# Sentinel™

## Guida all'installazione e alla configurazione

**Agosto 2021**

## Note legali



Le sole garanzie valide per prodotti e servizi di Micro Focus, le sue affiliate e i concessori di licenza ("Micro Focus") sono specificate nelle dichiarazioni esplicite di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto riportato nel presente documento deve essere interpretato come garanzia aggiuntiva. Micro Focus non sarà da ritenersi responsabile per errori tecnici o editoriali contenuti nel presente documento né per eventuali omissioni. Le informazioni di questo documento sono soggette a modifiche senza preavviso.

Per ulteriori informazioni, ad esempio note relative alla certificazione e marchi di fabbrica, vedere http://www.microfocus.com/about/legal/.

# Sommario

# 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?

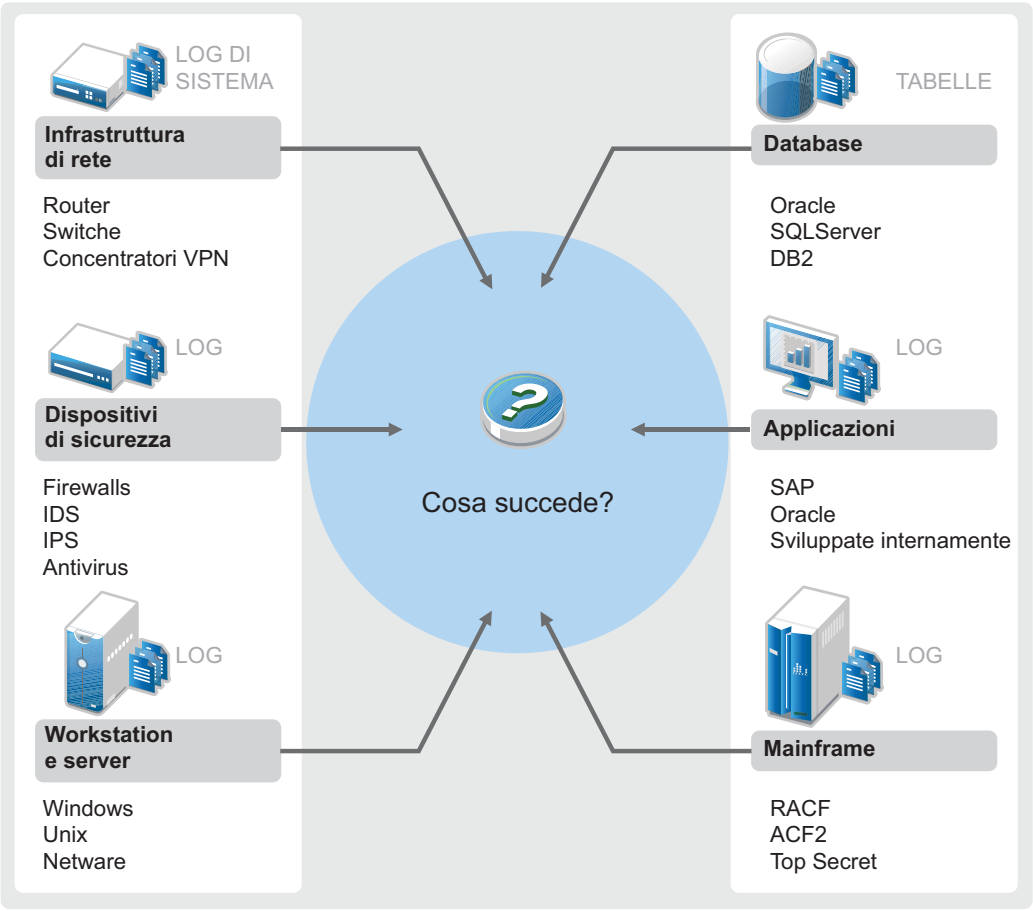
Sentinel è una soluzione SIEM (Security, Information and Event Management) e di monitoraggio della conformità. che monitora automaticamente gli ambienti IT più complessi e garantisce la sicurezza necessaria per proteggerli.



## 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:

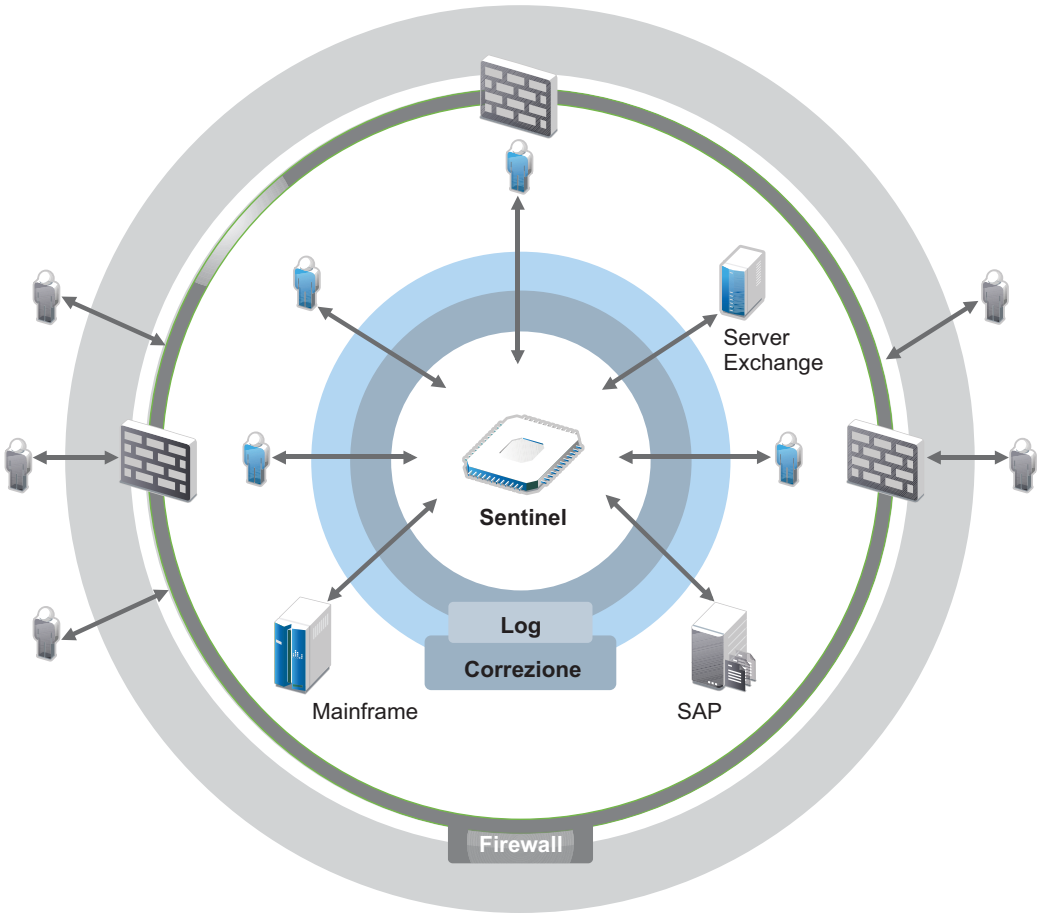
- Raccogliere i dati.
- Consolidare i dati.
- Standardizzazione di dati di tipo diverso in eventi facilmente confrontabili.
- Mappare gli eventi a normative standard.
- Analizzare i dati.
- Confrontare gli eventi di più sistemi per stabilire se sussistono problemi per la sicurezza.
- Inviare notifiche 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

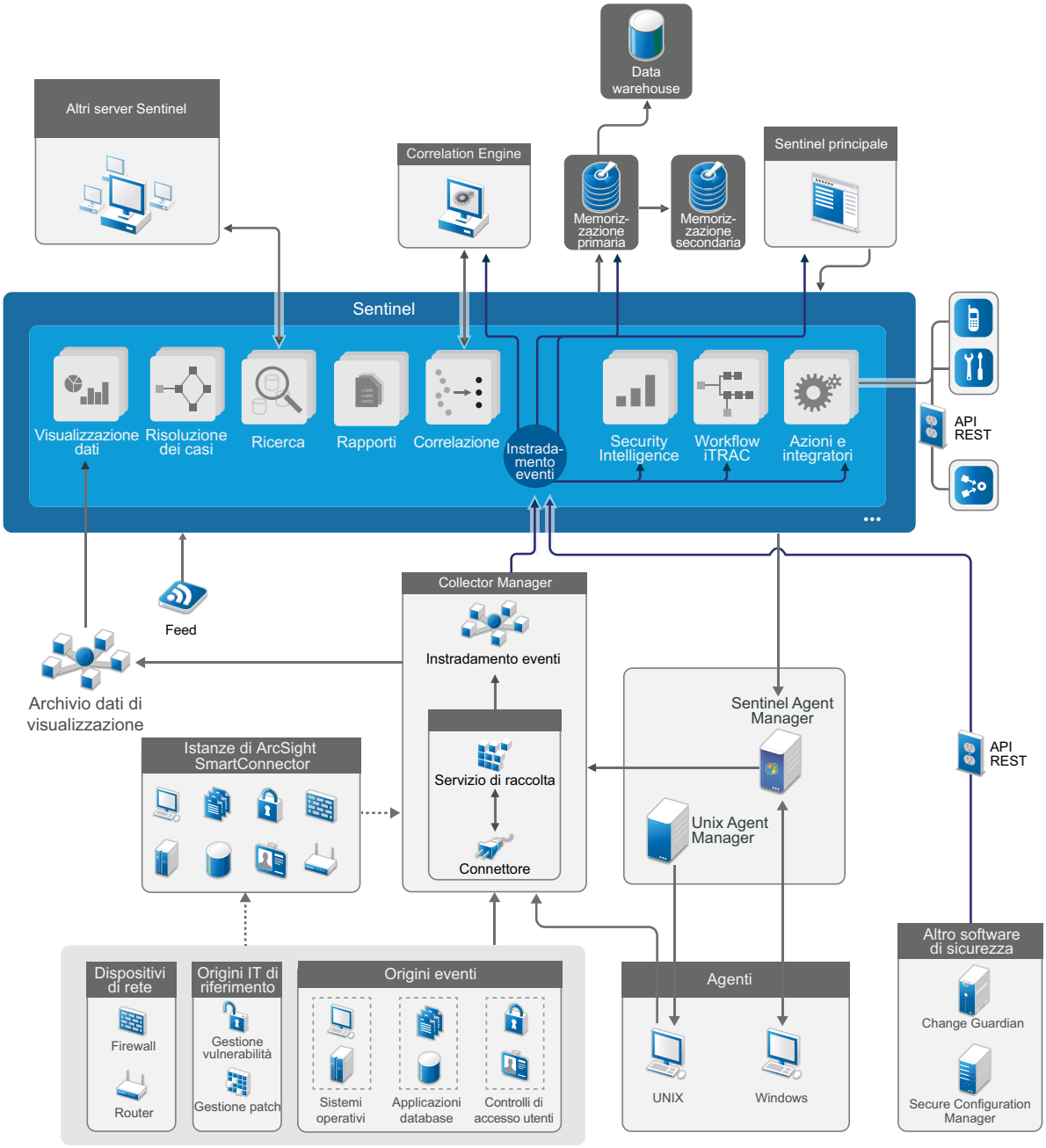
Sentinel gestisce costantemente le informazioni e gli eventi relativi alla sicurezza, sfruttando l'ambiente IT dell'utente per fornire una soluzione di monitoraggio completa.

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 un'unità di memorizzazione dati basata su file, 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 22

# 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 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 23
- “Streaming delle mappe” 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.

# 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, come opzione di memorizzazione dei dati è possibile scegliere di utilizzare la memorizzazione tradizionale basata su file. 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.

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 42.

# 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. Inoltre, adesso le regole di correlazione sono associate all'ID MITRE ATT&CK. Per ulteriori informazioni sulla correlazione, consultare “Correlating Event Data (Correlazione dei dati evento)” nella *Sentinel User Guide* (Guida dell'utente di Sentinel).

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 “Correlating Event Data (Correlazione dei dati evento)” nella *Sentinel User Guide* (Guida dell'utente di Sentinel).

# 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 dell'utente di Sentinel).

# 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 Sentinel).

# 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)” nella *Sentinel User Guide* (Guida dell'utente di Sentinel).

# 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 Sentinel).

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 Sentinel).

# 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 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 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)” nella *Sentinel User Guide* (Guida dell'utente di Sentinel).

# 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 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 la *Sentinel User Guide* (Guida dell'utente di Sentinel).

# 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.

---

**Nota:** Tutti gli host utilizzati per il server Sentinel e i relativi componenti devono essere configurati in un ambiente in grado di risolvere gli indirizzi DNS in modo bidirezionale (da nome host a IP e da IP a nome host).

---

# 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 151.

| ❒ | 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).<br><br>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 65. |
| ❒ | Configurare Sentinel. | Parte IV, “Configurazione di Sentinel,” a pagina 101. |
| ❒ | 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 15, “Installazione di servizi di raccolta e connettori aggiuntivi”, a pagina 97. |

| ❒ | Task | Vedere |
|---|---|---|
| ❒ | Installare istanze aggiuntive di Collector Manager e Correlation Engine in base alle esigenze del proprio ambiente. | Parte III, “Installazione di Sentinel,” a pagina 65. |

# 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<br>◆ Raccolta di dati diversi dagli eventi (dati delle risorse, di vulnerabilità e di identità degli utenti)<br>◆ Mappatura contestuale in linea<br>◆ Memorizzazione degli eventi con policy di permanenza e di non rifiuto<br>◆ Instradamento degli eventi alla memorizzazione tradizionale (interna ed esterna)<br>◆ Ricerche e visualizzazione degli eventi<br>◆ Raccolta, memorizzazione e visualizzazione del flusso IP<br>◆ Generazione di rapporti<br>◆ Abilitazione di FIPS 140-2 (Federal Information Processing Standard Publication 140-2, Standard federale dell'elaborazione delle informazioni, pubblicazione 140-2)<br>◆ Azioni attivate manualmente<br>◆ 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 |
| Correlazione<br>◆ Correlazione di modelli degli eventi in tempo reale<br>◆ Azioni attivate da regole di correlazione<br>◆ Valutazione degli avvisi<br>◆ Visualizzazione degli avvisi | Sì | No |
| Security Intelligence<br>◆ Regole di anomalie<br>◆ Analisi statistica in tempo reale | Sì | No |

# 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.

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 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.

