCSI LIO Server** (Server iSCSI LIO) e installare il pacchetto iSCSI LIO.

   ---
8. (Condizionale) Se richiesto, installare il software necessario:
   - Per SLES 11 SP4: `iscsitarget RPM`
   - Per SLES 12 SP1 o versione successiva: `iscsiliotarget RPM`
9. (Condizionale) Se si utilizza SLES 12 SP1 o versione successiva, effettuare i seguenti passaggi su tutti i nodi del cluster:
   - **9a** Eseguire il comando seguente per aprire il file contenente il nome dell'iniziatore iSCSI:

     ```
     cat /etc/iscsi/initiatorname.iscsi
     ```
   - **9b** Prendere nota del nome dell'iniziatore per utilizzarlo durante la configurazione degli iniziatori iSCSI:

Ad esempio:

```
InitiatorName=iqn.1996-04.de.suse:01:441d6988994
```

I nomi degli iniziatori verranno utilizzati durante la configurazione di iSCSI Target Client Setup.

10 Fare clic su **Servizio** e selezionare l'opzione **In avvio** affinché il servizio venga avviato quando si avvia il sistema operativo.

11 Selezionare la scheda **Global** (Globale), deselezionare **No Authentication** (Nessuna autenticazione) per abilitare l'autenticazione, quindi specificare le credenziali necessarie per l'autenticazione in entrata e in uscita.

L'opzione **No Authentication** (Nessuna autenticazione) è abilitata per default. Tuttavia, è necessario abilitare l'autenticazione affinché la configurazione sia sicura.

12 Fare clic su **Destinazioni** e successivamente su **Aggiungi** per aggiungere una nuova destinazione.

La destinazione iSCSI genererà automaticamente un ID e visualizzerà un elenco vuoto di LUN (unità) disponibili.

13 Fare clic su **Aggiungi** per aggiungere un nuovo LUN.

14 Non modificare il numero 0 dei LUN, spostarsi nella finestra di dialogo **Percorso** (in Tipo=fileio) e selezionare il file `/localdata` precedentemente creato. Se per la memorizzazione si utilizza un disco dedicato, specificare un dispositivo di blocco, ad esempio `/dev/sdc`.

15 Ripetere i passaggi 13 e 14, ma questa volta aggiungere LUN 1 e selezionare `/networkdata`.

16 (Condizionale) Se si utilizza SLES 11 SP4, effettuare i passaggi seguenti:

16a Non modificare i valori di default delle altre opzioni, fare clic su **OK** e successivamente su **Next** (Avanti).

16b (Condizionale) Se al passaggio 11 è stata abilitata l'autenticazione, fornire le credenziali di autenticazione.

Selezionare un client, scegliere **Edit Auth** (Modifica·autenticazione) > **Incoming Authentication** (Autenticazione in entrata) e specificare il nome utente e la password.

17 (Condizionale) Se si utilizza SLES 12 SP1 o versione successive, effettuare i seguenti passaggi:

17a Lasciare le altre opzioni ai valori di default e fare clic su **Next** (Avanti).

17b Fare clic su **Aggiungi**. Quando viene richiesto il nome del client, specificare il nome dell'iniziatore copiato al passaggio 9. Ripetere questo passaggio per aggiungere tutti i nomi dei client, specificando i nomi degli iniziatori.

In Client List (Elenco client) verrà visualizzato l'elenco dei nomi dei client.

17c (Condizionale) Se al passaggio 11 è stata abilitata l'autenticazione, fornire le credenziali di autenticazione.

Selezionare un client, scegliere **Edit Auth** (Modifica autenticazione) > **Incoming Authentication** (Autenticazione in entrata) e specificare il nome utente e la password. Ripetere l'operazione per tutti i client.

18 Fare nuovamente clic su **Avanti** per selezionare le opzioni di autenticazione di default e successivamente su **Fine** per uscire dalla configurazione. Se richiesto, accettare il riavvio di iSCSI.

19 Uscire da YaST.

Nota: mediante la procedura vengono esposte due destinazioni iSCSI nel server all'indirizzo IP 10.0.0.3. Verificare in ciascun nodo del cluster che sia possibile montare il dispositivo di memorizzazione condivisa per i dati locali.

Configurazione degli iniziatori iSCSI

Per formattare i dispositivi degli iniziatori iSCSI, eseguire la procedura seguente.

Per ulteriori informazioni sulla configurazione degli iniziatori iSCSI, vedere Configuring the iSCSI Initiator (Configurazione dell'iniziatore iSCSI) nella documentazione di SUSE.

1. Eseguire la connessione a un nodo del cluster (node01) e avviare YaST.
2. Selezionare **Dispositivi di rete** > **Impostazioni di rete**.
3. Verificare che la scheda **Panoramica** sia selezionata.
4. Selezionare la NIC secondaria nell'elenco visualizzato e spostarsi con il tasto TAB su Modifica, quindi premere Invio.
5. Fare clic su **Address** (Indirizzo) e assegnare l'indirizzo IP statico 10.0.0.1, che sarà l'indirizzo IP utilizzato per le comunicazioni iSCSI interne.
6. Fare clic su **Avanti** e successivamente su **OK**.
7. Fare clic su **Servizi di rete** > **Iniziatore iSCSI**.
8. Se richiesto, installare il software necessario (RPM `iscsiclient`).
9. Fare clic su **Servizio** e selezionare **In avvio** affinché il servizio iSCSI venga avviato in fase di avvio.
10. Fare clic su **Destinazioni rilevate** e selezionare **Rilevazione**.
11. Specificare l'indirizzo IP della destinazione iSCSI (10.0.0.3).

    (Condizionale) Se al passaggio 11 della “Configurazione delle destinazioni iSCSI” a pagina 196 è stata abilitata l'autenticazione, deselezionare **No Authentication** (Nessuna autenticazione). Nel campo **Outgoing Authentication** (Autenticazione in uscita), digitare il nome utente e la password specificati durante la configurazione delle destinazioni iSCSI.

    Fare clic su **Avanti**.
12. Selezionare la destinazione iSCSI rilevata con indirizzo IP 10.0.0.3 e successivamente **Login**.
13. eseguire i passaggi seguenti:

    13a Passare alla modalità automatica nel menu a discesa **Startup** (Avvio).

    13b (Condizionale) Se è stata abilitata l'autenticazione, deselezionare **No Authentication** (Nessuna autenticazione).

    Il nome utente e la password specificati al passaggio 11 dovrebbero apparire nella sezione **Outgoing Authentication** (Autenticazione in uscita). Se le credenziali non vengono visualizzate, immetterle in questa sezione.

    13c Fare clic su **Avanti**.
14. Passare alla scheda **Destinazioni connesse** per verificare la connessione alla destinazione.
15. Uscire dalla configurazione. Eseguendo questa procedura le destinazioni iSCSI vengono montate come dispositivi di blocco nel nodo del cluster.
16. Nel menu principale di YaST, selezionare **Sistema** > **Partizionatore**.
17. In System View (Vista di sistema) dovrebbero apparire nell'elenco i nuovi dischi rigidi dei tipi seguenti (ad esempio `/dev/sdb` e `/dev/sdc`):
    - In SLES 11 SP4: IET-VIRTUAL-DISK
    - In SLES 12 SP1 o versione successiva: LIO-ORG-FILEIO

    Spostarsi con il tasto TAB sulla prima voce dell'elenco (che dovrebbe essere la memorizzazione primaria), selezionare il disco e premere Invio.

18 Selezionare **Aggiungi** per aggiungere una nuova partizione nel disco vuoto. Formattare il disco come partizione primaria, ma non montarlo. Verificare che l'opzione **Do not mount partition** (Non montare la partizione) sia selezionata.

19 Selezionare **Next** (Avanti) e, dopo aver verificato le modifiche che verranno apportate, fare clic su **Finish** (Fine).

Il disco formattato (ad esempio `/dev/sdb1`) dovrebbe essere pronto. Nei passaggi seguenti della procedura è definito `/dev/<SHARED1>`.

20 Tornare a **Partitioner** (Partizionatore) e ripetere la procedura di creazione delle partizioni/formattazione (passaggi da 16 a 19) per `/dev/sdc` o qualsiasi altro dispositivo di blocco utilizzato per la memorizzazione secondaria. Si dovrebbe così ottenere una partizione `/dev/sdc1` o un disco formattato simile (di seguito definito `/dev/<NETWORK1>`).

21 Uscire da YaST.

22 (Condizionale) Se si esegue un'installazione tradizionale ad alta disponibilità, creare un punto di montaggio e provare il montaggio della partizione locale come segue (il nome esatto del dispositivo potrebbe variare a seconda dell'implementazione specifica):

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

Deve essere possibile creare dei file nella nuova partizione e vederli nell'ubicazione in cui la partizione è stata montata.

23 (Condizionale) Se si esegue un'installazione tradizionale ad alta disponibilità, per lo smontaggio:

```
# umount /var/opt/novell
```

24 (Condizionale) Per le installazioni in modalità applicazione ad alta disponibilità, ripetere i passaggi da 1 a 15 per verificare che in ciascun nodo del cluster sia possibile montare la memorizzazione condivisa locale. Al passaggio 5 sostituire l'indirizzo IP del nodo con un diverso indirizzo IP per ciascun nodo del cluster.