---

**Nota**

- Tutti gli host utilizzati per il server Sentinel e i relativi componenti devono essere configurati in un ambiente in grado di risolvere gli indirizzi DNS in modo bidirezionale (da nome host a IP e da IP a nome host).
- prima di installare Sentinel, verificare che l'ambiente sia protetto e aggiornato con gli aggiornamenti di sicurezza più recenti.

---

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” a pagina 37
- “Ambiente virtuale” a pagina 37


## 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 sui consigli relativi al computer fisico, vedere i Requisiti di sistema per 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

In base alla frequenza degli eventi al secondo (EPS), è possibile scegliere di utilizzare la memorizzazione tradizionale per memorizzare e indicizzare i dati di Sentinel.

***Tabella 6-1*** *Memorizzazione tradizionale*

| **Memorizzazione tradizionale** |
| --- |
| I dati vengono memorizzati di default nella memorizzazione tradizionale basata su file e l'indicizzazione viene eseguita in locale nel server Sentinel.<br><br>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 42.<br><br>È facilmente scalabile in verticale fino a circa 20000 EPS. Per ottenere EPS molto più elevati, è necessario aggiungere ulteriori server Sentinel.<br><br>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.<br><br>I dati vengono contrassegnati in base ai tenant, ma su disco non vengono suddivisi in base a tale criterio.<br><br>La replica dei dati e la disponibilità devono essere eseguite manualmente o tramite costosi meccanismi di memorizzazione, ad esempio dischi SAN. |

# 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 Sentinel).

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 43.

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

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 43. 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 94.

## 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 |
| 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 di Elasticsearch”, a pagina 71.
- **Abilitazione della visualizzazione degli eventi:** la visualizzazione degli eventi è disabilitata di default. Per abilitare la visualizzazione degli eventi, vedere Capitolo 18, “Configurazione di Elasticsearch per la visualizzazione degli eventi”, a pagina 109.
- **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 72.

## 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

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 65.

---

**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 65.

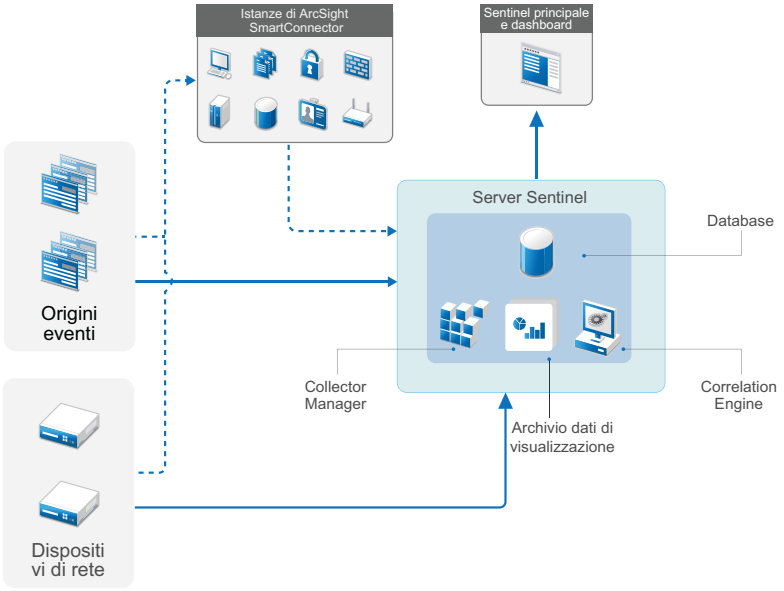
**Nota:** in un sistema è possibile installare una sola istanza di Correlation Engine. Le istanze aggiuntive di Correlation Engine possono essere installate in sistemi remoti e successivamente connesse al server Sentinel.

# 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 6-1*** *Installazione all-in-one*



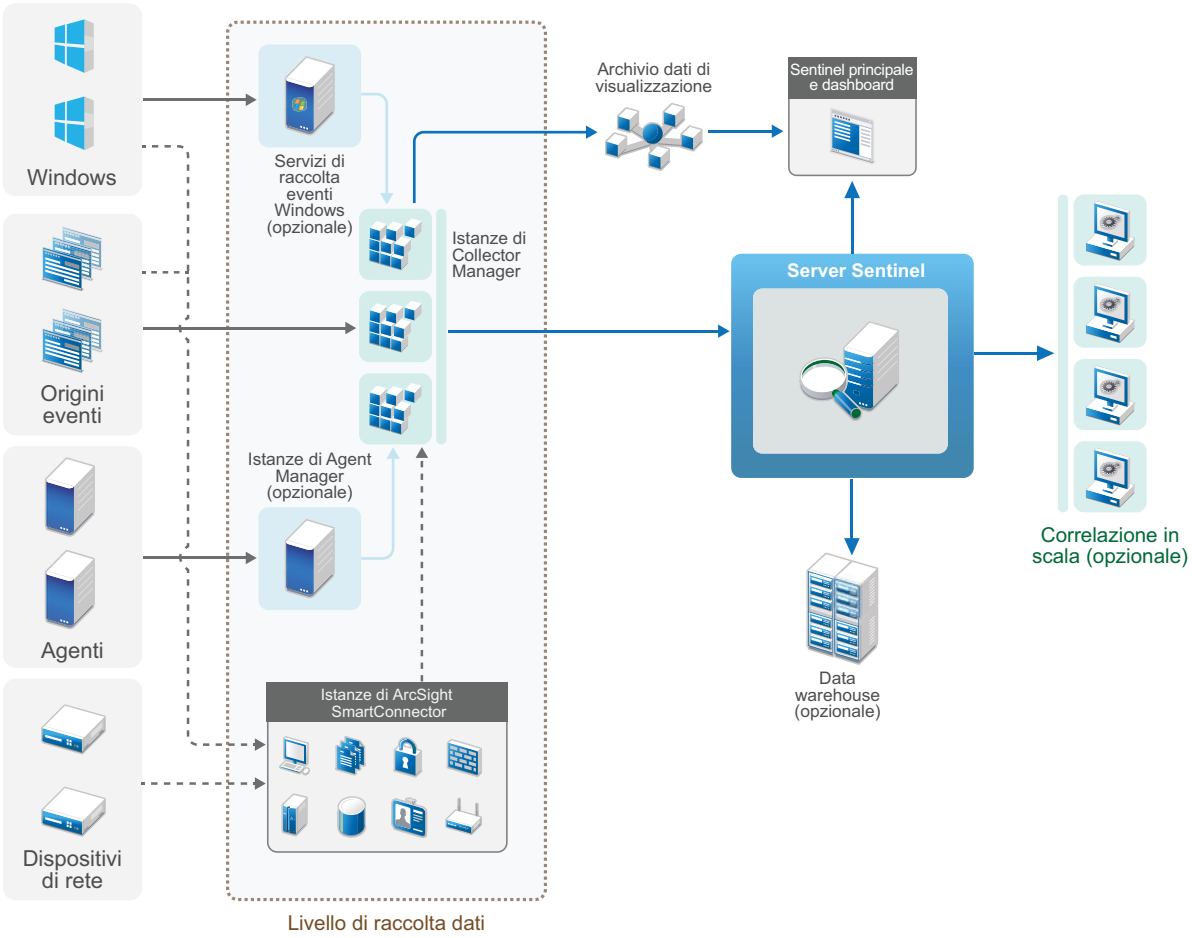

# Installazione distribuita a un livello

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.

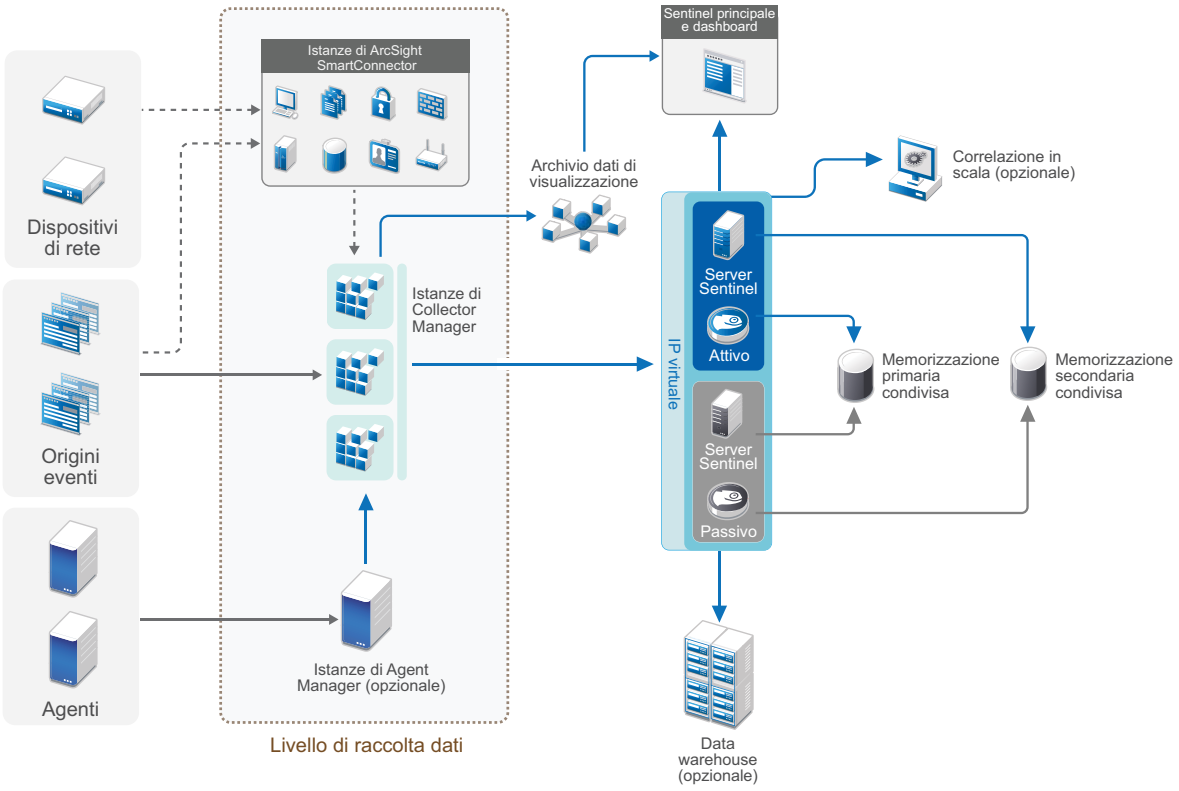
***Figura 6-2*** *Installazione distribuita a un livello*




# 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 203.

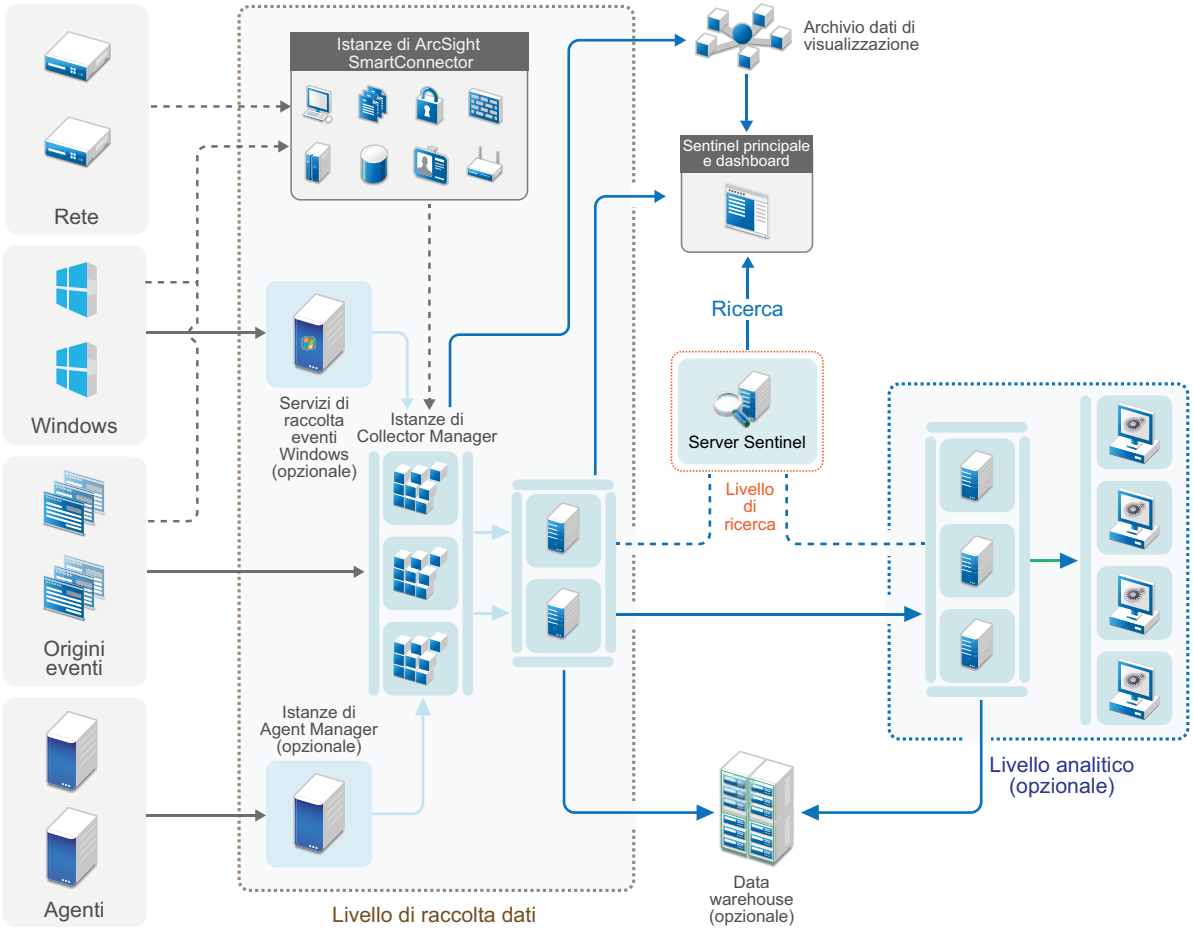
***Figura 6-3*** *Installazione distribuita a un livello con alta disponibilità*




# 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 6-4*** *Installazione distribuita a due e tre livelli*



# 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 e Sentinel Control Center 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 132.

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 139.

- 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 52. |

| 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.<br><br>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 76.<br><br>"Installazione in modalità automatica" a pagina 81<br><br>Capitolo 22, "Abilitazione della modalità FIPS 140-2 in un'installazione esistente di Sentinel", a pagina 125 |
| 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 132. |
| Importare i certificati nell'archivio chiavi FIPS di Sentinel. | "Importazione di certificati nel database di archivio chiavi FIPS" a pagina 139 |

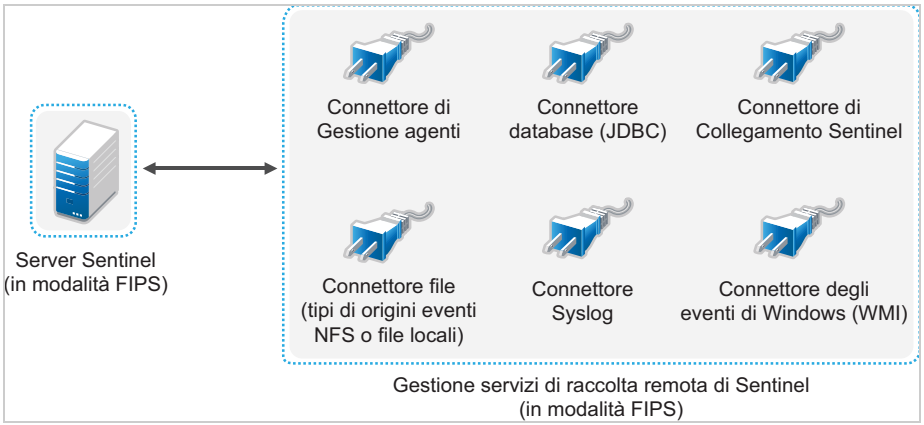
**Nota:** prima di iniziare la conversione alla modalità FIPS, eseguire il backup dei sistemi Sentinel in uso. Se successivamente il server dovrà essere riportato alla modalità non FIPS, l'unica procedura plausibile prevede il ripristino da una copia di backup. Per ulteriori informazioni sul ripristino della modalità non FIPS, vedere "Ripristino di Sentinel nella modalità non FIPS" a pagina 140.

# 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 125.

---

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 127.

---

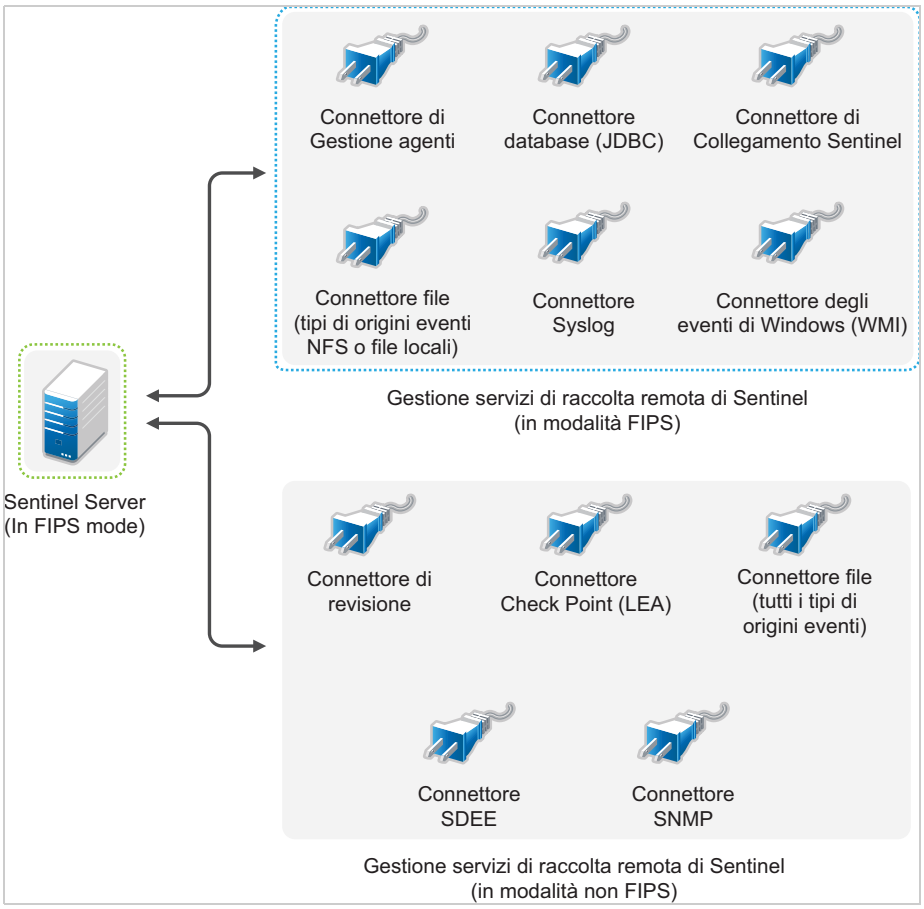
3 Accertarsi che il server FIPS e le istanze remote di Collector Manager comunichino fra di loro.

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 127.

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 132.

## 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 125.

---

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 127.

**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 131.

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 127.

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 132.

   **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). |
| 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 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. |

| Porte | Direzione | Necessaria/ Facoltativa | Descrizione |
|---|---|---|---|
| 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. |
| TCP 7443 | In entrata | Facoltativo | La porta consente a un sistema Sentinel di ricevere gli eventi da altri software SIEM, 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). |

| 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). |
| TCP 7443 | In entrata | Obbligatoria | Utilizzata dal connettore del server HTTP. |

# 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.<br><br>Durante l'installazione e la configurazione di Collector Manager, lasciare aperta questa porta. |
| TCP 7443 | In entrata | Obbligatoria | Utilizzata dal connettore del server HTTP. |

## 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). |
| 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). |
| TCP 7443 | In entrata | Obbligatoria | Utilizzata dal connettore del server HTTP. |

# 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. |

| Porte | Direzione | Necessaria/ Facoltativa | Descrizione |
|---|---|---|---|
| TCP 8443 | In uscita | Obbligatoria | Avvia una connessione con la porta del server Web Sentinel.<br><br>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. |
| 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). |

# 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. |
| 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 75.

- **Modalità automatica:** se si desidera installare più server Sentinel, istanze di Collector Manager o istanze di Correlation Engine nella propria distribuzione, è possibile registrare le opzioni di installazione in un file di configurazione durante l'installazione standard o personalizzata e

utilizzare successivamente 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 81.

# Installazione in modalità applicazione

Con l'installazione in modalità applicazione si installa sia il sistema operativo SLES 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 14, “Installazione in modalità applicazione”, a pagina 87.

# III 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, Security Intelligence, i dati degli avvisi e così via.
- **Elasticsearch:** indicizza eventi e avvisi per la ricerca e la visualizzazione. 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
- **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.
- **Correlation Engine:** elabora gli eventi contenuti nel flusso in tempo reale per stabilire se devono attivare una o più delle regole di correlazione.
- **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 257.
- ❒ 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 57 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).
- ❒ **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. Pertanto, verificare che i pacchetti seguenti siano installati prima di installare Sentinel:
    - `bc`
    - `bash`
    - `coreutils`
    - `gettext`
    - `glibc`
    - `grep`
    - `libgcc`
    - `libstdc`
    - `lsof`
    - `openssl`

- `sed`
- `insserv`
- `net-tools`
- `libX` (per RHEL 7.x)
- `zlib` (fino a SLES 12.x e RHEL 7.x, 8.x)
- `python-libs` (fino a SLES 12.x e RHEL 7.x)
- `netstat` (fino a SLES 12.x e RHEL 7.x) o `ss` (per SLES 15 e versioni successive)
- `pam-modules` (disponibile solo se si installa Legacy-Module su SLES 15.x)

❒ **Per Sentinel con memorizzazione tradizionale:**

Per visualizzare le visualizzazioni degli eventi come utente root, impostare la proprietà `vm.max_map_count=262144` nel file `/etc/sysctl.conf`. Dopo aver aggiunto la proprietà, eseguire `sysctl -p` per applicare le modifiche.

# 12 Installazione 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 i nodi Elasticsearch esterni, completare i prerequisiti seguenti:

- Se sono stati installati i nodi esterni Elasticsearch 5.6.13 con Sentinel 8.3 o versioni precedenti, disinstallare Elasticsearch, quindi installare Elasticsearch 7.7.0. Per ulteriori informazioni sull'installazione, vedere Installazione di Elasticsearch.
- In base alla frequenza EPS, installare Elasticsearch in modalità cluster con il numero di nodi e di repliche consigliato nei Requisiti di sistema per Sentinel.

## Installazione di Elasticsearch

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

**Per installare e configurare Elasticsearch:**

1. Installare la versione di JDK supportata da Elasticsearch.
2. Accertarsi che l'utente Elasticsearch abbia accesso a Java.
3. Effettuare il download della versione certificata dell'RPM di Elasticsearch. Per ulteriori informazioni sulla versione certificata di Elasticsearch e l'URL di download, vedere la pagina dei requisiti di sistema di Sentinel.
4. Installare Elasticsearch:

   ```
   rpm -ivh elasticsearch-<version>.rpm
   ```

5. Eseguire i task specificati nelle istruzioni successive all'installazione di RPM.
6. 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 ricaricare le modifiche apportate ai file.

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 Riavviare Elasticsearch.

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

# 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 `<percorso_di_installazione_di_sentinel>/etc/opt/novell/sentinel/config/elasticsearch-index.properties` e aggiornare le proprietà elencate nella tabella in base alle necessità.

***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. |
| 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. |

| Proprietà | Valore di default | Note |
|---|---|---|
| es.num.shards | 6 | Indica il numero di partizioni primarie per indice.<br><br>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.<br><br>Si consiglia di utilizzare un cluster con un minimo di 2 nodi considerando il failover e l'alta disponibilità. |

# 13 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 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 Per installare Sentinel, specificare il comando seguente nella radice della directory estratta:

   `./install-sentinel`

   oppure

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

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

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

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

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

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

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

7 Specificare 2 per elaborare una configurazione personalizzata di Sentinel.

8 Immettere 1 per utilizzare la chiave della licenza di valutazione di default

oppure

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

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

10 Specificare la password per l'utente del database `dbauser` e confermarla nuovamente.

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

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

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

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

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

oppure

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

Il valore di default è 1.

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

15a 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.

---

15b Inserire i certificati esterni nel database dell'archivio chiavi per stabilire l'attendibilità, premere y e specificare il percorso del file del certificato, quindi aggiungere il percorso del certificato `http` di Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando viene richiesto il certificato esterno.

15c Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel Capitolo 23, “Esecuzione di Sentinel in modalità FIPS 140-2”, a pagina 129.

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.

## 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 "Vantaggi delle installazioni distribuite" a pagina 43.

È possibile installare più di un'istanza di Collector Manager o di Correlation Engine.

---

**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.

---

È possibile registrare i parametri di installazione durante l'installazione interattiva e utilizzare i file registrati per un'installazione automatica su altri sistemi. È possibile specificare i seguenti file per registrare l'installazione:

- <*File_risposta*>: registra i parametri di installazione specificati durante l'installazione.
- <*File_configurazione*>: specificarlo solo se si dispone di più server Sentinel. È possibile utilizzare questo file per connettere l'istanza di Collector Manager e di Correlation Engine a un server Sentinel diverso da quello registrato nel file di risposta. Durante l'installazione interattiva vengono creati i segnaposto per i dettagli del server Sentinel. È possibile aggiornare successivamente il file con i dettagli pertinenti del server Sentinel e utilizzarlo insieme al file di risposta durante l'installazione automatica.

  ---

  **Nota:** questa opzione è disponibile solo in Sentinel 8.2 SP3 o versioni successive.

  ---

**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, effettuare le operazioni seguenti:**

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 (Condizionale) Per eseguire l'installazione senza registrarla, specificare il comando seguente:

- **Per Collector Manager:**

  ```
  ./install-cm
  ```

- **Per Correlation Engine:**

  ```
  ./install-ce
  ```

8 (Condizionale) Per eseguire l'installazione e registrarla, eseguire una delle seguenti operazioni:

- (Condizionale) Se si dispone di un solo server Sentinel, specificare il comando seguente:
  - **Per Collector Manager:**

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

  - **Per Correlation Engine:**

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

- (Condizionale) Se si dispone di più server Sentinel, specificare il comando seguente:
  - **Per Collector Manager:**

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

  - **Per Correlation Engine:**

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

Per ulteriori informazioni sull'utilizzo del file di risposta o del file di configurazione, vedere "Installazione in modalità automatica" a pagina 81.