25 (Condizionale) Per le installazioni tradizionali ad alta disponibilità, ripetere i passaggi da 1 a 15, 22 e 23 al fine di verificare che in ciascun nodo del cluster sia possibile montare la memorizzazione condivisa locale. Al passaggio 6 sostituire l'indirizzo IP del nodo con un diverso indirizzo IP per ciascun nodo del cluster.

Installazione di Sentinel

Per installare Sentinel è possibile utilizzare due metodi: installazione di tutti i componenti nella memorizzazione condivisa (utilizzando l'opzione `--location` per ridirigere l'installazione di Sentinel nell'ubicazione in cui è stata montata la memorizzazione condivisa) oppure installazione dei soli dati variabili dell'applicazione nella memorizzazione condivisa.

Installare Sentinel in ciascun nodo del cluster in cui l'applicazione può risiedere. Dopo aver installato Sentinel per la prima volta, è necessario eseguire un'installazione completa che includa i file binari dell'applicazione, i file di configurazione e i database. Per le installazioni successive in altri nodi del cluster, è necessario installare solo l'applicazione. I dati di Sentinel saranno disponibili dopo il montaggio della memorizzazione condivisa.

Installazione nel primo nodo

- “Installazione tradizionale ad alta disponibilità” a pagina 200
- “Installazione dell'applicazione Sentinel ad alta disponibilità” a pagina 200

Installazione tradizionale ad alta disponibilità

1. Eseguire la connessione a un nodo del cluster (node01) e aprire una finestra della console.
2. Effettuare il download del programma di installazione di Sentinel (file tar.gz) e memorizzarlo in `/tmp` nel nodo del cluster.
3. Per iniziare l'installazione, effettuare i passaggi seguenti:
   - **3a** Eseguire i seguenti comandi:

     ```
     mount /dev/<SHARED1> /var/opt/novell
     cd /tmp
     tar -xvzf sentinel_server*.tar.gz
     cd sentinel_server*
     ./install-sentinel --record-unattended=/tmp/install.props
     ```
   - **3b** Quando viene richiesto di selezionare il metodo di configurazione, specificare `2` per selezionare Configurazione personalizzata.
4. Eseguire l'installazione configurando il prodotto secondo necessità.
5. Avviare Sentinel e provare le funzioni di base. Per accedere al prodotto è possibile utilizzare l'indirizzo IP standard esterno del nodo cluster.
6. Chiudere Sentinel e smontare la memorizzazione condivisa utilizzando i comandi seguenti:

   ```
   rcsentinel stop
   umount /var/opt/novell
   ```

   Con questa operazione si rimuovono gli script di avvio automatico, affinché il cluster possa gestire il prodotto.

   ```
   cd /
   insserv -r sentinel
   ```

Installazione dell'applicazione Sentinel ad alta disponibilità

L'applicazione Sentinel ad alta disponibilità include il software Sentinel già installato e configurato. Per configurare il software Sentinel per l'alta disponibilità, utilizzare la procedura seguente:

1. Eseguire la connessione a un nodo del cluster (node01) e aprire una finestra della console.
2. Accedere alla seguente directory:

   ```
   cd /opt/novell/sentinel/setup
   ```
3. Registrare la configurazione:
   - **3a** Eseguire il comando seguente:

     ```
     ./configure.sh --record-unattended=/tmp/install.props --no-start
     ```

     Mediante questa operazione la configurazione viene registrata nel file `install.props`, necessario per configurare le risorse del cluster mediante lo script `install-resources.sh`.
   - **3b** Quando viene richiesto di selezionare il metodo di configurazione, specificare `2` per selezionare Configurazione personalizzata.
   - **3c** Quando viene richiesta la password, specificare `2` per immettere una nuova password.

     Se si specifica `1`, la password non viene memorizzata nel file `install.props`.

4 Chiudere Sentinel utilizzando il comando seguente:

```
rcsentinel stop
```

Con questa operazione si rimuovono gli script di avvio automatico, affinché il cluster possa gestire il prodotto.

```
insserv -r sentinel
```

5 Spostare la cartella dei dati di Sentinel nella memorizzazione condivisa utilizzando i comandi seguenti. Grazie a questo spostamento i nodi potranno utilizzare la cartella dei dati di Sentinel mediante la memorizzazione condivisa.

```
mkdir -p /tmp/new

mount /dev/<SHARED1> /tmp/new

mv /var/opt/novell/* /tmp/new

umount /tmp/new/
```

6 Verificare che la cartella dei dati di Sentinel sia stata spostata nella memorizzazione condivisa utilizzando i comandi seguenti:

```
mount /dev/<SHARED1>  /var/opt/novell/

umount /var/opt/novell/
```

Installazione in nodi successivi

- “Installazione tradizionale ad alta disponibilità” a pagina 201
- “Installazione dell'applicazione Sentinel ad alta disponibilità” a pagina 202

Ripetere l'istallazione negli altri nodi:

Il programma di installazione iniziale di Sentinel crea un account utente a disposizione del prodotto, che utilizza l'ID utente successivo disponibile al momento dell'istallazione. Le installazioni successive in modalità automatica avverranno tentando di utilizzare il medesimo ID utente per la creazione degli account, ma esiste la possibilità che si generino conflitti (se i nodi del cluster non sono identici al momento dell'istallazione). Si consiglia di eseguire una delle operazioni seguenti:

- Sincronizzare il database degli account utente in tutti i nodi del cluster (manualmente, tramite LDAP o simili), verificando che la sincronizzazione venga eseguita prima delle installazioni successive. In questo caso il programma di installazione rileverà la presenza dell'account utente e utilizzerà quello esistente.
- Monitorare il risultato delle installazioni successive in modalità automatica; se non è possibile creare l'account utente con lo stesso ID utente verrà generato un avviso.

Installazione tradizionale ad alta disponibilità

1 Eseguire la connessione a ciascun nodo aggiuntivo (node02) del cluster e aprire una finestra della console.

2 Eseguire i seguenti comandi:

```
cd /tmp

scp root@node01:/tmp/sentinel_server*.tar.gz .

scp root@node01:/tmp/install.props .
```

```
tar -xvzf sentinel_server*.tar.gz

cd sentinel_server*

./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props

insserv -r sentinel
```

Installazione dell'applicazione Sentinel ad alta disponibilità

1. Eseguire la connessione a ciascun nodo aggiuntivo (node02) del cluster e aprire una finestra della console.
2. Eseguire il comando seguente:

   ```
   insserv -r sentinel
   ```

3. Interrompere i servizi Sentinel.

   ```
   rcsentinel stop
   ```

4. Rimuovere la directory Sentinel.

   ```
   rm -rf /var/opt/novell/*
   ```

Al termine della procedura Sentinel dovrebbe essere installato in tutti i nodi, ma è probabile che funzioni correttamente soltanto nel primo nodo fino a quando non verrà eseguita la sincronizzazione di varie chiavi durante la configurazione delle risorse del cluster.

Installazione del cluster

È necessario installare il software del cluster solo in caso di installazioni tradizionali ad alta disponibilità. L'applicazione Sentinel ad alta disponibilità include il software del cluster e non richiede un'installazione manuale.

Per configurare SLES High Availability Extension con un overlay di agenti risorse specifici di Sentinel, utilizzare la procedura seguente:

1. Installare il software del cluster in ciascun nodo.
2. Registrare ciascun nodo nel cluster manager.
3. Verificare che ciascun nodo appaia nella console di gestione del cluster.

   Nota: Il Resource Agent OCF di Sentinel è un semplice script di shell che esegue una vasta gamma di controlli per verificare che Sentinel funzioni correttamente. Se per il monitoraggio di Sentinel non si utilizza il Resource Agent OCF, è necessario sviluppare una soluzione di monitoraggio analoga per l'ambiente cluster locale. Per sviluppare la propria soluzione, esaminare il Resource Agent esistente memorizzato nel file `Sentinelha.rpm` nel pacchetto di download di Sentinel.

   ---

4. Installare il software principale SLE HAE come indicato nella documentazione di SLE HAE.Per informazioni sull'installazione dei componenti aggiuntivi di SLES, vedere la Guida per la distribuzione.
5. Ripetere il passaggio 4 su tutti i nodi del cluster. Il componente aggiuntivo installerà il software principale per la gestione del cluster e le comunicazioni, nonché vari Resource Agent utilizzati per monitorare le risorse del cluster.