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 Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.

11 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.

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

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

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

**14a** Il numero di porta del canale di comunicazione del server Sentinel.

**14b** Il numero di porta del server Web Sentinel.

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

Se in modalità FIPS:

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

Se non in modalità FIPS:

```
<sentinel_installation_path>/opt/novell/sentinel/jdk/jre/bin/keytool -
list -keystore
<sentinel_installation_path>/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 13.

---

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

---

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

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

**18** (Condizionale) Se l'Elenco revoche certificati è abilitato nel server, selezionare Sì quando richiesto, quindi effettuare le operazioni seguenti:

**18a** Copiare il certificato da *<CONFIG_HOME>*/config/ del server a *<CONFIG_HOME>*/config/ dell'istanza di Collector Manager o di Correlation Engine. Il valore di default di *<CONFIG_HOME>* è /etc/opt/novell/sentinel.

**18b** Quando richiesto, fare clic su Sì.

**18c** Specificare la password per il certificato del client.

**19** (Condizionale) Se si sceglie la configurazione personalizzata, immettere yes o y per abilitare la modalità FIPS 140-2 in Sentinel, quindi aggiungere il percorso del certificato http di Elasticsearch <percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks quando viene richiesto il certificato esterno.

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

21 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. È possibile registrare i parametri di installazione durante l'installazione interattiva ed eseguire successivamente i file registrati su altri sistemi.

- Accertarsi di aver registrato i parametri di installazione in un file. Per ulteriori informazioni sulla creazione del file di risposta, vedere:
  - "Installazione standard del server Sentinel" a pagina 75
  - "Installazione personalizzata del server Sentinel" a pagina 76
  - "Installazione di Collector Manager e Correlation Engine" a pagina 78.

---

**Nota:** per l'istanza di Collector Manager e di Correlation Engine, uilizzare il file di configurazione per connettere l'istanza di Collector Manager e di Correlation Engine a un server Sentinel diverso rispetto a quello registrato nel file di risposta. Aggiornare il file con i dettagli pertinenti del server Sentinel e utilizzarlo insieme al file di risposta durante l'installazione automatica.

---

**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 un'installazione in modalità automatica:**

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 (Condizionale) Per installare il server Sentinel in modalità automatica, specificare il comando seguente:

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

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) Per installare le istanze di Collector Manager, specificare il comando seguente:

- Per utilizzare il file di risposta:

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

- Per utilizzare il file di risposta e il file di configurazione:

  ```
  ./install-cm -u <response_filename> -i <configuration_filename>
  ```

6 (Condizionale) Per installare le istanze di Correlation Engine, specificare il comando seguente:

- Per utilizzare il file di risposta:

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

- Per utilizzare il file di risposta e il file di configurazione:

  ```
  ./install-ce -u <response_filename> -i <configuration_filename>
  ```

7 (Condizionale) Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nella Capitolo 23, “Esecuzione di Sentinel in modalità FIPS 140-2”, a pagina 129. Aggiungere il percorso del certificato `http` Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando viene richiesto il certificato esterno.

# 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.

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 (Condizionale) Se l'ubicazione della directory non di default specificata è già esistente prima del Passo 4 a pagina 83, assicurarsi che l'utente `novell` disponga delle autorizzazioni di proprietà per la directory. Eseguire il comando seguente per assegnare le autorizzazioni di proprietà:

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

7 Specificare il comando seguente per passare all'utente non root appena creato, vale a dire `novell`:

```
su novell
```

8 (Condizionale) Per eseguire un'installazione interattiva:

**8a** 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` |

**8b** Continuare con il Passo 11.

9 (Condizionale) Per eseguire un'installazione del server Sentinel 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 75 o "Installazione personalizzata del server Sentinel" a pagina 76.

**9a** Per eseguire l'installazione, specificare il comando seguente:

**ubicazione di default:** `./install-sentinel -u <nome_file_risposta>`

**ubicazione diversa da quella di default:** `./install-sentinel --location=/foo -u <nome_file_risposta>`

**9b** Continuare con il Passo 14.

**10** (Condizionale) Per eseguire un'installazione di un'istanza di Collector Manager o di Correlation Engine in modalità automatica, assicurarsi di aver registrato i parametri di installazione in un file.

---

**Nota:** utilizzare il file di configurazione per connettere l'istanza di Collector Manager e di Correlation Engine a un server Sentinel diverso da quello registrato nel file di risposta. Aggiornare il file con i dettagli pertinenti del server Sentinel e utilizzarlo insieme al file di risposta durante l'installazione automatica.

---

Per informazioni sulla creazione del file di risposta o del file di configurazione, vedere "Installazione di Collector Manager e Correlation Engine" a pagina 78.

**10a** Specificare il comando appropriato in base al componente che si sta installando:

| Componente | Comando |
|---|---|
| Collector Manager | ◆ Per utilizzare il file di risposta:<br>◆ **ubicazione di default:** `./install-cm -u <nome_file_risposta>`<br>◆ **ubicazione diversa da quella di default:** `./install-cm --location=/foo -u <nome_file_risposta>`<br>◆ Per utilizzare il file di risposta e il file di configurazione:<br>◆ **ubicazione di default:**<br>`./install-cm -u <nome_file_risposta> -i <nome_file_configurazione>`<br>◆ **ubicazione diversa da quella di default:**<br>`./install-cm --location =/foo -u <nome_file_risposta> -i <file_configurazione>`<br>L'installazione continua con i valori del server Sentinel specificati nel file di configurazione e con gli altri valori dei parametri di installazione memorizzati nel file di risposta. |
| Correlation Engine | ◆ Per utilizzare il file di risposta:<br>◆ **ubicazione di default:** `./install-ce -u <nome_file_risposta>`<br>◆ **ubicazione diversa da quella di default:** `./install-ce --location=/foo -u <nome_file_risposta>`<br>◆ Per utilizzare il file di risposta e il file di configurazione:<br>◆ **ubicazione di default:**<br>`./install-ce -u <nome_file_risposta> -i <nome_file_configurazione>`<br>◆ ubicazione diversa da quella di default:<br>`./install-ce --location =/foo -u <nome_file_risposta> -i <_configurazione>`<br>L'installazione continua con i valori del server Sentinel specificati nel file di configurazione e con gli altri valori dei parametri di installazione memorizzati nel file di risposta. |

**10b** Continuare con la Passo 14.

**11** 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.

**12** 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.

13 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 75.
- Se si sceglie di procedere con la configurazione personalizzata, continuare con Passo 7 mediante Passo 14 in “Installazione personalizzata del server Sentinel” a pagina 76.

14 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.

# 14 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 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.

In base alla versione di Sentinel, il programma di installazione dell'applicazione installa il sistema operativo SLES certificato:

- Per la versione 8.2, il programma di installazione dell'applicazione installa SLES 12 SP3.
- Per la versione 8.2 SP2, il programma di installazione dell'applicazione installa SLES 12 SP4.
- Per la versione 8.3 SP1, il programma di installazione dell'applicazione installa SLES 12 SP5.

L'immagine dell'applicazione Sentinel è racchiusa in un pacchetto in formato ISO oppure OVF che può essere installato negli ambienti virtuali. Per informazioni sulle piattaforme di virtualizzazione supportate, vedere i Requisiti di sistema per 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 installa l'applicazione Sentinel in formato ISO nell'hardware fisico, effettuare il download dell'immagine disco ISO dell'applicazione dal sito del supporto 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 accedere 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 console 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 92.

## 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 88.

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 l'autenticazione forte, è necessario fornire l'ID e il segreto del client Sentinel. Per ulteriori informazioni sui metodi di autenticazione, vedere "Authentication Methods" (Metodi di autenticazione) nella *Sentinel Administration Guide* (Guida all'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 88.

# 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

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 accedere 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 console 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 90.

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 l'autenticazione forte, è necessario fornire l'ID e il segreto del client Sentinel. Per ulteriori informazioni sui metodi di autenticazione, vedere "Authentication Methods" (Metodi di autenticazione) nella *Sentinel Administration Guide* (Guida all'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" a pagina 93
- "Creazione di partizioni per la memorizzazione tradizionale" a pagina 94
- "Configurazione dell'applicazione con SMT" a pagina 95

# 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.

In base al sistema operativo installato, è possibile eseguire la registrazione per gli aggiornamenti nei seguenti modi:

- Se si utilizza SLES 12 SP3 o versioni successive, è possibile eseguire la registrazione per gli aggiornamenti tramite la console di gestione dell'applicazione Sentinel.
- Se si utilizza SLES 12 SP3 o versioni successive, è possibile eseguire la registrazione mediante comandi.


- "Registrazione tramite la console di gestione dell'applicazione Sentinel" a pagina 93
- "Registrazione mediante comandi" a pagina 93


## Registrazione tramite la console di gestione dell'applicazione Sentinel

**Per eseguire la registrazione mediante la console di gestione dell'applicazione Sentinel:**

1. Avviare l'applicazione Sentinel effettuando una delle seguenti operazioni:
   - Eseguire il login a Sentinel e fare clic su **Sentinel Main** > **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

**Per eseguire la registrazione mediante comandi:**

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_emalI>"`

- 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 40. 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 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-8-OS-Updates sle-12-x86_64
smt-repos -e Sentinel-Server-8-Prod-Updates sle-12-x86_64
smt-repos -e Sentinel-Collector-Manager-8-OS-Updates sle-12-x86_64
smt-repos -e Sentinel-Collector-Manager-8-Prod-Updates sle-12-x86_64
smt-repos -e Sentinel-Correlation-Engine-8-OS-Updates sle-12-x86_64
smt-repos -e Sentinel-Correlation-Engine-8-Prod-Updates sle-12-x86_64
```

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

## Esecuzione dell'upgrade dell'applicazione

Per informazioni sull'upgrade dell'applicazione, vedere la “Esecuzione dell'upgrade dell'applicazione Sentinel” a pagina 167.

# 15 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.

# 16 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>`

  ---

  **Nota:** A partire da SLES15 viene utilizzato il seguente comando:

  `ss -tln |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.

  ---

  **Nota:** Per accedere all'interfaccia utente principale di Sentinel, eseguire i passaggi seguenti:

  1. Accedere alla directory `<cartella_di_installazione_di_sentinel>/etc/opt/novell/sentinel/config/`
  2. Abilitare `sentinel.sentinel.redirection` nel file `Configuration.properties` impostandone il valore su `true`.
  3. Riavviare Sentinel: `rcsentinel restart`.
  4. Eseguire il login a Sentinel utilizzando l'URL:

     `https://IP_AddressOrDNS_Sentinel_server:<port>/sentinel/`

  ---

# IV Configurazione di Sentinel

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

# 17 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

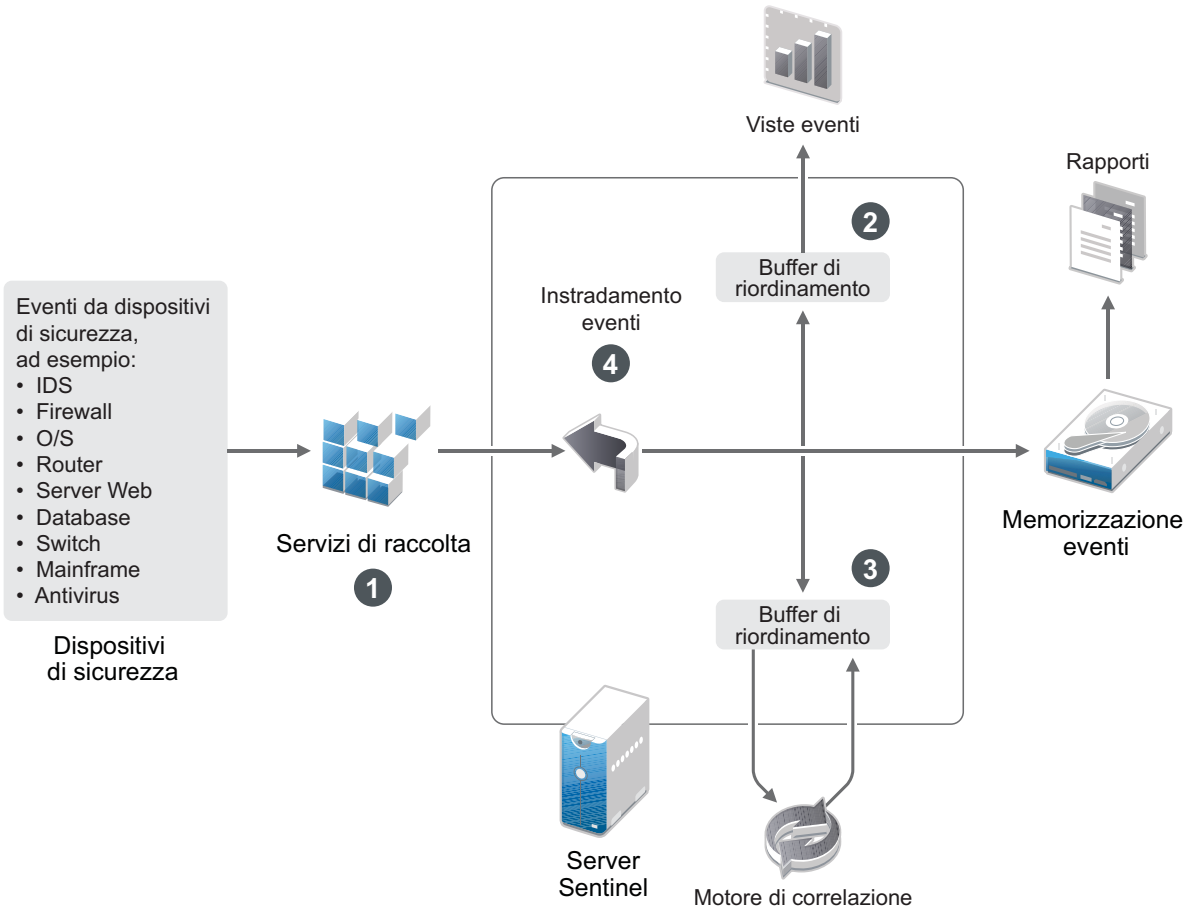
Sentinel è un sistema distribuito e consiste in diversi processi che possono essere realizzati in varie parti della rete. L'origine eventi potrebbe inoltre indurre alcuni ritardi. Per gestire al meglio tale situazione, prima dell'elaborazione i processi di Sentinel riordinano gli eventi in un flusso 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 17-1*** *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 Sentinel).
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.

# 18 Configurazione di Elasticsearch per la visualizzazione degli eventi

Sebbene Elasticsearch richieda una configurazione minima, è necessario prendere in considerazione diverse impostazioni prima di andare in produzione.

---

**Nota:** Nella configurazione del cluster Elasticsearch, in base all'integrità dei nodi, qualsiasi nodo connesso/disponibile per primo viene aggiornato nel file `kibana.yml`. Tale approccio di progettazione consente di ridurre il carico nel nodo del server Sentinel (per ottenere prestazioni migliori). Il file `kibana.yml` viene aggiornato tramite Sentinel in base all'integrità del nodo (che esegue la connessione per primo).

---



## Abilitazione della visualizzazione degli eventi in Sentinel

1 Passare all'utente `novell`:

```
su novell
```

Se la versione java è 292, eseguire i passaggi 2 e 3. Per individuare la versione Java a livello di sistema operativo, eseguire `java -version` dal prompt dei comandi.

2 (Condizionale) Impostare JAVA_HOME al JDK di Sentinel integrato:

```
JAVA_HOME=/opt/novell/sentinel/jdk
```

3 (Condizionale) Impostare PATH per Java all'ubicazione del JDK di Sentinel:

```
PATH=$JAVA_HOME/bin:$PATH
```

4 Generare un'autorità di certificazione (CA) per il cluster nel nodo Sentinel. Eseguire il comando seguente nella home directory di Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

```
./bin/elasticsearch-certutil ca
```

Viene richiesto di specificare il nome file e la password del certificato CA. Il nome file di default è `elastic-stack-ca.p12`.

5 Generare i certificati e le chiavi private per il nodo Elasticsearch preintegrato di Sentinel. A tal scopo, eseguire il comando seguente nella home directory di Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

```
./bin/elasticsearch-certutil cert --ca <CA certificate filename>.p12 --
out config/certs/node-1.p12
```

Viene richiesto di immettere la password per il certificato CA. Viene inoltre richiesto di creare una password per il certificato generato.

6 Aggiungere le seguenti impostazioni al file `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.yml` nel nodo Sentinel:

- `xpack.security.transport.ssl.enabled: true`
- `xpack.security.transport.ssl.keystore.path: certs/node-1.p12`
- `xpack.security.transport.ssl.truststore.path: certs/node-1.p12`
- `xpack.security.transport.ssl.verification_mode: certificate`

7 Memorizzare la password del file del certificato dell'`archivio attendibilità` e dell'`archivio chiavi` generata in precedenza nell'archivio chiavi di Elasticsearch. A tal scopo, eseguire i comandi seguenti nella home directory di Elasticsearch: `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.truststore.secure_password
```

8 Eseguire il login al server Sentinel come utente `novell`.

9 Aprire il file `/etc/opt/novell/sentinel/config/configuration.properties`.

10 (Condizionale) Se si utilizza Sentinel in modalità ad alta disponibilità, verificare che la proprietà `sentinel.ha.cluster` sia impostata su `true` per tutti i nodi del cluster.

11 Impostare `eventvisualization.traditionalstorage.enabled` su `true`.

12 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.

13 (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 35, “Migrazione dei dati in Elasticsearch”, a pagina 199.

---

**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.

---

# Elasticsearch in modalità cluster

1 Completare i passaggi nella sezione “Abilitazione della visualizzazione degli eventi in Sentinel” a pagina 109.

2 Configurare il file `/etc/elasticsearch/elasticsearch.yml` su ciascun nodo Elasticsearch esterno aggiornando o aggiungendo le seguenti informazioni:

| Proprietà e valore | Note |
|---|---|
| discovery.seed_hosts: [<IP del nodo Elasticsearch master idoneo nel cluster>,<IP del nodo Elasticsearch master idoneo nel cluster>,<IP del nodo Elasticsearch master idoneo nel cluster> e così via] | |
| 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_ | Se si utilizza il nome host anziché l'indirizzo IP, assicurarsi che il nome host sia risolvibile da tutti i nodi nel cluster Elasticsearch e dal server Sentinel. |
| thread_pool.write.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.<br>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.<br>Configurare più percorsi per la memorizzazione dei dati di Elasticsearch, ad esempio /es1, /es2 e così via.<br>Per ottimizzare le prestazioni e la gestibilità, montare ciascun percorso in un disco fisico separato (JBOD). |

**3** Ripetere tutti i passaggi precedenti in ciascun nodo Elasticsearch esterno del cluster di Elasticsearch.

4 Nel nodo Elasticsearch del server Sentinel, configurare il file <percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3drparty/elastcisearch/config/elasticsearch.yml come indicato di seguito:

   **4a** Verificare che i valori di cluster.name e discovery.seed_hosts nel file elasticsearch.yml siano gli stessi del file elasticsearch.yml nel nodo Elasticsearch esterno.

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

   Ad esempio:
   ServerList=<*IP1_Elasticsearch*>:<*Porta*>,<*IP2_Elasticsearch*>:<*Porta*>

6 **Abilitazione della comunicazione sicura tra i nodi Elasticsearch esterni e tra Sentinel e il cluster Elasticsearch in presenza di una configurazione del cluster Elasticsearch esterno**

   L'ultima versione di Sentinel consente la comunicazione sicura tra il server Sentinel e il cluster Elasticsearch esterno e tra i diversi nodi del cluster Elasticsearch. In questa sezione viene illustrata la procedura per abilitare tali impostazioni sicure nei casi in cui al server Sentinel sia connesso un cluster Elasticsearch esterno.

   **Passaggi da seguire per proteggere la comunicazione all'interno del cluster tra i nodi Elasticsearch:**

   1. Generare i certificati per tutti i nodi Elasticsearch esterni nel cluster. È possibile creare prima tutti i certificati Elasticsearch esterni nel nodo Sentinel stesso e quindi copiarli nei rispettivi nodi Elasticsearch. A tal scopo, eseguire innanzitutto il comando seguente nella home directory di Elasticsearch <percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch dell'istanza di Sentinel:

      ```
      ./bin/elasticsearch-certutil cert --ca <CA certificate filename>.p12 --out config/certs/newNode.p12
      ```

      Viene richiesto di immettere la password per il certificato CA. Viene inoltre richiesto di creare una password per il certificato generato.

   2. Copiare i certificati nei rispettivi nodi Elasticsearch esterni. Ad esempio, copiare il file newNode.p12 nella directory /etc/elasticsearch/certs/ di newNode del cluster Elasticsearch esterno. Fornire le autorizzazioni di lettura/scrittura ai certificati sui nuovi computer utilizzando il comando chmod.

      **Nota:** Se la directory certs non è presente, è necessario crearla.

   3. Dopo aver generato e copiato i certificati in tutti i nodi Elasticsearch esterni, aggiungere le seguenti impostazioni nel file /etc/elasticsearch/elasticsearch.yml di tutti i nodi Elasticsearch esterni:

      - xpack.security.enabled: true
      - xpack.security.transport.ssl.enabled: true
      - xpack.security.transport.ssl.keystore.path: certs/newNode.p12
      - xpack.security.transport.ssl.truststore.path: certs/newNode.p12
      - xpack.security.transport.ssl.verification_mode: certificate

4. In ciascun nodo Elasticsearch esterno, memorizzare la password per il file del certificato dell'`archivio chiavi` e dell'`archivio attendibilità` generato nell'archivio chiavi di Elasticsearch. A tal scopo, eseguire i comandi seguenti nella home directory di Elasticsearch `/usr/share/elasticsearch` di tutti i nodi Elasticsearch esterni:

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.keystore.secure_password
   ```

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.truststore.secure_password
   ```

**Passaggi da seguire per proteggere le comunicazioni tra Sentinel e il cluster Elasticsearch:**

1. Passare all'utente `novell`:

   ```
   su novell
   ```

2. Eseguire il comando seguente per generare un certificato `http` per un nodo Elasticsearch esterno dal computer Sentinel:

   ```
   <sentinel_installation_path>/opt/novell/sentinel/bin/javacert.sh --
   generateES <provide path where the http certificate should be
   generated, example /opt/http.pks> <http certificate password>
   <keyalias>
   ```

3. Copiare il certificato `http` nel nodo Elasticsearch. Ad esempio, copiare il file `http.pks` nella directory ES_PATH_CONF`/certs/` del nodo Elasticsearch. Fornire le autorizzazioni di lettura/scrittura ai certificati sui nuovi computer.

   **Nota:** Se la directory `certs` non è presente, è necessario crearla.

4. Aggiungere le seguenti impostazioni al file ES_PATH_CONF`/elasticsearch.yml` in tutti i nodi Elasticsearch esterni:
   - `xpack.security.http.ssl.enabled: true`
   - `xpack.security.http.ssl.keystore.path: certs/http.pks`
5. Eseguire il comando seguente nella home directory di Elasticsearch `/usr/share/elasticsearch` di tutti i nodi Elasticsearch esterni per salvare la password del certificato `http` nell'archivio chiavi di Elasticsearch:

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.http.ssl.keystore.secure_password
   ```

**7** Riavviare Sentinel:

```
rcsentinel restart
```

**8** Riavviare tutti i nodi Elasticsearch esterni:

```
/etc/init.d/elasticsearch restart
```

**9** Eseguendo i comandi indicati di seguito, verificare che il cluster Elasticsearch sia stato formato:

```
cd <sentinel_installation_path>/opt/novell/sentinel/bin
```

```
./elasticsearchRestClient.sh <sentinel_ip> <Port used for the
Elasticsearch> GET _cat/nodes
```

10 Assicurarsi che tutti i dati degli avvisi e degli eventi esistenti (se disponibili) siano stati spostati nei nodi Elasticsearch esterni.

11 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:

**11a** Arrestare il nodo interno (server Sentinel)

```
rcsentinel stopES
```

**11b** Impostare i seguenti nodi interni nel file `elasticsearch.yml`:

```
node.master: true
node.data: false
node.ingest: false
```

**11c** Eseguire `elasticsearch-node repurpose` per ripulire tutte le partizioni

```
<sentinel_installation_path>/opt/novell/sentinel/3rdparty/
elasticsearch/bin/elasticsearch-node -v repurpose
```

**11d** Avviare il nodo Elasticsearch interno

```
rcsentinel startES
```

**11e** Riavviare tutti i nodi Elasticsearch esterni:

```
/etc/init.d/elasticsearch restart
```

---

**Importante:** Ogni volta che un nodo Elasticsearch esterno viene arrestato, il cluster Elasticsearch viene riavviato automaticamente e ciò potrebbe causare un problema temporaneo con l'avvio dei dashboard tramite Kibana e la ricerca degli avvisi.

Al riavvio del server Sentinel, assicurarsi di riavviare anche i nodi Elasticsearch esterni.

---

# 19 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`.

# 20 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 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 Administration Guide* (Guida all'amministrazione di Sentinel).

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 la prova dei controlli, consultare "Installing and Managing Solution Packs (Installazione e gestione dei pacchetti soluzione)" nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel).

# 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.

# 21 Implementazione dell'Elenco revoche certificati in un'installazione esistente di Sentinel

### Autenticazione SSL reciproca in Sentinel

Sentinel viene utilizzato per standardizzare i protocolli di sicurezza in reti, server, computer e strutture logiche per migliorare la sicurezza generale.

Sentinel supporta l'Autenticazione SSL reciproca per fornire una cache locale dei dati di revoca implementando la funzione Elenco revoche certificati (CRL, Certificate Revocation List). L'Elenco revoche certificati consente di bloccare un client compromesso anche quando Sentinel non è connesso a Internet per convalidare le credenziali del certificato di un client revocato.

Elenco revoche certificati è un elenco di certificati digitali revocati dall'autorità di certificazione (CA) emittente prima della data di scadenza pianificata e che non devono più essere considerati attendibili. Gli Elenchi revoche certificati rappresentano una black list e vengono utilizzati da vari endpoint, inclusi i browser Web, per verificare la validità e l'affidabilità di un certificato.

In questo capitolo vengono fornite informazioni sui seguenti argomenti:



## Abilitazione della Comunicazione SSL reciproca e dell'Elenco revoche certificati

**Per abilitare la Comunicazione SSL reciproca e l'Elenco revoche certificati nel server Sentinel:**

1. Accedere alla directory <*percorso_di_installazione_di_sentinel*>/opt/novell/sentinel/bin.
2. Eseguire il comando seguente come utente novell:

   ```
   ./createDefaultMutualCert.sh
   ```

3. (Condizionale) Se il certificato viene creato tramite lo script prima della conversione del server in modalità FIPS, effettuare le operazioni seguenti:
   - **3a** Accedere a <*percorso_di_installazione_di_sentinel*>/opt/novell/sentinel/bin/.
   - **3b** Eseguire il comando seguente:

```
./convert_to_fips -i <sentinel_installation_path>
/etc/opt/novell/sentinel/config/
.defaultRestClient.p12
```

**3c** Riavviare Sentinel:

```
rcsentinel restart
```

**4** Accedere alla directory <*percorso_di_installazione_di_sentinel*>/opt/novell/sentinel/setup in Collector Manager e Correlation Engine.