6. Installare un RPM aggiuntivo per rendere disponibili i Resource Agent aggiuntivi specifici di Sentinel per il cluster. L'RPM per l'alta disponibilità è disponibile nel file `novell-Sentinelha-<versione_Sentinel>*.rpm`, incluso nel download di default di Sentinel, che è stato decompresso per installare il prodotto.
7. Copiare il file `novell-Sentinelha-<versione_Sentinel>*.rpm` nella directory `/tmp` di ciascun nodo del cluster, quindi eseguire i comandi seguenti:

```
cd /tmp
```

```
rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

Configurazione del cluster

Per registrare ciascun nodo come membro del cluster, è necessario configurare il software del cluster. Nell'ambito di questa configurazione, per garantire la coerenza del cluster è inoltre possibile impostare risorse di fencing e STONITH (Shoot The Other Node In The Head).

Importante: Nella procedura descritta in questa sezione vengono utilizzati i comandi `rcopenais` e `openais`, compatibili soltanto con SLES 11 SP4. Per SLES 12 SP2 e versioni successive, utilizzare il comando `systemctl pacemaker.service`.

Ad esempio, nel caso del comando `/etc/rc.d/openais start`, utilizzare il comando `systemctl start pacemaker.service`.

Per la configurazione del cluster, utilizzare la procedura seguente:

Per questa soluzione è necessario utilizzare indirizzi IP privati per le comunicazioni all'interno del cluster e la modalità unicast per evitare di richiedere un indirizzo multicast all'amministratore di rete. Inoltre, è necessario utilizzare una destinazione iSCSI configurata nella stessa macchina virtuale SLES in cui risiede la memorizzazione condivisa e che funge da dispositivo SBD (Split Brain Detection) per il fencing.

Configurazione di SBD

1. Eseguire la connessione a `storage03` e avviare una sessione della console. Per creare un file vuoto delle dimensioni desiderate, eseguire il comando seguente:

   ```
   dd if=/dev/zero of=/sbd count=<dimensione file> bs=<dimensione bit>
   ```

   Ad esempio, per creare un file di 1 MB contenente gli zeri copiati dallo pseudo dispositivo `/dev/zero`, eseguire il comando seguente:

   ```
   dd if=/dev/zero of=/sbd count=1024 bs=1024
   ```

2. Eseguire YaST dalla riga di comando o l'interfaccia grafica: `/sbin/yast`
3. Selezionare **Servizi di rete** > **Destinazione iSCSI**.
4. Fare clic su **Destinazioni** e selezionare la destinazione esistente.
5. Selezionare **Modifica**. L'interfaccia utente visualizzerà un elenco di LUN (unità) disponibili.
6. Selezionare **Aggiungi** per aggiungere un nuovo LUN.
7. Non modificare il numero 2 dei LUN. Spostarsi nella finestra di dialogo **Percorso** e selezionare il file `/sbd` che è stato creato.

8 Non modificare le impostazioni di default delle altre opzioni, selezionare **OK** e successivamente **Avanti**, quindi fare nuovamente clic su **Avanti** per selezionare le opzioni di autenticazione di default.

9 Per uscire dalla configurazione, fare clic su **Fine**. Se necessario, riavviare il servizio. Uscire da YaST.

Nota: per eseguire le operazioni seguenti è necessario che ciascun nodo del cluster sia in grado di risolvere il nome host di tutti gli altri nodi del cluster (in caso contrario il servizio di sincronizzazione file csync2 non potrà essere eseguito). Se il DNS non è stato configurato o non è disponibile, aggiungere le voci per ciascun host nel file `/etc/hosts` in cui sono elencati gli indirizzi IP e i relativi nomi host (come segnalato dal comando hostname). Verificare inoltre di non aver assegnato un nome host a un indirizzo IP di loopback.

Eseguire la procedura seguente per esporre una destinazione iSCSI per il dispositivo SBD nel server all'indirizzo IP 10.0.0.3 (storage03).

Configurazione del nodo

Eseguire la connessione a un nodo del cluster (node01) e aprire una finestra della console:

1 Esegui YaST.

2 Aprire **Servizi di rete** > **Iniziatore iSCSI**.

3 Selezionare **Destinazioni connesse** e successivamente la destinazione iSCSI precedentemente configurata.

4 Selezionare l'opzione **Logout** per eseguire il logout dalla destinazione.

5 Passare alla scheda **Discovered Targets** (Destinazioni rilevate), selezionare la **destinazione** e ripetere il login per aggiornare l'elenco dei dispositivi (lasciare l'opzione di avvio impostata su **Automatic** (Automatico) e deselezionare **No Authentication** (Nessuna autenticazione)).

6 Selezionare **OK** e uscire dallo strumento per l'iniziatore iSCSI.

7 Aprire **Sistema** > **Partizionatore** e individuare il dispositivo SBD definito come 1MB IET-VIRTUAL-DISK. Comparirà nell'elenco come **/dev/sdd** o simile. Annotare la voce usata.

8 Uscire da YaST.

9 Eseguire il comando `ls -l /dev/disk/by-id/` e annotare l'ID del dispositivo collegato al nome del dispositivo precedentemente individuato.

10 (Condizionale) Eseguire uno dei comandi seguenti:

- Se si utilizza SLES 11 SP4:

  ```
  sleha-init
  ```

- Se si utilizza SLES 12 SP1 o versione successiva:

  ```
  ha-cluster-init
  ```

11 Quando viene richiesto l'indirizzo di rete per l'associazione, specificare l'indirizzo IP esterno della NIC (172.16.0.1).

12 Accettare l'indirizzo multicast e la porta di default. La sostituzione verrà effettuata successivamente.

13 Immettere `y` per abilitare SBD, quindi specificare `/dev/disk/by-id/<id dispositivo>`, in cui `<id dispositivo>` è l'ID del dispositivo precedentemente individuato (per completare automaticamente il percorso utilizzare il tasto Tab).

14 (Condizionale) Durante l'operazione seguente immettere `N` quando richiesto:

```
Do you wish to configure an administration IP? [y/N]
```

Per configurare un indirizzo IP di amministrazione, specificare l'indirizzo IP virtuale durante le operazioni descritte in “Configurazione delle risorse” a pagina 206.

15 Completare la procedura guidata e verificare che non vengano segnalati errori.

16 Avviare YaST.

17 Selezionare **Elevata disponibilità** > **Cluster** (o solo Cluster in alcuni sistemi).

18 Nella casella sulla sinistra, verificare che l'opzione **Canali di comunicazione** sia selezionata.

19 Spostarsi con il tasto TAB sulla prima riga della configurazione e modificare **udp** impostando **udpu** (in questo modo si disabilita la modalità multicast e si seleziona quella unicast).

20 Selezionare **Aggiungi l'indirizzo di un membro** e specificare il nodo (172.16.0.1), quindi ripetere l'operazione e aggiungere gli altri nodi del cluster (172.16.0.2).

21 Per completare la configurazione, selezionare **Fine**.

22 Uscire da YaST.

23 Eseguire il comando /etc/rc.d/openais per riavviare i servizi del cluster con il nuovo protocollo di sincronizzazione.

Eseguire la connessione a ciascun nodo aggiuntivo (node02) e aprire una finestra della console:

1 Esegui YaST.

2 Aprire **Servizi di rete** > **Iniziatore iSCSI**.

3 Selezionare **Destinazioni connesse** e successivamente la destinazione iSCSI precedentemente configurata.

4 Selezionare l'opzione **Logout** per eseguire il logout dalla destinazione.

5 Passare alla scheda **Discovered Targets** (Destinazioni rilevate), selezionare la **destinazione** e ripetere il login per aggiornare l'elenco dei dispositivi (lasciare l'opzione di avvio impostata su **Automatic** (Automatico) e deselezionare **No Authentication** (Nessuna autenticazione)).

6 Selezionare **OK** e uscire dallo strumento per l'iniziatore iSCSI.

7 (Condizionale) Eseguire uno dei comandi seguenti:

- Se si utilizza SLES 11 SP4:

  ```
  sleha-join
  ```

- Se si utilizza SLES 12 SP1 o versione successiva:

  ```
  ha-cluster-join
  ```

8 Immettere l'indirizzo IP del primo nodo del cluster.

(Condizionale) Se il cluster non si avvia correttamente, eseguire le operazioni seguenti:

1 Eseguire il comando `crm status` per verificare se i nodi sono stati uniti. Se l'unione non è stata eseguita, riavviare tutti i nodi del cluster.

2 Copiare manualmente il file `/etc/corosync/corosync.conf` da `node01` a `node02` o eseguire `csync2 -x -v` in `node01`, oppure configurare manualmente il cluster in `node02` mediante YaST.

3 (Condizionale) Se il comando `csync2 -x -v` eseguito al passaggio 1 non ha sincronizzato tutti i file, effettuare le operazioni seguenti:

3a Cancellare il database csync2 nella directory `/var/lib/csync2` in tutti i nodi.

3b In tutti i nodi, aggiornare il database csync2 affinché corrisponda al file system, ma senza contrassegnare nulla come elemento da sincronizzare con altri server:

```
csync2 -cIr /
```

3c Nel nodo attivo, eseguire le operazioni seguenti:

3c1 Trovare tutte le differenze tra i nodi attivi e passivi, quindi contrassegnare tali differenze per la sincronizzazione:

```
csync2 -TUXI
```

3c2 Reimpostare il database per forzare il nodo attivo a ignorare eventuali conflitti:

```
csync2 -fr /
```

3c3 Avviare la sincronizzazione con tutti gli altri nodi:

```
csync2 -xr /
```

3d In tutti i nodi, verificare che tutti i file siano sincronizzati:

```
csync2 -T
```

Con questo comando vengono elencati solo i file che non sono sincronizzati.

4 Eseguire il comando seguente in `node02`:

Per SLES 11 SP4:

```
/etc/rc.d/openais start
```

Per SLES 12 SP1 e versione successiva:

```
systemctl start pacemaker.service
```

(Condizionale) Se il servizio `xinetd` non aggiunge correttamente il nuovo servizio `csync2`, lo script non funzionerà correttamente. Il servizio `xinetd` è necessario affinché l'altro nodo possa eseguire la sincronizzazione dei file di configurazione del cluster fino a questo nodo. Se si rilevano errori del tipo `csync2 run failed`, potrebbe essersi verificato questo problema.

Per risolvere il problema, eseguire il comando `kill -HUP `cat /var/run/xinetd.init.pid` e avviare nuovamente lo script `sleha-join`.

5 Eseguire `crm_mon` in ciascun nodo per verificare che il cluster funzioni correttamente. Per verificare il cluster è inoltre possibile utilizzare la console Web 'hawk'. Il nome di login di default è `hacluster` e la password `linux`.

(Condizionale) A seconda dell'ambiente dell'utente, eseguire le operazioni seguenti per modificare ulteriori parametri:

1 Affinché un errore in un solo nodo di un cluster comprendente due nodi non interrompa improvvisamente tutto il cluster, impostare l'opzione globale `no-quorum-policy` su `ignore`:

```
crm configure property no-quorum-policy=ignore
```

Nota: se nel cluster sono presenti più di due nodi, non impostare questa opzione.

---

2 Affinché la gestione delle risorse ne consenta l'esecuzione e lo spostamento, impostare l'opzione globale del cluster `default-resource-stickiness` su 1:

```
crm configure property default-resource-stickiness=1
```

Configurazione delle risorse

In SLE HAE vengono forniti di default alcuni Resource Agent. Se non si desidera utilizzare SLE HAE, queste risorse aggiuntive dovranno essere monitorate utilizzando un'altra tecnologia:

- Una risorsa del file system corrispondente alla memorizzazione condivisa utilizzata dal software.

- Una risorsa con indirizzo IP corrispondente all'indirizzo IP virtuale utilizzato per l'accesso ai servizi.
- Il database PostgreSQL in cui vengono memorizzati i metadati delle configurazioni e degli eventi.

Per la configurazione delle risorse, utilizzare la procedura seguente:

Lo script `crm` facilita la configurazione del cluster. Tale script recupera le variabili necessarie per la configurazione dal file per l'installazione in modalità automatica generato durante l'installazione di Sentinel. Se non è stato generato il file di configurazione o se si desidera cambiare la configurazione delle risorse, è possibile modificare lo script secondo necessità utilizzando la procedura seguente.

1. Eseguire la connessione al nodo originale in cui è stata eseguita l'installazione di Sentinel.

   Nota: utilizzare il nodo in cui è stata eseguita l'installazione completa di Sentinel.

2. Modificare lo script in modo che appaia come segue, dove `<SHARED1>` è il volume condiviso creato precedentemente:

   ```
   mount /dev/<SHARED1> /var/opt/novell
   ```

   ```
   cd /usr/lib/ocf/resource.d/novell
   ```

   ```
   ./install-resources.sh
   ```

3. (Condizionale) Potrebbero verificarsi dei problemi con le nuove risorse in arrivo nel cluster. Se si verifica questo problema, eseguire il seguente comando su node02:

   Per SLES 11 SP4:

   ```
   /etc/rc.d/openais start
   ```

   Per SLES 12 SP1:

   ```
   systemctl start pacemaker.service
   ```

4. Lo script `install-resources.sh` richiederà un paio di valori, più precisamente l'indirizzo IP virtuale che si desidera venga utilizzato per l'accesso a Sentinel e il nome del dispositivo usato per la memorizzazione condivisa, quindi creerà automaticamente le risorse di cluster necessarie. Si noti che per l'esecuzione dello script il volume condiviso deve già essere stato montato e il file dell'istallazione in modalità automatica (`/tmp/install.props`) creato durante l'installazione di Sentinel deve essere presente. Non è necessario eseguire questo script in altri nodi oltre a quello installato per primo, in quanto tutti i file relativi alla configurazione verranno sincronizzati automaticamente con gli altri nodi.
5. Se l'ambiente del cliente è diverso da quello della soluzione consigliata da , è possibile modificare il file `resources.cli` (nella stessa directory) e cambiare le definizioni originarie dalla stessa ubicazione. Ad esempio, la soluzione consigliata utilizza una semplice risorsa del file system, ma è possibile utilizzare anche una risorsa cLVM maggiormente capace di riconoscere il cluster.
6. Dopo aver eseguito lo script di shell, è possibile inviare un comando `crm status` e il risultato dovrebbe essere analogo a quello riportato di seguito:

   ```
   crm status
   ```

   ```
   Last updated: Thu Jul 26 16:34:34 2012
   Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
   Stack: openais
   Current DC: node01 - partition with quorum
   Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
   2 Nodes configured, 2 expected votes
   5 Resources configured.
   ```

```
Online: [ node01, node02 ]
stonith-sbd    (stonith:external/sbd):    Started node01
 Resource Group: sentinelgrp
     sentinelip    (ocf::heartbeat:IPaddr2):    Started node01
     sentinelfs    (ocf::heartbeat:Filesystem):    Started node01
     sentineldb    (ocf::novell:pgsql):    Started node01
     sentinelserver    (ocf::novell:sentinel):    Started node01
```

7 A questo punto è necessario configurare nel cluster le risorse per Sentinel. È possibile analizzare come vengono configurate e raggruppate nello strumento di gestione del cluster, ad esempio eseguendo un comando di stato crm.

Configurazione della memorizzazione secondaria

Per configurare la memorizzazione secondaria in modo che Sentinel possa eseguire la migrazione delle partizioni degli eventi in una memorizzazione meno costosa, eseguire la procedura seguente:

Nota: questa procedura è facoltativa e la memorizzazione secondaria non deve necessariamente essere ad alta disponibilità e configurata come il resto del sistema. È possibile utilizzare qualsiasi directory, montata da un SAN o meno, un volume NFS o un volume CIFS.

---

1 Nell'interfaccia principale di Sentinel, fare clic su **Memorizzazione** nella barra dei menu superiore.

2 Selezionare **Configurazione**.

3 Selezionare uno dei pulsanti di scelta della memorizzazione secondaria non configurata.

Utilizzare una destinazione iSCSI semplice come ubicazione di rete per la memorizzazione condivisa, praticamente con la stessa configurazione della memorizzazione primaria. Nell'ambiente di produzione dell'utente le tecnologie di memorizzazione potrebbero essere diverse.

Per configurare la memorizzazione secondaria affinché Sentinel possa utilizzarla, eseguire la procedura seguente:

Nota: Per Destinazione iSCSI, la destinazione verrà montata come directory da utilizzare come memorizzazione secondaria. È necessario configurare il montaggio come una risorsa del file system in modo analogo alla configurazione del file system per la memorizzazione primaria. Non è stato configurato automaticamente nello script di installazione delle risorse poiché sono possibili altre varianti.

---

1 Riesaminare i passaggi precedenti per stabilire quale partizione sia stata creata per l'uso come memorizzazione secondaria (`/dev/<NETWORK1>` o qualcosa del tipo `/dev/sdc1`). Se necessario, creare una directory vuota in cui sia possibile montare la partizione (ad esempio `/var/opt/netdata`).

2 Configurare il file system di rete come risorsa cluster utilizzando l'interfaccia principale di Sentinel o eseguendo il comando:

```
crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
```

in cui `/dev/<NETWORK1>` è la partizione creata come descritto nella precedente sezione Configurazione della memorizzazione condivisa e <PATH> è una directory locale in cui può essere montata.

3 Aggiungere la nuova risorsa al gruppo di risorse gestite:

```
 crm resource stop sentinelgrp
 crm configure delete sentinelgrp
 crm configure group sentinelgrp sentinelip sentinelfs sentinelnetfs sentineldb
sentinelserver
 crm resource start sentinelgrp
```

4. È possibile eseguire la connessione al nodo in cui risiedono le risorse (utilizzare il comando `crm status` o `Hawk`) e verificare che la memorizzazione secondaria sia montata correttamente (utilizzare il comando `mount`).
5. Eseguire il login all'interfaccia principale di Sentinel.
6. Selezionare **Memorizzazione** e successivamente **Configurazione**, quindi selezionare il dispositivo **SAN (montato localmente)** nella memorizzazione secondaria non configurata.
7. Digitare il percorso in cui è stata montata la memorizzazione secondaria, ad esempio `/var/opt/netdata`.

Utilizzare versioni semplici delle risorse necessarie, come ad esempio l'agente risorsa del file system. È possibile utilizzare anche risorse cluster più sofisticate, quali cLVM, cioè una versione del file system con volume logico.

38 Configurazione di Sentinel ad alta disponibilità come SSDM

In questo capitolo vengono fornite informazioni sulla configurazione dell'impostazione di Sentinel ad alta disponibilità come SSDM. Queste istruzioni sono valide sia per le installazioni tradizionali che per le installazioni in modalità applicazione.

Per configurare l'impostazione di Sentinel ad alta disponibilità come SSDM:

1. Installare e configurare la memorizzazione scalabile per Sentinel. Per ulteriori informazioni, consultare la Capitolo 13, “Installazione e configurazione della memorizzazione scalabile”, a pagina 87.
2. Abilitare la memorizzazione scalabile nel nodo attivo. Per ulteriori informazioni, vedere “Enabling Scalable Storage Post-Installation” (Abilitazione della memorizzazione scalabile dopo l'installazione) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).
3. Eseguire il comando seguente nel nodo attivo:

   ```
   csync2 -x -v
   ```

   La configurazione di SSDM viene così sincronizzata in tutti i nodi passivi.
4. (Condizionale) Se il comando `csync2 -x -v` eseguito al passaggio 3 non ha eseguito la sincronizzazione di tutti i file, effettuare i passaggi seguenti:
   - **4a** Cancellare il database csync2 (nella directory `/var/lib/csync2`) in tutti i nodi.
   - **4b** Eseguire il comando seguente in tutti i server per aggiornare il database csync2 in funzione del file system, ma senza contrassegnare nulla come elemento da sincronizzare con altri server:

     ```
     csync2 -cIr /
     ```
   - **4c** Eseguire il comando seguente per trovare tutte le differenze tra server con autorità e server remoti e contrassegnare per la sincronizzazione:

     ```
     csync2 -TUXI
     ```
   - **4d** Eseguire il comando seguente per reimpostare il database al fine di forzare il server attuale come risolutore di eventuali conflitti:

     ```
     csync2 -fr /
     ```
   - **4e** Eseguire il comando seguente per avviare la sincronizzazione con tutti gli altri server:

     ```
     csync2 -xr /
     ```
   - **4f** Eseguire il comando seguente per verificare che tutti i file siano sincronizzati:

     ```
     csync2 -T
     ```

     Se la sincronizzazione ha esito positivo non verrà visualizzato alcun file nell'elenco.

39 Upgrade di Sentinel in configurazione ad alta disponibilità

Quando si esegue l'upgrade di Sentinel in un ambiente ad alta disponibilità, è necessario eseguire prima di tutto l'upgrade dei nodi passivi del cluster e continuare con quelli attivi.

Prerequisiti

- Effettuare il download della versione più recente del programma di installazione dal sito Web dei download.
- Se si utilizza il sistema operativo SLES con il kernel versione 3.0.101 o successive, è necessario caricare manualmente nel computer il driver del processo Watchdog. Per individuare il driver del processo Watchdog appropriato per l'hardware del computer in uso, rivolgersi al fornitore dell'hardware. Per caricare il driver del processo Watchdog, eseguire le operazioni seguenti:
  1. Al prompt dei comandi, eseguire il comando seguente per caricare il driver del processo Watchdog nella sessione attuale:

     `/sbin/modprobe -v --ignore-install <nome processo Watchdog>`
  2. Affinché il computer carichi automaticamente il driver del processo Watchdog a ogni avvio, aggiungere la riga seguente nel file `/etc/init.d/boot.local`:

     `/sbin/modprobe -v --ignore-install <nome processo Watchdog>`

Esecuzione dell'upgrade di un'installazione tradizionale ad alta disponibilità di Sentinel

In questa sezione vengono fornite informazioni sull'upgrade di un'installazione tradizionale di Sentinel e del sistema operativo in un'installazione tradizionale di Sentinel.

Importante: Nella procedura descritta in questa sezione vengono utilizzati i comandi `rcopenais` e `openais`, compatibili soltanto con SLES 11 SP4. Per SLES 12 SP2 e versioni successive, utilizzare il comando `systemctl pacemaker.service`.

Ad esempio, nel caso del comando `/etc/rc.d/openais start`, utilizzare il comando `systemctl start pacemaker.service`.

Upgrade di Sentinel ad alta disponibilità

1. Abilitare la modalità di manutenzione nel cluster:

   ```
   crm configure property maintenance-mode=true
   ```

   La modalità di manutenzione facilita l'eliminazione di eventuali disturbi sulle risorse del cluster in esecuzione mentre si esegue l'aggiornamento di Sentinel. Il comando seguente può essere eseguito da uno qualsiasi dei nodi del cluster.

2. Verificare che la modalità di manutenzione sia attiva:

   ```
   crm status
   ```

   Le risorse del cluster devono apparire nello stato non gestito.

3. Upgrade del nodo passivo del cluster:

   3a Arrestare lo stack del cluster:

   ```
   rcopenais stop
   ```

   Arrestando lo stack del cluster le risorse rimangono accessibili e si evitano isolamenti dei nodi.

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

   3c Estrarre i file di installazione dal file .tar:

   ```
   tar xfz <nomefile_installazione>
   ```

   3d Nella directory in cui risiedono i file di installazione estratti, eseguire il comando seguente:

   ```
   ./install-sentinel --cluster-node
   ```

   3e Al termine dell'upgrade, riavviare lo stack del cluster:

   ```
   rcopenais start
   ```

   Ripetere il Passo 3 per tutti i nodi passivi del cluster.

   3f Rimuovere gli script di avvio automatico affinché il cluster possa gestire il prodotto.

   ```
   cd /
   insserv -r sentinel
   ```

4. Upgrade del nodo attivo del cluster:

   4a eseguire il backup della configurazione, quindi creare un'esportazione ESM.

   Per ulteriori informazioni, vedere “Backing Up and Restoring Data” (Backup e ripristino dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.1) .

   4b Arrestare lo stack del cluster:

   ```
   rcopenais stop
   ```

   Arrestando lo stack del cluster le risorse rimangono accessibili e si evitano isolamenti dei nodi.

   4c Effettuare il login come utente `root` al server in cui si desidera eseguire l'upgrade di Sentinel.

   4d Per estrarre i file di installazione dal file .tar, eseguire il comando seguente:

   ```
   tar xfz <nomefile_installazione>
   ```

   4e Nella directory in cui risiedono i file di installazione estratti, eseguire il comando seguente:

   ```
   ./install-sentinel
   ```

   4f Al termine dell'upgrade, riavviare lo stack del cluster:

```
rcopenais start
```

4g Rimuovere gli script di avvio automatico affinché il cluster possa gestire il prodotto.

```
cd /
insserv -r sentinel
```

4h Per sincronizzare eventuali modifiche apportate ai file di configurazione, eseguire il comando seguente:

```
csync2 -x -v
```

5 Disabilitare la modalità di manutenzione nel cluster:

```
crm configure property maintenance-mode=false
```

Il comando seguente può essere eseguito da uno qualsiasi dei nodi del cluster.

6 Verificare che la modalità di manutenzione sia disattivata:

```
crm status
```

Le risorse del cluster devono apparire avviate.

7 (Facoltativo) Verificare che l'upgrade di Sentinel sia stato eseguito correttamente:

```
rcsentinel version
```

Upgrade del sistema operativo

In questa sezione vengono fornite informazioni su come eseguire l'upgrade del sistema operativo a una versione principale, come l'upgrade da SLES 11 a SLES 12, in un cluster Sentinel ad alta disponibilità. Quando si esegue l'upgrade del sistema operativo, è necessario effettuare alcuni task di configurazione affinché Sentinel ad alta disponibilità funzioni correttamente dopo l'upgrade del sistema operativo.

Effettuare i passaggi descritti nelle sezioni seguenti:

- “Upgrade del sistema operativo” a pagina 215
- “Configurazione delle destinazioni iSCSI” a pagina 216
- “Configurazione degli iniziatori iSCSI” a pagina 217
- “Configurazione del cluster ad alta disponibilità” a pagina 218

Upgrade del sistema operativo

Per eseguire l'upgrade del sistema operativo:

1 Eseguire il login come utente `root` in qualsiasi nodo del cluster Sentinel ad alta disponibilità.

2 Eseguire il comando seguente per abilitare la modalità di manutenzione nel cluster:

```
crm configure property maintenance-mode=true
```

La modalità di manutenzione facilita l'eliminazione di eventuali disturbi sulle risorse del cluster in esecuzione mentre si esegue l'upgrade del sistema operativo.

3 Eseguire il comando seguente per verificare che la modalità di manutenzione sia attiva:

```
crm status
```

Le risorse del cluster devono apparire nello stato non gestito.

4 Assicurarsi di aver eseguito l'upgrade di Sentinel alla versione 8.2 o successive in tutti i nodi del cluster.

5 Assicurarsi che tutti i nodi del cluster siano registrati in SLES e SLESHA.

6 Per eseguire l'upgrade del sistema operativo nel nodo passivo del cluster, effettuare i passaggi seguenti:

   6a Eseguire il comando seguente per interrompere lo stack del cluster:

   ```
   rcopenais stop
   ```

   Interrompendo lo stack del cluster le risorse rimangono inaccessibili e si evita il fencing dei nodi.

   6b Eseguire l'upgrade del sistema operativo. Per ulteriori informazioni, vedere Upgrade del sistema operativo.

7 Ripetere il passaggio 6 in tutti i nodi passivi per eseguire l'upgrade del sistema operativo.

8 Ripetere il passaggio 6 sul nodo attivo per eseguire l'upgrade del sistema operativo su tale nodo.

9 Ripetere il passaggio 6b per eseguire l'upgrade del sistema operativo nell'area di memorizzazione condivisa.

10 Assicurarsi che sia stato eseguito l'upgrade del sistema operativo a SLES12 SP3 su tutti i nodi del cluster.

Configurazione delle destinazioni iSCSI

Per configurare le destinazioni iSCSI:

1 Nella memorizzazione condivisa, verificare che sia installato il pacchetto iSCSI LIO. Se non è ancora installato, passare a YaST2 Software Management e installare il pacchetto iSCSI LIO (`isccliotarget` RPM).

2 Effettuare i passaggi seguenti in tutti i nodi del cluster:

   2a Eseguire il comando seguente per aprire il file contenente il nome dell'iniziatore iSCSI:

   ```
   cat /etc/iscsi/initiatorname.iscsi
   ```

   2b Prendere nota del nome dell'iniziatore per utilizzarlo durante la configurazione degli iniziatori iSCSI:

   Ad esempio:

   ```
   InitiatorName=iqn.1996-04.de.suse:01:441d6988994
   ```

   I nomi degli iniziatori verranno utilizzati durante la configurazione di iSCSI Target Client Setup.

3 Fare clic su **Service** (Servizio) e selezionare l'opzione **When Booting** (In avvio) affinché il servizio venga avviato quando si avvia il sistema operativo.

4 Selezionare la scheda **Global** (Globale), deselezionare **No Authentication** (Nessuna autenticazione) per abilitare l'autenticazione, quindi specificare il nome utente e la password per l'autenticazione in entrata e in uscita.

   L'opzione **No Authentication** (Nessuna autenticazione) è abilitata per default. Tuttavia, è necessario abilitare l'autenticazione affinché la configurazione sia sicura.

5 Fare clic su **Targets** (Destinazioni) e successivamente su **Add** (Aggiungi) per aggiungere una nuova destinazione.

6 Fare clic su **Aggiungi** per aggiungere un nuovo LUN.

7 Non modificare il numero 0 del LUN, spostarsi nella finestra di dialogo **Path** (Percorso), nel tipo fileio, e selezionare il file `/localdata` precedentemente creato. Se per la memorizzazione si utilizza un disco dedicato, specificare un dispositivo di blocco, ad esempio `/dev/sdc`.

8 Ripetere i passaggi 6 e 7, ma questa volta aggiungere LUN 1 e selezionare `/networkdata`.

9 Ripetere i passaggi 6 e 7, ma questa volta aggiungere LUN 2 e selezionare `/sbd`.

10 Non modificare i valori di default delle altre opzioni. Fare clic su **Avanti**.

11 Fare clic su **Aggiungi**. Quando viene richiesto il nome del client, specificare il nome dell'iniziatore copiato al passaggio 2. Ripetere questo passaggio per aggiungere tutti i nomi dei client, specificando i nomi degli iniziatori.

   In Client List (Elenco client) verrà visualizzato l'elenco dei nomi dei client.

12 (Condizionale) Se al passaggio 4 è stata abilitata l'autenticazione, fornire le credenziali di autenticazione immesse al passaggio 4.

   Selezionare un client, scegliere **Edit Auth** (Modifica·autenticazione) > **Incoming Authentication** (Autenticazione in entrata) e specificare il nome utente e la password. Ripetere l'operazione per tutti i client.

13 Fare nuovamente clic su **Next** (Avanti) per selezionare le opzioni di autenticazione di default e successivamente su **Finish** (Fine) per uscire dalla configurazione. Se richiesto, riavviare iSCSI.

14 Uscire da YaST.

Configurazione degli iniziatori iSCSI

Per configurare gli iniziatori iSCSI:

1 Eseguire la connessione a un nodo del cluster (node01) e avviare YaST.

2 Fare clic su **Servizi di rete** > **Iniziatore iSCSI**.

3 Se richiesto, installare il software necessario (RPM `iscsiclient`).

4 Fare clic su **Service** (Servizio) e selezionare **When Booting** (In avvio) affinché il servizio iSCSI venga avviato in fase di avvio.

5 Fare clic su **Discovered Targets** (Destinazioni rilevate).

   Nota: se vengono visualizzate eventuali destinazioni iSCSI esistenti, eliminarle.

   Selezionare **Discovery** (Rilevazione) per aggiungere una nuova destinazione iSCSI.

6 Specificare l'indirizzo IP della destinazione iSCSI (10.0.0.3).

   (Condizionale) Se al passaggio 4 di “Configurazione delle destinazioni iSCSI” a pagina 216 è stata abilitata l'autenticazione, deselezionare **No Authentication** (Nessuna autenticazione). Nella sezione **Outgoing Authentication** (Autenticazione in uscita), immettere le credenziali di autenticazione specificate durante la configurazione delle destinazioni iSCSI.

   Fare clic su **Avanti**.

7 Selezionare la destinazione iSCSI rilevata con indirizzo IP 10.0.0.3 e successivamente **Log In** (Login).

8 eseguire i passaggi seguenti:

   8a Passare alla modalità automatica nel menu a discesa **Startup** (Avvio).

   8b (Condizionale) Se è stata abilitata l'autenticazione, deselezionare **No Authentication** (Nessuna autenticazione).

   Il nome utente e la password specificati dovrebbero apparire nella sezione **Outgoing Authentication** (Autenticazione in uscita). Se le credenziali non vengono visualizzate, immetterle in questa sezione.

   8c Fare clic su **Avanti**.

9 Passare alla scheda **Connected Targets** (Destinazioni connesse) per verificare che la connessione alla destinazione sia stata eseguita.

10 Uscire dalla configurazione. Eseguendo questa procedura le destinazioni iSCSI vengono montate come dispositivi di blocco nel nodo del cluster.

11 Nel menu principale di YaST, selezionare **Sistema** > **Partizionatore**.

12 In System View (Vista di sistema), dovrebbero essere visibili nell'elenco i nuovi dischi rigidi del tipo LIO-ORG-FILEIO (ad esempio `/dev/sdb` e `/dev/sdc`), insieme ai dischi già formattati (ad esempio `/dev/sdb1` o `/dev/<SHARED1`).

13 Ripetere i passaggi da 1 a 12 in tutti i nodi.

Configurazione del cluster ad alta disponibilità

Per configurare il cluster ad alta disponibilità:

1 Avviare YaST2 e scegliere **High Availability** (Alta disponibilità) > **Cluster**.

2 Se richiesto, installare il pacchetto per l'alta disponibilità e risolvere le dipendenze.

Dopo l'installazione del pacchetto per l'alta disponibilità, appare la segnalazione Cluster-Communication Channels (Cluster-Canali di comunicazione).

3 Assicurarsi che come opzione di trasporto sia stato selezionato `Unicast`.

4 Selezionare **Add a Member Address** (Aggiungi indirizzo di un membro) e specificare l'indirizzo IP del nodo, quindi ripetere l'operazione per aggiungere tutti gli altri indirizzi IP dei nodi del cluster.

5 Assicurarsi che l'opzione **Auto Generate Node ID** (Generazione automatica ID nodo) sia selezionata.

6 Assicurarsi che il servizio HAWK sia abilitato in tutti i nodi. Se non è ancora stato abilitato, eseguire il comando seguente per abilitarlo:

```
service hawk start
```

7 Eseguire il comando seguente:

```
ls -l /dev/disk/by-id/
```

Viene visualizzato l'ID della partizione SBD. Ad esempio, `scsi-1LIO-ORG_FILEIO:33caaa5a-a0bc-4d90-b21b-2ef33030cc53`.

Copiare l'ID.

8 Aprire il file sbd (`/etc/sysconfig/sbd`) e modificare l'ID di `SBD_DEVICE` specificando l'ID copiato al passaggio 7.

9 Eseguire i comandi seguenti per riavviare il servizio pacemaker:

```
rcpacemaker restart
```

10 Eseguire i comandi seguenti per rimuovere gli script di avvio automatico, in modo che il cluster possa gestire il prodotto.