**5** Eseguire il comando seguente e seguire le istruzioni visualizzate per rendere Collector Manager e Correlation Engine compatibili con il server Sentinel:

```
./configure.sh
```

---

**Nota:** Se Collector Manager e Correlation Engine sono in modalità Elenco revoche certificati e non sono in grado di connettersi al server, eseguire l'upgrade della **versione cURL** sul computer alla versione 7.60 o successiva.

---

# Creazione e importazione di un certificato personalizzato

**Per creare e importare un certificato personalizzato:**

**1** Creare la chiave pubblica e privata utilizzando il comando seguente:

```
openssl req -new -text -out <public_key_name> -keyout
<private_key_name>
```

**2** Creare un certificato X.509 autofirmato utilizzando il comando seguente:

```
openssl req -x509 -days 365 -in
 <public_key_name> -text -key
 <private_key_name> -out
 <certificate_name>
```

**3** Importare il certificato generato nell'archivio chiavi di Sentinel:

```
<sentinel_installation_path>
/opt/novell/sentinel/bin/javacert.sh --import
 <sentinel_installation_path>
/etc/opt/novell/sentinel/config/.webserverkeystore.jks
 <password of the keystore>  <alias_name> <certificate_name>
```

**4** Convertire il certificato generato nel formato p12:

```
openssl pkcs12 -inkey <private_key_name>  -in <certificate_name> -
export -out <certificate_name.p12>
```

**5** Per visualizzare l'elenco dei certificati importati nell'archivio chiavi, eseguire il comando seguente:

```
<sentinel_installation_path>
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.webserverkeystore.jks
```

**6** Riavviare il server Sentinel.

# Avvio di Sentinel tramite Comunicazione SSL reciproca

**Per avviare Sentinel tramite la Comunicazione SSL reciproca:**

1. Effettuare il download del file del certificato .defaultRestClient.p12 creato in "Abilitazione della Comunicazione SSL reciproca e dell'Elenco revoche certificati" a pagina 119.

   È anche possibile utilizzare un certificato personalizzato. Per ulteriori informazioni sulla creazione di un certificato personalizzato, vedere "Creazione e importazione di un certificato personalizzato" a pagina 120.
2. Importare il certificato<*nome_certificato.p12*> nel browser dell'applicazione client.
3. Ricaricare il browser dell'applicazione client.
4. Per avviare Sentinel, utilizzare il seguente URL:

   `https://<indirizzo_ip_di_sentinel>:<porta_di_sentinel>`
5. Selezionare il certificato importato nel passaggio precedente, quindi fare clic su **OK**.

# Revoca del certificato e aggiunta all'Elenco revoche certificati

**Per revocare il certificato e aggiungerlo all'Elenco revoche certificati:**

1. Creare una directory per l'Elenco revoche certificati:

   `mkdir /etc/<CRL_directory>`
2. Passare alla directory creata:

   `cd /etc/<CRL_directory>`
3. Creare il file di indice per l'Elenco revoche certificati:

   `touch index.txt`
4. Creare un file di numero Elenco revoche certificati temporaneo:

   `echo 00 > pulp_crl_number`
5. Modificare il file `openssl.cnf` presente nella directory `/etc/ssl/` (su SLES) o `/etc/pki/tls/` (su RHEL).

   ---

   **Nota:** Se il percorso del file non è noto, eseguire il comando `openssl version -a | grep OPENSSLDIR` per individuare la directory contenente il file `openssl.cnf`.

   ---

   `database = /etc/<CRL_directory>/index.txt`

   `crlnumber = /etc/<CRL_directory>/pulp_crl_number`

   (Facoltativo) È possibile creare un file di configurazione personalizzato con la configurazione necessaria per l'Elenco revoche certificati.
6. Convertire il certificato da revocare in formato `crt`:

```
openssl pkcs12 -in <certificate in p12 format> -clcerts -nokeys -out
<certificate_name.crt>
```

7 Revocare il certificato:

```
openssl ca -revoke <certificate_name.crt>
-keyfile <private_key> -cert
<X.509 certificate>
```

8 Generare il file Elenco revoche certificati per il certificato revocato:

```
openssl ca -gencrl -keyfile <private_key>
-cert <X.509 certificate> -out /etc/
<CRL_directory>/crl.pem
```

9 Aggiungere il certificato revocato al file Elenco revoche certificati esistente:

**9a** Eseguire il comando seguente:

```
cat <sentinel_installation_path>/etc/opt/
novell/sentinel/config/<Sentinel CRL File Name>
/etc/<CRL_directory>/
crl.pem > temp.pem
```

**9b** Eseguire il comando seguente:

```
mv temp.pem <sentinel_installation_path>/etc/opt/
novell/sentinel/config/<Sentinel CRL File Name>
```

È possibile fare riferimento al <Nome file Elenco revoche certificati di Sentinel> dalla chiave `sentinel.webserver.crlfile` della proprietà, disponibile in <percorso_di_installazione_di_sentinel>/etc/opt/novell/sentinel/config/configuration.properties

10 (Condizionale) Se sono presenti più certificati da revocare, ripetere i passaggi da 6 a 9 per ciascuno di essi.

11 Riavviare il server Sentinel.

# Disabilitazione della funzione Elenco revoche certificati

**Per disabilitare la funzione Elenco revoche certificati:**

1 Passare alla directory:

```
<sentinel_installation_path>/etc/opt/novell/sentinel/3rdparty/jetty
```

2 Eseguire il comando seguente:

```
mv jetty-ssl-context.xml.crl.bkp jetty-ssl-context.xml
```

3 Nel file <percorso_di_installazione_di_sentinel>/etc/opt/novell/sentinel/config/configuration.properties, rimuovere le seguenti proprietà:

- `sentinel.client.cert.password=<cert.password>`
- `sentinel.validate.crl=true`
- `sentinel.webserver.crlfile=/config/pulp_crl.pem`

4 Riavviare il server Sentinel.

```
rcsentinel restart
```

5 Accedere alla directory <*percorso_di_installazione_di_sentinel*>/opt/novell/sentinel/setup in Collector Manager e Correlation Engine.

6 Eseguire il comando seguente e seguire le istruzioni visualizzate per rendere Collector Manager e Correlation Engine compatibili con il server Sentinel:

```
./configure.sh
```

---

**Nota:** Se Collector Manager e Correlation Engine sono in modalità Elenco revoche certificati e non sono in grado di connettersi al server, eseguire l'upgrade della **versione cURL** sul computer alla versione 7.60 o successiva.

---

# 22 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.

   Aggiungere il percorso del certificato `http` Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando viene richiesto il certificato esterno.

   (Condizionale) Se Elasticsearch è in modalità cluster, copiare nel server Sentinel tutti i certificati `http` dei nodi Elasticsearch esterni creati nella sezione "Impostazioni in Elasticsearch per la comunicazione cluster sicura" a pagina 184. Aggiungere il percorso del certificato `http` Elasticsearch copiato in precedenza `<percorso_dei_certificati_copiati_in_precedenza>//<nome_certificati>` quando viene richiesto il certificato esterno. Ripetere questo passaggio per assicurarsi che siano stati aggiunti tutti i certificati Elasticsearch esterni.

   (Condizionale) Se si utilizza la funzione Elenco revoche certificati, aggiungere il percorso del certificato del client `<percorso_di_installazione_di_sentinel>/etc/opt/novell/sentinel/config/.defaultRestClient.p12` quando viene richiesto il certificato esterno.

È possibile utilizzare il certificato del client di default (.defaultRestClient.p12) o un certificato personalizzato. Per ulteriori informazioni sulla creazione di un certificato personalizzato, vedere “Creazione e importazione di un certificato personalizzato” a pagina 120.

5 (Condizionale) Se nell'ambiente viene utilizzata l'autenticazione a più fattori o l'autenticazione forte:

**5a** Eseguire lo script `create_mfa_fips_keys.sh` e seguire le istruzioni visualizzate.

**Nota:** Lo script richiede la password per il database nss.

**5b** Fornire l'ID e il segreto del client Sentinel. Per ulteriori informazioni sui metodi di autenticazione, vedere “Authentication Methods” (Metodi di autenticazione) nella Sentinel Administration Guide (Guida all'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 Riavviare il server Sentinel.

7 Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel Capitolo 23, “Esecuzione di Sentinel in modalità FIPS 140-2”, a pagina 129.

# Abilitazione della modalità FIPS nell'applicazione tradizionale/Sentinel ad alta disponibilità

1 Nel nodo attivo:

**1a** Completare i passaggi riportati nella sezione “Abilitazione dell'esecuzione in modalità FIPS 140-2 nel server Sentinel” a pagina 125.

**1b** Eseguire il comando seguente per sincronizzare le proprietà di configurazione in tutti i nodi passivi:

- `csync2 -x -v`

**1c** Assicurarsi che la cartella sia sincronizzata con tutti i nodi passivi:

- `/etc/opt/novell/sentinel/3rdparty/nss`

**1d** (Condizionale) Se la cartella `/etc/opt/novell/sentinel/3rdparty/nss` non è sincronizzata, copiare tale cartella manualmente dal nodo attivo a ciascuno dei nodi passivi del cluster:

- `scp -pr /etc/opt/novell/sentinel/3rdparty/nss <ip o nome del nodo passivo>:/etc/opt/novell/sentinel/3rdparty/`

2 Nel nodo passivo:

2a Assicurarsi che la cartella `nss` disponga dell'autorizzazione dell'utente `novell` sul nodo passivo:

2a1 Eseguire il login al nodo passivo.

2a2 Modificare la proprietà della cartella in utente `novell`:

- `chown –R novell:novell /etc/opt/novell/sentinel/3rdparty/nss`

2a3 Impostare l'autorizzazione appropriata per la cartella:

- `chmod –R 600 /etc/opt/novell/sentinel/3rdparty/nss`

2b Ripetere il passaggio 2a su tutti i nodi passivi del cluster.

2c Eseguire ripetutamente il comando seguente dal nodo attivo per assicurarsi che tutti i file correlati a FIPS siano aggiornati su tutti i nodi passivi:

- `csync2 –x –v`

# 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.

Copiare il certificato `http` Elasticsearch interno (`<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` nel server Sentinel) generato durante l'installazione di Sentinel e aggiungere il percorso del certificato `http` di Elasticsearch copiato in precedenza `<percorso del certificato copiato in precedenza>/<nome di certificato>` quando viene richiesto il certificato esterno.

(Condizionale) Se Elasticsearch è in modalità cluster, copiare nell'istanza remota di Collector Manager tutti i certificati `http` dei nodi Elasticsearch esterni creati nella sezione Impostazioni in Elasticsearch per la comunicazione cluster sicura. Aggiungere il percorso del certificato `http` Elasticsearch copiato in precedenza `<percorso_dei_certificati_copiati_in_precedenza>//<nome_certificati>` quando viene richiesto il certificato esterno. Ripetere questo passaggio per assicurarsi che siano stati aggiunti tutti i certificati Elasticsearch esterni.

5 Riavviare Collector Manager oppure Correlation Engine.

6 Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel Capitolo 23, “Esecuzione di Sentinel in modalità FIPS 140-2”, a pagina 129.

# 23 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 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 139.
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 139.

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 139.

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 139.

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 139.

---

**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 139.

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 139.

**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 139.

   **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 139.

   **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 139.

## 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 139.

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 139.

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 65.

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 8.5.

---

# 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 140
- "Ripristino della modalità non FIPS in istanze remote di Collector Manager o di Correlation Engine" a pagina 141


## 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.

# 24 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. Spostarsi in `<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.

---

# 25 Limitazione del numero di sessioni attive simultanee

In Sentinel 8.2 SP3 o versioni successive, è possibile limitare il numero di sessioni attive simultanee che si desidera concedere all'utente, al tenant o a entrambi. In caso di attacco, la limitazione del numero di sessioni impedisce agli utenti malintenzionati di avviare sessioni oltre il limite consentito.

Se si limitano le sessioni per utente e tenant, gli utenti non saranno in grado di avviare ulteriori sessioni una volta che il numero totale di sessioni avviate da più utenti raggiunge il limite consentito per il tenant.

Per default, Sentinel non limita le sessioni simultanee. È necessario configurare manualmente tale limite.

---

**Nota:** questa funzione è disponibile solo in modalità non MFA.

---

**Per limitare il numero di sessioni attive simultanee:**

1. Eseguire il login al server Sentinel.
2. Aprire il file `/<percorso_di_installazione_di_sentinel>/etc/opt/novell/sentinel/config/configuration.properties`.
3. (Condizionale) Per configurare il limite per tenant, impostare la proprietà `concurrent.overall.sessions` al valore desiderato.
4. (Condizionale) Per configurare il limite per utente, impostare la proprietà `concurrent.per.user.sessions` al valore desiderato.
5. Salvare il file.
6. Riavviare il server Sentinel.

# 26 Chiusura delle sessioni inattive

In Sentinel 8.2 SP3 o versioni successive, è possibile configurare Sentinel in modo da terminare una sessione in assenza di attività da parte dell'utente per un periodo di tempo specificato. Sentinel visualizza un messaggio di avviso un minuto prima della fine della durata specificata. Se un utente mantiene una sessione inattiva per tale durata, Sentinel esegue il logout dell'utente dalla sessione.

Per default, Sentinel non tiene traccia dell'inattività dell'utente. È necessario configurare manualmente Sentinel per terminare le sessioni inattive.

**Per impostare il periodo di timeout di inattività:**

1. Eseguire il login al server Sentinel.
2. Aprire il file `/<percorso_di_installazione_di_sentinel>etc/opt/novell/sentinel/config/ui-configuration.properties`.
3. Impostare il valore desiderato per la proprietà `user.inactivity.time` in millisecondi.
4. Aggiornare il browser mediante il quale è stato eseguito il login a Sentinel.

# 27 Configurazione della raccolta dati del flusso IP

Sentinel si avvale delle istanze di ArcSight SmartConnector che consentono di controllare la rete aziendale tramite la raccolta dati del flusso IP. 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.
- 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.

Per configurare la raccolta dati del flusso IP, è necessario 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.

# V Esecuzione dell'upgrade di Sentinel

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

**Importante**

- Dopo aver eseguito l'upgrade da Sentinel 8.3 o versioni precedenti a Sentinel 8.4, i dashboard personalizzati Kibana esistenti non verranno visualizzati. Assicurarsi di aver ricreato il dashboard personalizzato dopo aver eseguito l'upgrade a Sentinel 8.4.
- Se il parametro Imposta alla scadenza non è stato impostato sulle partizioni prima dell'upgrade, l'opzione non può essere impostata sulla partizione ripristinata dopo l'upgrade a Sentinel 8.4.
- Dopo aver eseguito l'upgrade a Sentinel 8.4 da una versione precedente a Sentinel 8.3.1, poiché l'upgrade aggiorna anche i formati di dati sottostanti, i dati degli eventi esistenti non saranno disponibili per le operazioni di Sentinel quali le funzionalità di ricerca o di creazione di rapporti. Per abilitare la ricerca dei dati, dopo l'upgrade è necessario indicizzare nuovamente tutte le partizioni dei dati degli eventi nel sistema. Per ulteriori informazioni, vedere Re-indexing Event Data Partitions (Reindicizzazione delle partizioni dei dati degli eventi) nella Sentinel Administration Guide (Guida all'amministrazione di Sentinel).
- Quando si esegue l'upgrade del server Sentinel, assicurarsi di eseguire l'upgrade dei sistemi Collector Manager e Correlation Engine, del server Sentinel di destinazione nell'integratore di Collegamento Sentinel e del server Sentinel di destinazione nell'integratore Syslog alla stessa versione del server Sentinel. In caso contrario, potrebbero verificarsi dei problemi nel sistema.

# 28 Elenco di controllo per l'implementazione

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

***Tabella 28-1*** *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. | Note di rilascio di Sentinel 8.5 |
| ❒ | 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 29, “Prerequisiti”, a pagina 155 |

# 29 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

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. 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 Sentinel).

# 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.

# 30 Upgrade dell'installazione tradizionale di Sentinel

Le procedure descritte in questo capitolo illustrano come eseguire l'upgrade di Sentinel.

È possibile eseguire l'upgrade da Sentinel 8.2 o versioni successive.

---

**Importante:** Se si esegue l'upgrade da versioni precedenti di Sentinel 8.3.0.0, i passaggi seguenti sono applicabili.

---

**Importante:** Quando si esegue l'upgrade del server Sentinel, assicurarsi di eseguire l'upgrade dei sistemi Collector Manager e Correlation Engine alla stessa versione del server Sentinel. In caso contrario, potrebbero verificarsi dei problemi nel sistema.

---

Il processo di upgrade esegue le seguenti operazioni:

- Esegue la migrazione dei dati di Security Intelligence e degli avvisi da MongoDB a PostgreSQL.

  Ora Sentinel memorizza i dati di Security Intelligence, degli avvisi e così via in PostgreSQL anziché in MongoDB. Il processo di upgrade eseguirà la migrazione dei dati a PostgreSQL e, in caso di esito positivo, proseguirà automaticamente con il processo di upgrade. Se la migrazione dei dati ha esito negativo, non sarà possibile eseguire l'upgrade di Sentinel.
- Genera uno script di pulizia che è possibile utilizzare per rimuovere i dati e gli RPM relativi a MongoDB.
- I dati memorizzati in MongoDB vengono conservati come backup.


- “Esecuzione dell'upgrade di Sentinel” a pagina 157
- “Upgrade di Sentinel come utente non root” a pagina 159
- “Upgrade di Collector Manager o di Correlation Engine” a pagina 161
- “Upgrade del sistema operativo” a pagina 162


## Esecuzione dell'upgrade di Sentinel

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

**Per eseguire l'upgrade del server Sentinel:**

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 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, vedere "Maintaining Custom Settings in XML Files" (Conservazione delle impostazioni personalizzate nei file XML) nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel).

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 all'ubicazione estratta del programma di installazione, ad esempio:

```
cd /opt/sentinel_server-<version>*
```

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 **Importante:** Se si esegue l'upgrade da versioni precedenti di Sentinel 8.3.0.0, i passaggi seguenti sono applicabili.

---

**10a** (Condizionale) Selezionare l'opzione di migrazione richiesta. Esegue la migrazione dei dati di Security Intelligence e degli avvisi da MongoDB a PostgreSQL.

Se si seleziona l'opzione **Only upgrade without migrating data** (Esegui solo upgrade senza migrare i dati), il server Sentinel dovrebbe essere attivo e in esecuzione.

---

**Avviso:** Accertarsi di selezionare l'opzione appropriata poiché non è possibile ripetere la procedura dopo il completamento del processo di upgrade.

---

Se la migrazione dei dati ha esito positivo, i dati memorizzati in MongoDB vengono conservati come backup e il processo di upgrade di Sentinel procede automaticamente.

Il completamento dell'upgrade potrebbe richiedere alcuni minuti.

**10b** (Condizionale) Se la migrazione dei dati non viene eseguita correttamente:

**10b1** Ripulire i dati di cui è stata eseguita la migrazione parziale. Per ulteriori informazioni, vedere "Pulizia dei dati da PostgreSQL in caso di errore di migrazione" a pagina 179.

**10b2** Ripetere dal Passo 7 al Passo 10 riportati in precedenza fino a eseguire l'upgrade di Sentinel.

11 (Condizionale) Prima dell'upgrade, se è abilitata la visualizzazione degli eventi, dopo aver eseguito l'upgrade a Sentinel 8.4.0.0, Elasticsearch viene arrestato poiché viene abilitato con il plug-in di sicurezza X-Pack; per avviare Elasticsearch, attenersi alla procedura descritta in "Impostazioni in Elasticsearch per la comunicazione cluster sicura" a pagina 184.

12 Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.

13 (Condizionale) Se il file `delete_old_cluster.sh` si trova nella cartella bin (`/opt/novell/sentinel/3rdparty/postgresql/bin`), vuol dire che è stato eseguito l'upgrade del database PostgreSQL a una versione principale (ad esempio, da 8.0 a 9.0). Eliminare i vecchi file PostgreSQL dal database PostgreSQL. Il percorso della cartella potrebbe essere diverso nel caso di installazioni in percorsi personalizzati.

Per cancellare i vecchi file PostgreSQL:

**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 Eseguire il login a Sentinel e verificare i dati migrati, ad esempio avvisi, dati di Security Intelligence e così via.

15 Ora i dati in MongoDB sono ridondanti poiché Sentinel 8.3 e versioni successive memorizzerà i dati solo in PostgreSQL. Per liberare spazio su disco, eliminare i dati. Per ulteriori informazioni, consultare “Rimozione dei dati da MongoDB” a pagina 183.

16 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 161.

# 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 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 Sentinel).

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.

- Passare all'ubicazione estratta del programma di installazione, ad esempio:

  ```
  cd /opt/sentinel_server-8.4.0.0*
  ```

6 Estrarre l'RPM `squashfs` dai file di installazione di Sentinel.

7 Installare `squashfs` nel server Sentinel.

```
rpm -Uvh <install_filename>
```

8 Passare all'utente `novell`:

```
su novell
```

9 (Condizionale) Per eseguire un upgrade interattivo:

**9a** Accedere alla directory di installazione di Sentinel ed eseguire il comando seguente:

```
./bin/root_install_prepare
```

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 il 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.

---

13 **Importante:** Se si esegue l'upgrade da versioni precedenti di Sentinel 8.3.0.0, i passaggi seguenti sono applicabili.

---

**13a** (Condizionale) Selezionare l'opzione di migrazione. Esegue la migrazione dei dati di Security Intelligence e degli avvisi da MongoDB a PostgreSQL.

---

**Avviso:** Accertarsi di selezionare l'opzione appropriata poiché non è possibile ripetere la procedura dopo il completamento del processo di upgrade.

---

Se la migrazione dei dati ha esito positivo, i dati memorizzati in MongoDB vengono conservati come backup e il processo di upgrade di Sentinel procede automaticamente.

Il completamento dell'upgrade potrebbe richiedere alcuni minuti.

**13b** (Condizionale) Se la migrazione dei dati non viene eseguita correttamente:

**13b1** Ripulire i dati di cui è stata eseguita la migrazione. Per ulteriori informazioni, vedere "Pulizia dei dati da PostgreSQL in caso di errore di migrazione" a pagina 179.

**13b2** Ripetere dal Passo 7 al Passo 13 riportati in precedenza fino a eseguire l'upgrade di Sentinel.

**14** (Condizionale) Prima dell'upgrade, se è abilitata la visualizzazione degli eventi, dopo aver eseguito l'upgrade a Sentinel 8.4.0.0, Elasticsearch viene arrestato poiché viene abilitato con il plug-in di sicurezza X-Pack; per avviare Elasticsearch, attenersi alla procedura descritta in "Impostazioni in Elasticsearch per la comunicazione cluster sicura" a pagina 184.

**15** Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.

**16** (Condizionale) Se il file `delete_old_cluster.sh` si trova nella cartella bin (`/opt/novell/sentinel/3rdparty/postgresql/bin`), vuol dire che è stato eseguito l'upgrade del database PostgreSQL a una versione principale (ad esempio, da 8.0 a 9.0). Eliminare i vecchi file PostgreSQL dal database PostgreSQL. Il percorso della cartella potrebbe essere diverso nel caso di installazioni in percorsi personalizzati.

Per cancellare i vecchi file PostgreSQL:

**16a** Passare all'utente novell.

```
su novell
```

**16b** Passare alla cartella `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

**16c** Cancellare i vecchi file PostgreSQL utilizzando il comando seguente:

```
./delete_old_cluster.sh
```

**17** Eseguire il login a Sentinel e verificare i dati migrati, ad esempio avvisi, dati di Security Intelligence e così via.

**18** Ora i dati in MongoDB sono ridondanti poiché Sentinel 8.3 e versioni successive memorizzerà i dati solo in PostgreSQL. Per liberare spazio su disco, eliminare i dati. Per ulteriori informazioni, consultare "Rimozione dei dati da MongoDB" a pagina 183.

# 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 Sentinel).

**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. Prima di eseguire l'upgrade di Sentinel, assicurarsi di fare riferimento ai requisiti di sistema per la compatibilità. Per informazioni, vedere Requisiti di sistema di Sentinel.

**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 Come utente root, impostare la proprietà `vm.max_map_count=262144` nel file `/etc/sysctl.conf`. Dopo aver aggiunto la proprietà, eseguire `sysctl -p` per applicare le modifiche.

7 (Condizionale) Durante il processo di upgrade a SLES 15 SP1 o SLES 15 SP2, viene visualizzato il seguente avviso:

```
avviso: versione non supportata della chiave: V3
```

È possibile ignorare l'avviso o adottare una soluzione alternativa per evitare che l'avviso venga visualizzato. Per ulteriori informazioni sulla soluzione alternativa, consultare la documentazione di SLES.

8 (Condizionale) Se si utilizza Mozilla Network Security Services (NSS), due file RPM dipendenti, `libfreebl3 hmac` e `libsoftokn3 hmac`, non vengono installati. Installare manualmente i seguenti file RPM: `libfreebl3 hmac` e `libsoftokn3 hmac`.

9 (Condizionale) Se si esegue l'upgrade da SLES12SP4 a SLES15SP1 o SLES15SP2 in modalità FIPS, è necessario innanzitutto eseguire l'upgrade del sistema operativo SLES, applicare le patch più recenti del sistema operativo, quindi avviare Sentinel.

10 (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`

**10a** Se vengono rilevati errori, eseguire il comando seguente per risolverli:

```
rpm --rebuilddb --dbpath <ubicazione_installazione>/rpm
```

Esempio: `# rpm --rebuilddb --dbpath /custom/rpm`

**10b** Eseguire il comando indicato al passaggio 7 per verificare che non siano presenti errori.

11 Ripetere la procedura per i componenti seguenti:

- Istanze di Collector Manager
- Istanze di Correlation Engine

12 Riavviare il servizio Sentinel:

```
rcsentinel restart
```

Questo passaggio non è valido per Sentinel ad alta disponibilità.

**Dipendenza dalla versione di Python per l'upgrade di Sentinel**

Per il corretto processo di upgrade di Sentinel è necessario utilizzare versioni compatibili della libreria Python. Questo aspetto diventa molto importante quando si esegue l'upgrade da una versione precedente del sistema operativo a una nuova versione. Ad esempio, da un'installazione di Sentinel basata su SLES 11 SP4 a una versione del sistema operativo basata su SLES 15 SP2 di Sentinel. Prima di avviare il processo di upgrade di Sentinel, è consigliabile verificare la versione di Python. Se la versione Python nella finestra di Sentinel esistente cambia dopo un upgrade del sistema operativo, è obbligatorio seguire la procedura indicata di seguito.

Si consideri uno scenario di esempio.