```
cd /
```

```
insserv -r sentinel
```

11 Ripetere i passaggi da 1 a 10 in tutti i nodi del cluster.

12 Per sincronizzare eventuali modifiche apportate ai file di configurazione, eseguire il comando seguente:

```
csync2 -x -v
```

13 Eseguire il comando seguente per disabilitare la modalità di manutenzione nel cluster:

```
crm configure property maintenance-mode=false
```

Il comando seguente può essere eseguito da uno qualsiasi dei nodi del cluster.

14 Eseguire il comando seguente per verificare che la modalità di manutenzione sia disattivata:

```
crm status
```

Le risorse del cluster devono apparire avviate.

Esecuzione dell'upgrade di un'installazione in modalità applicazione ad alta disponibilità di Sentinel

È possibile eseguire l'upgrade di un'installazione in modalità applicazione di Sentinel ad alta disponibilità utilizzando la patch Zypper.

Importante: Nella procedura descritta in questa sezione vengono utilizzati i comandi `rcopenais` e `openais`, compatibili soltanto con SLES 11 SP4. Per SLES 12 SP2 e versioni successive, utilizzare il comando `systemctl pacemaker.service`.

Ad esempio, nel caso del comando `/etc/rc.d/openais start`, utilizzare il comando `systemctl start pacemaker.service`.

- “Esecuzione dell'upgrade dell'applicazione Sentinel ad alta disponibilità mediante Zypper” a pagina 219

Esecuzione dell'upgrade dell'applicazione Sentinel ad alta disponibilità mediante Zypper

Prima di eseguire l'upgrade è necessario registrare tutti i nodi dell'applicazione mediante Sentinel Appliance Manager. Per ulteriori informazioni, vedere la “Registrazione degli aggiornamenti” a pagina 106. Se non viene eseguita la registrazione dell'applicazione, in Sentinel appare un avviso di colore giallo.

1. Abilitare la modalità di manutenzione nel cluster.

   ```
   crm configure property maintenance-mode=true
   ```

   La modalità di manutenzione facilita l'eliminazione di eventuali disturbi sulle risorse del cluster in esecuzione mentre si esegue l'aggiornamento del software Sentinel. Il comando seguente può essere eseguito da uno qualsiasi dei nodi del cluster.

2. Verificare che la modalità di manutenzione sia attiva.

   ```
   crm status
   ```

   Le risorse del cluster devono apparire nello stato non gestito.

3. Upgrade del nodo passivo del cluster:

   3a Arrestare lo stack del cluster.

   ```
   rcopenais stop
   ```

   Interrompendo lo stack del cluster le risorse rimangono inaccessibili e si evita il fencing dei nodi.

   3b Effettuare il download degli aggiornamenti per l'applicazione Sentinel ad alta disponibilità.

   ```
   zypper -v patch
   ```

   3c (Condizionale) Se nel programma di installazione viene visualizzato un messaggio che richiede di risolvere la dipendenza per il pacchetto OpenSSH, immettere l'opzione appropriata per eseguire il downgrade del pacchetto OpenSSH.

3d (Condizionale) Se nel programma di installazione viene visualizzato un messaggio che indica una modifica nell'architettura ncgOverlay, immettere l'opzione appropriata per accettare la modifica dell'architettura.

3e (Condizionale) Se nel programma di installazione viene visualizzato un messaggio che richiede di risolvere la dipendenza di alcuni pacchetti dell'applicazione, immettere l'opzione appropriata per disinstallare i pacchetti dipendenti.

3f Al termine dell'upgrade, riavviare lo stack del cluster.

```
rcopenais start
```

4 Ripetere il passaggio 3 per tutti i nodi passivi del cluster.

5 Upgrade del nodo attivo del cluster:

5a eseguire il backup della configurazione, quindi creare un'esportazione ESM.

Per ulteriori informazioni sul backup dei dati, vedere "Backing Up and Restoring Data" (Backup e ripristino dei dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

5b Arrestare lo stack del cluster.

```
rcopenais stop
```

Interrompendo lo stack del cluster le risorse rimangono inaccessibili e si evita il fencing dei nodi.

5c Effettuare il download degli aggiornamenti per l'applicazione Sentinel ad alta disponibilità.

```
zypper -v patch
```

5d (Condizionale) Se nel programma di installazione viene visualizzato un messaggio che richiede di risolvere la dipendenza per il pacchetto OpenSSH, immettere l'opzione appropriata per eseguire il downgrade del pacchetto OpenSSH.

5e (Condizionale) Se nel programma di installazione viene visualizzato un messaggio che indica una modifica nell'architettura ncgOverlay, immettere l'opzione appropriata per accettare la modifica dell'architettura.

5f (Condizionale) Se nel programma di installazione viene visualizzato un messaggio che richiede di risolvere la dipendenza di alcuni pacchetti dell'applicazione, immettere l'opzione appropriata per disinstallare i pacchetti dipendenti.

5g Al termine dell'upgrade, riavviare lo stack del cluster.

```
rcopenais start
```

5h Per sincronizzare eventuali modifiche apportate ai file di configurazione, eseguire il comando seguente:

```
csync2 -x -v
```

6 Disabilitare la modalità di manutenzione nel cluster.

```
crm configure property maintenance-mode=false
```

Il comando seguente può essere eseguito da uno qualsiasi dei nodi del cluster.

7 Verificare che la modalità di manutenzione sia disattivata.

```
crm status
```

Le risorse del cluster devono apparire avviate.

8 (Facoltativo) Verificare che l'upgrade di Sentinel sia stato eseguito correttamente:

```
rcsentinel version
```

9 (Condizionale) Per eseguire l'upgrade del sistema operativo, vedere "Upgrade del sistema operativo" a pagina 162.

40 backup e recupero d'emergenza

Il cluster di failover ad alta disponibilità descritto nel presente documento offre un livello ridondanza sufficiente affinché, in caso di errore del servizio in un nodo, venga eseguito automaticamente il failover e il ripristino in un altro nodo del cluster. Quando si verifica un evento di questo tipo è importante che venga ripristinato il normale stato operativo del nodo in stato di errore, così che la ridondanza del sistema sia disponibile nel caso in cui si verifichi un altro errore. In questa sezione si illustra come ripristinare un nodo che si trova in diverse condizioni di errore.

Backup

Quando un cluster di failover ad alta disponibilità come quello descritto nel presente documento offre un livello di ridondanza, è comunque importante effettuare regolarmente i tradizionali backup della configurazione e dei dati che non sarebbero facilmente ripristinabili in caso di perdita o danneggiamento. Nella sezione “Backing Up and Restoring Data” (Backup e ripristino dei dati) della *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.1) si descrive come utilizzare gli strumenti integrati di Sentinel per eseguire il backup. Tali strumenti devono essere utilizzati nel nodo attivo del cluster, poiché il nodo passivo non disporrà dell'accesso necessario al dispositivo di memorizzazione condivisa. È possibile utilizzare anche altri strumenti di backup reperibili in commercio, ma potrebbero avere requisiti diversi per quanto riguarda il nodo in cui possono essere utilizzati.

PlateSpin

Errore temporaneo

Nel caso in cui l'errore sia temporaneo e non si riscontrino danneggiamenti evidenti del software dell'applicazione e del sistema operativo e della configurazione, è sufficiente eliminare l'errore temporaneo, ad esempio riavviando il nodo, e ripristinare così il normale stato operativo. Per il failback del servizio in esecuzione sul nodo originale del cluster è possibile utilizzare l'interfaccia utente per la gestione del cluster.

Danneggiamento dei nodi

Se l'errore ha causato un danneggiamento del software dell'applicazione o del sistema operativo, oppure della configurazione presente nel sistema di memorizzazione del nodo, il software danneggiato deve essere reinstallato. Per ripristinare il normale stato operativo del nodo è necessario

ripetere la procedura descritta precedentemente in questo documento per l'aggiunta di un nodo al cluster. Per il failback del servizio in esecuzione sul nodo originale del cluster è possibile utilizzare l'interfaccia utente per la gestione del cluster.

Configurazione dei dati del cluster

In caso di danneggiamento dei dati nel dispositivo di memorizzazione condivisa tale da non consentire il ripristino del dispositivo stesso, tutto il cluster risulterà danneggiato in modo tale da non consentire il ripristino automatico mediante il cluster di failover ad alta disponibilità descritto nel presente documento. Nella sezione “Backing Up and Restoring Data” (Backup e ripristino dei dati) della *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.1) si descrive come utilizzare gli strumenti integrati di Sentinel per eseguire il ripristino di un backup. Tali strumenti devono essere utilizzati nel nodo attivo del cluster, poiché il nodo passivo non disporrà dell'accesso necessario al dispositivo di memorizzazione condivisa. È possibile utilizzare anche altri strumenti di backup e ripristino reperibili in commercio, ma potrebbero avere requisiti diversi per quanto riguarda il nodo in cui possono essere utilizzati.

VIII Appendici

A Soluzione dei problemi

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

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.

Non viene creato l'UUID per le istanze di Collector Manager e Correlation Engine

Se un server Collector Manager 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 di Collector Manager. Ciò si verifica a causa degli UUID duplicati.

Nei sistemi in cui Collector Manager è stato appena installato, 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 Collector Manager.

   L'UUID viene generato automaticamente dall'istanza di Collector Manager.

Dopo aver eseguito il login l'interfaccia principale di Sentinel appare vuota in 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. Scegliere **Strumenti > Opzioni Internet > 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**.

Sentinel non si avvia in Internet Explorer 11 con Windows Server 2012 R2

Quando si utilizza Windows Server 2012 R2, Sentinel non si avvia in Internet Explorer 11 a causa delle configurazioni di sicurezza di default di Internet Explorer 11. Prima di avviare Sentinel, è necessario aggiungerlo manualmente all'elenco dei siti attendibili.

Per aggiungere Sentinel all'elenco dei siti attendibili:

1. Aprire Internet Explorer 11.
2. Fare clic sull'icona **Impostazioni** > **Opzioni Internet** > scheda **Sicurezza** > **Siti attendibili** > **Siti**.
3. Aggiungere l'host di Sentinel all'elenco dei siti attendibili.

Impossibile eseguire i rapporti locali con la licenza EPS di default

Se nell'ambiente si utilizza la licenza di default per 25 EPS e si esegue un rapporto, il rapporto ha esito negativo con il seguente errore: `La licenza per la ricerca distribuita è scaduta`.

per eseguire i rapporti nella stessa JVM di Sentinel, effettuare le operazioni seguenti:

1. Eseguire il login al server Sentinel e aprire il file `/etc/opt/novell/sentinel/config/obj-component.JasperReportingComponent.properties`.
2. Individuare la proprietà `reporting.process.oktorunstandalone`.
3. (Condizionale) Se la proprietà non è presente nel file, aggiungerla.
4. Impostare la seguente proprietà su `false`. Ad esempio:

   ```
   reporting.process.oktorunstandalone=false
   ```
5. Riavviare Sentinel.

Dopo la conversione del nodo attivo alla modalità FIPS 140-2 in Sentinel High Availability, è necessario avviare manualmente la sincronizzazione

Problema: quando si converte il nodo attivo alla modalità FIPS 140-2 in Sentinel High Availability, la sincronizzazione per convertire tutti i nodi passivi alla modalità FIPS 140-2 non viene eseguita completamente. La sincronizzazione deve essere avviata manualmente.

Soluzione: sincronizzare manualmente tutti i nodi passivi alla modalità FIPS 140-2 come indicato di seguito:

1. Eseguire il login come utente root nel nodo attivo.
2. Aprire il file `/etc/csync2/csync2.cfg`.
3. Modificare la riga seguente:

   ```
   include /etc/opt/novell/sentinel/3rdparty/nss/*;
   ```

   come segue

   ```
   include /etc/opt/novell/sentinel/3rdparty/nss;
   ```
4. Salvare il file `csync2.cfg`.
5. Avviare manualmente la sincronizzazione eseguendo il comando seguente:

   ```
   csync2 -x -v
   ```

Nell'interfaccia principale di Sentinel appare una pagina vuota dopo la conversione a Sentinel Scalable Data Manager

Problema: dopo aver abilitato SSDM, quando si esegue il login all'interfaccia principale di Sentinel, il browser visualizza una pagina vuota.

Soluzione: chiudere il browser e ripetere il login all'interfaccia principale di Sentinel. Questo problema si verifica quando si esegue il login all'interfaccia principale di Sentinel per la prima volta dopo aver abilitato SSDM.

Nella pagina della pianificazione non viene visualizzato il pannello Campi evento quando si modifica una ricerca salvata

Problema: quando si modifica una ricerca salvata di cui è stato eseguito l'upgrade da Sentinel 7.2 a una versione più recente, il pannello **Campi evento**, utilizzato per specificare i campi di output nel file CSV del rapporto di ricerca, non è presente nella pagina della pianificazione.

Soluzione: dopo aver eseguito l'upgrade di Sentinel, per visualizzare il pannello **Campi evento** nella pagina della pianificazione, ricreare e ripianificare la ricerca.

Sentinel non restituisce alcun evento correlato quando si effettua la ricerca di eventi relativi alla regola installata utilizzando la ricerca Totale attivazioni di default

Problema: in Sentinel non viene restituito alcun evento correlato quando si cercano tutti gli eventi correlati generati dopo l'installazione o l'abilitazione della regola facendo clic sull'icona accanto a **Totale attivazioni** nel pannello **Statistiche attività** della pagina Riepilogo correlazione per la regola.

Soluzione: modificare il valore nel campo **Da** della pagina Ricerca evento impostando un orario precedente a quello popolato nel campo e fare nuovamente clic su **Cerca**.

Nel dashboard di Security Intelligence viene visualizzata una durata non valida quando si rigenera la linea di base

Problema: quando si rigenera la linea di base di Security Intelligence, le relative date iniziale e finale sono errate e viene visualizzato il valore 1/1/1970.

Soluzione: al termine della rigenerazione della linea di base le date vengono aggiornate correttamente.

Il server Sentinel viene chiuso in caso di numero elevato di eventi in una sola partizione quando si effetua una ricerca

Problema: quando si effettua una ricerca, il server Sentinel viene chiuso in caso di numero elevato di eventi in una sola partizione.

Soluzione: creare policy di permanenza affinché nel corso di una giornata siano aperte almeno due partizioni. L'utilizzo di più partizioni aperte contribuisce a ridurre il numero di eventi indicizzati nelle partizioni stesse.

Si possono creare policy di permanenza che filtrino gli eventi in base al campo `estzhour` utilizzato per controllare l'orario della giornata. È quindi possibile creare una policy di permanenza utilizzando `estzhour:[0 TO 11]` come filtro e un'altra con `estzhour:[12 TO 23]`.

Per ulteriori informazioni, vedere “Configuring Data Retention Policies” (Configurazione delle policy di permanenza dei dati) nella *Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

Errore dello script report_dev_setup.sh quando si configurano le porte di Sentinel per le eccezioni del firewall nelle installazioni di upgrade dell'applicazione Sentinel

Problema: in Sentinel viene visualizzato un errore quando si utilizza lo script `report_dev_setup.sh` per configurare le porte di Sentinel per le eccezioni del firewall.

Soluzione: configurare le porte di Sentinel per le eccezioni del firewall eseguendo le operazioni seguenti:

1. Aprire il file `/etc/sysconfig/SuSEfirewall2`.
2. Modificare la riga seguente:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   come segue

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Riavviare Sentinel.

B Disinstallazione

In questa appendice sono riportate informazioni relative alla disinstallazione di Sentinel e ai task post-disinstallazione.

Elenco di controllo per la disinstallazione

Per disinstallare Sentinel, utilizzare l'elenco di controllo seguente:

- ❒ Disinstallare il server Sentinel.
- ❒ Disinstallare eventuali istanze di Collector Manager e di Correlation Engine.
- ❒ Per completare la disinstallazione, eseguire i task post-disinstallazione.

Disinstallazione di Sentinel

Per disinstallare Sentinel è disponibile uno script di disinstallazione. 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.

Avviso: 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.

Disinstallazione del server Sentinel

Per disinstallare il server Sentinel, utilizzare la procedura seguente:

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

   Nota: 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, tale utente può disinstallare il server Sentinel.

   ---

2. Accedere alla directory seguente:

   ```
   <sentinel_installation_path>/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.

Disinstallazione di Collector Manager e di Correlation Engine

Per disinstallare le istanze di Collector Manager e di Correlation Engine, effettuare le operazioni seguenti:

1 Eseguire il login come `root` al computer in cui risiedono le istanze di Collector Manager e di Correlation Engine.

   Nota: se l'installazione è stata eseguita come un utente `root`, non è possibile eseguire la disinstallazione delle istanze remote di Collector Manager e di Correlation Engine come 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 l'istanza di Collector Manager o di Correlation Engine sarà rimossa insieme a tutti i dati associati.

4 Immettere y per rimuovere l'istanza di Collector Manager o di Correlation Engine.

   Lo script prima interrompe il servizio, quindi lo rimuove completamente. Tuttavia, l'icona di Collector Manager e di Correlation Engine rimane visualizzata nell'interfaccia principale di Sentinel nello stato inattivo.

5 (Condizionale) Se è stata abilitata la visualizzazione degli eventi, è necessario reinstallare il plug-in di sicurezza per Elasticsearch. Per ulteriori informazioni, consultare “Reinstallazione del plug-in di sicurezza per Elasticsearch” a pagina 84.

6 Per eliminare manualmente Collector Manager e Correlation Engine, effettuare i passaggi seguenti nell'interfaccia principale di Sentinel:

   Collector Manager:

   1. Accedere a **Gestione origini eventi > Visualizzazione in diretta**.
   2. Fare clic con il pulsante destro del mouse sull'istanza di Collector Manager che si desidera eliminare, quindi scegliere **Elimina**.

   Correlation Engine:

   1. Andare all'interfaccia **Sentinel Main** come amministratore.
   2. Espandere **Correlazione**, quindi selezionare l'istanza di Correlation Engine che si desidera eliminare.
   3. Fare clic sul pulsante **Elimina** (icona del cestino).

Disinstallazione dell'istanza di NetFlow Collector Manager

Per disinstallare l'istanza di NetFlow Collector Manager, utilizzare la procedura seguente:

1. Eseguire il login al computer in cui risiede l'istanza di NetFlow Collector Manager.

   Nota: Eseguire il login con la medesima autorizzazione utente utilizzata per l'installazione dell'istanza di NetFlow Collector Manager.

2. Passare alla directory seguente:

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

3. Eseguire il comando seguente:

   ```
   ./uninstall–sentinel
   ```

4. Per disinstallare l'instanza di Collector Manager, immettere `y`.

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

Task successivi alla disinstallazione

La disinstallazione del server Sentinel non include la rimozione dell'utente amministratore di Sentinel dal sistema operativo. L'operazione deve essere eseguita manualmente.

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.