**Scenario:** upgrade da Sentinel 8.2 (basato su SLES 11 SP4) a Sentinel 8.4 (basato su SLES 15 SP2).

In questo scenario, l'esecuzione di `python -V` nella finestra SLES 11 SP4 riporta che la versione di Python utilizzata è la 2.6.x. Si prevede che, dopo un upgrade del sistema operativo, verrà eseguito l'upgrade di Python alla versione 2.7.x. Questa differenza può potenzialmente causare un problema di compatibilità menzionato di seguito.

Dopo l'upgrade del sistema operativo e prima dell'upgrade della versione di Sentinel:

Come primo passaggio dell'upgrade, procedere con l'upgrade del sistema operativo da SLES 11 SP4 a SLES 15 SP2. Durante l'upgrade di un sistema operativo, è possibile che venga installata una versione più recente della libreria Python, ad esempio Python 2.7.x. Quindi, l'esecuzione del comando `python -V` mostra la versione 2.7.x di Python. Tuttavia, nonostante il computer mostri questa versione di Python, è possibile che il file oggetto condiviso di Python (`plpython2.so`) installato con la versione precedente di Sentinel punti ancora a una versione 2.6.x di Python.

Eseguire il seguente comando:

```
ldd <sentinel_installation_path>/opt/novell/sentinel/3rdparty/postgresql/
lib/postgresql/plpython2.so
```

L'output di questo comando permette di capire in base a quale versione di Python è stato creato il file `plpython2.so`. Ad esempio, l'output `libpython2.6.so.1.0 => /usr/lib64/libpython2.6.so.1.0` indica che il file `.so` è basato sulla versione 2.6.x di Python e non funzionerà con una versione 2.7.x.

Questo conflitto può causare un errore nel processo di upgrade. Per risolvere questo problema, è necessario rimuovere la versione precedente del file `plpython2.so` (basata sulla versione 2.6.x) con una versione più recente del file `plpython2.so` (basata sulla versione 2.7.x) in base allo scenario fornito. Esiste un buona probabilità che queste versioni di Python siano diverse nelle configurazioni e si consiglia di utilizzare questi comandi di conseguenza.

Per effettuare questa operazione, attenersi alla procedura seguente:

1. Arrestare Sentinel utilizzando il comando seguente:

   ```
   rcsentinel stop
   ```

2. Accedere alla directory in cui si trova il file `plpython2.so`:

   ```
   cd <sentinel_installation_path>/opt/novell/sentinel/3rdparty/
   postgresql/lib/postgresql
   ```

3. Rimuovere il file `.so` esistente che punta alla versione 2.6.x utilizzando il comando seguente:

   ```
   rm plpython2.so
   ```

4. Estrarre il contenuto del file `2.7.x.so` di Python (dovrebbe essere presente nella directory `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/postgresql/lib/postgresql`):

   ```
   tar zxf plpython2.7.so.tar.gz
   ```

5. Impostare l'autorizzazione utente `novell` per il file:

   ```
   chown novell:novell plpython2.so
   ```

6. Verificare che il file punti alla versione corretta di Python (l'output ora dovrebbe puntare alla versione 2.7.x) utilizzando il comando seguente:

```
ldd <sentinel_installation_path>/opt/novell/sentinel/3rdparty/
postgresql/lib/postgresql/plpython2.so
```

Dopo aver completato i passaggi appena descritti e aver verificato che il file `plpython2.so` punti alla versione corretta di Python, procedere con il processo di upgrade di Sentinel.

# 31 Esecuzione dell'upgrade dell'applicazione Sentinel

Le procedure descritte in questo capitolo illustrano come eseguire l'upgrade dell'applicazione Sentinel.

A partire da Sentinel versione 8.3.00, viene utilizzato PostgreSQL anziché MongoDB per memorizzare i dati di Security Intelligence e degli avvisi. È possibile quindi eseguire l'upgrade dell'applicazione dopo avere eseguito la migrazione dei dati da MongoDB a PostgreSQL.

I dati memorizzati in MongoDB vengono conservati come backup ed è possibile eliminarli al termine del processo di upgrade di Sentinel.

---

**Importante:** Quando si esegue l'upgrade del server Sentinel, assicurarsi di eseguire l'upgrade dei sistemi Collector Manager e Correlation Engine alla stessa versione del server Sentinel. In caso contrario, potrebbero verificarsi dei problemi nel sistema.

---



## Prerequisiti per il processo di upgrade dell'applicazione

Prima di eseguire l'upgrade, soddisfare i seguenti prerequisiti:

1. È necessario avere installato Sentinel 8.2 o versione successiva.
2. È necessario avere installato SLES 12 SP3 o SLES 12 SP4.
    a. (Condizionale) Se si utilizza SLES 11 SP4 con Sentinel 8.2.0.0, si consiglia di ottenere tutti gli aggiornamenti del canale su SLES 11. Eseguire quindi l'upgrade del sistema operativo a SLES 12 SP3. Per ulteriori informazioni sul processo di upgrade del sistema operativo SLES, vedere "Upgrade del sistema operativo a SLES 12 SP3" a pagina 168. Effettuare il download ed eseguire l'utility post-upgrade dal sito WebMicro Focus Patch Finder.
    b. (Condizionale) Se si utilizza SLES 12 SP3 con Sentinel 8.2.0.0 ed è stata eseguita l'utility post upgrade `sentinel_sles_iso_os_post_upgrade-release-73.tar.gz`, è necessario effettuare il download ed eseguire l'utility post-upgrade `sentinel_sles_iso_os_post_upgrade-release-85.tar.gz` dal sito Web Micro Focus Patch Finder.
    c. (Condizionale) Se si utilizza SLES 12 SP3 con Sentinel 8.2.0.0 ed è stata eseguita l'utility post-upgrade `sentinel_sles_iso_os_post_upgrade-release-85.tar.gz` dal sito Web Micro Focus Patch Finder, seguire la procedura riportata in "Esecuzione dell'upgrade dell'applicazione" a pagina 171.

3. **Importante:** Se si utilizza una versione aggiornata di Sentinel 8.3.0.0 o una nuova installazione della versione 8.3.0.0, seguire la procedura riportata in “Esecuzione dell'upgrade dell'applicazione” a pagina 171.

   (Condizionale) Eseguire la migrazione dei dati di Security Intelligence, degli avvisi e così via da MongoDB a PostgreSQL. È possibile eseguire questa operazione solo dopo avere soddisfatto i prerequisiti precedenti. Per ulteriori informazioni sulla migrazione dei dati, vedere “Migrazione dei dati da MongoDB a PostgreSQL” a pagina 170.

   È necessario eseguire lo script di migrazione anche se non si dispone di dati di cui eseguire la migrazione, in quanto lo script di migrazione genera uno script di pulizia. È possibile utilizzare lo script di pulizia per rimuovere i dati MongoDB che risulteranno essere ridondanti dopo il processo di upgrade di Sentinel.

## Upgrade del sistema operativo a SLES 12 SP3

Il processo di upgrade del sistema operativo è necessario in quanto:

- Sentinel è ora disponibile solo sul canale SLES 12. Per continuare a ricevere gli aggiornamenti di Sentinel e del sistema operativo è quindi necessario innanzitutto eseguire l'upgrade al sistema operativo SLES 12 SP3 prima di eseguire l'upgrade di Sentinel.
- È possibile sfruttare le funzionalità di Sentinel Appliance Manager. Sentinel Appliance Manager fornisce un'interfaccia utente basata sul Web semplice che consente di configurare e gestire l'applicazione.

**Per eseguire l'upgrade del sistema operativo e configurare l'applicazione:**

1. Interrompere i servizi Sentinel:

   ```
   rcsentinel stop
   ```

2. (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
   ```

3. (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`.
4. 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.
5. 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.

---

**Importante:** Durante il processo di upgrade verrà richiesto di registrarsi a SLES 12 SP3. Ignorare la registrazione. La registrazione per gli aggiornamenti in questa schermata viene eseguita solo per gli aggiornamenti di SLES 12 SP3 dal canale SUSE Customer, che non è supportato. Inoltre non sarà possibile ricevere gli aggiornamenti di Sentinel. Effettuare quindi la registrazione per gli aggiornamenti solo dopo aver completato il passaggio 9 in modo da ricevere sia gli aggiornamenti di Sentinel che di SLES 12 SP3 dal canale di aggiornamento dell'applicazione Sentinel.

---

6 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
```

7 (Condizionale) Per Sentinel ad alta disponibilità, completare i passaggi descritti nelle seguenti sezioni:

- “Configurazione delle destinazioni iSCSI” a pagina 235
- “Configurazione degli iniziatori iSCSI” a pagina 237
- “Configurazione del cluster ad alta disponibilità” a pagina 238

8 Per configurare l'applicazione, eseguire la utility post-upgrade dal prompt dei comandi:

**8a** Decomprimere il file:

```
tar -xvf <post upgrade utility installer filename>.tar.gz
```

**8b** Passare alla directory in cui è stata estratta l'utility:

```
cd <post upgrade utility installer filename>
```

**8c** 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.

---

**8d** Per completare la configurazione, seguire le istruzioni visualizzate sullo schermo.

I pacchetti installati verranno riconfigurati dallo script che eseguirà anche la configurazione dei pacchetti per la gestione dell'applicazione.

**9** 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 93.

# Migrazione dei dati da MongoDB a PostgreSQL

È necessario eseguire la migrazione dei dati di Security Intelligence, degli avvisi e così via da MongoDB a PostgreSQL eseguendo lo script di migrazione.

Lo script di migrazione esegue le seguenti operazioni:

- Esegue la migrazione dei dati di Security Intelligence e degli avvisi a PostgreSQL.
- Genera uno script di pulizia che è possibile utilizzare per rimuovere da MongoDB i dati e gli RPM relativi a MongoDB.

---

**Avviso:** Una volta eseguita la migrazione dei dati, è necessario eseguire l'upgrade di Sentinel prima di avviarlo o riavviarlo. Ciò garantisce che non vi sia alcuna perdita dei dati in arrivo su Sentinel.

---

**Per eseguire la migrazione dei dati:**

**1** Effettuare il download di `Mongo_To_PostgreSQL_Migration_Utility_8.3.0.0-5575.tar.gz` dalla pagina di download del sito Web.

**2** Decomprimere i file.

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

---

**Importante:** Eseguire lo script di migrazione dal terminale del computer. Non utilizzare un software di emulazione del terminale come PuTty o MobaXterm.

---

**4** Eseguire il seguente script: `mongo_to_pgsql_migration.sh`.

**5** Selezionare l'opzione di migrazione in base alle proprie esigenze.

---

**Avviso:** Accertarsi di selezionare l'opzione appropriata poiché non è possibile ripetere la procedura dopo il completamento della migrazione.

---

Se i dati vengono migrati correttamente, sullo schermo verrà visualizzato un messaggio di conferma. Ora è possibile eseguire l'upgrade dell'applicazione.

**6** (Condizionale) Se la migrazione dei dati non viene eseguita correttamente:

**6a** Ripulire i dati di cui è stata eseguita la migrazione. Per ulteriori informazioni, consultare "Pulizia dei dati da PostgreSQL in caso di errore di migrazione" a pagina 179.

**6b** Ripetere questa procedura per eseguire la migrazione dei dati.

7 (Condizionale) Se durante l'esecuzione dello script di migrazione viene visualizzato il seguente messaggio di errore, completare le attività riportate in “Impossibile eseguire lo script di migrazione” a pagina 180:

```
 8101server:/opt # su novell
novell@8101server:/opt>
novell@8101server:/opt> ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as novell
novell@8101server:/opt>
novell@8101server:/opt> exit
exit
8101server:/opt #
8101server:/opt # ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as root
```

# Esecuzione dell'upgrade dell'applicazione

È possibile eseguire l'upgrade sia di Sentinel che del sistema operativo SLES mediante Sentinel Appliance Update Channel (Canale di aggiornamento dell'applicazione) o Subscription Management Tool (SMT). È necessario prima soddisfare i prerequisiti elencati in “Prerequisiti per il processo di upgrade dell'applicazione” a pagina 167, quindi eseguire l'upgrade dell'applicazione.



## Esecuzione dell'upgrade mediante Appliance Update Channel (canale di aggiornamento 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 dal prompt dei comandi:**

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 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, vedere "Maintaining Custom Settings in XML Files" (Conservazione delle impostazioni personalizzate nei file XML) nella *Sentinel Administration Guide* (Guida all'amministrazione di Sentinel).

3 Eseguire il login al computer dell'applicazione e aprire un prompt dei comandi come utente `root`.

4 Eseguire i seguenti comandi dal prompt dei comandi:

---

**Importante:** Ignorare il messaggio/la richiesta di riavvio fino al Passo 6 a pagina 172. È importante avviare Sentinel (passaggio 4c) prima di riavviare il computer.

---

**4a** `zypper -v patch`

**4b** `zypper up`

**4b1** Immettere Y per continuare.

**4c** (Condizionale) Prima dell'upgrade, se è abilitata la visualizzazione degli eventi, dopo aver eseguito l'upgrade a Sentinel 8.4.0.0, Elasticsearch viene arrestato poiché viene abilitato con il plug-in di sicurezza X-Pack; per avviare Elasticsearch, attenersi alla procedura descritta in "Impostazioni in Elasticsearch per la comunicazione cluster sicura" a pagina 184.

**4d** `rcsentinel start`

5 Aprire il file `/etc/sysctl.conf` e cercare `# 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
```

6 Riavviare l'applicazione.

7 (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
```

8 Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.

9 (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.

**9a** Passare all'utente Novell.

```
su novell
```

**9b** Passare alla cartella `bin`:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

9c Cancellare i vecchi file PostgreSQL utilizzando il comando seguente:

```
./delete_old_cluster.sh
```

10 (Condizionale) Per eseguire l'upgrade dell'istanza di di Collector Manager o di Correlation Engine, procedere come descritto nel Passo 3 fino al Passo 7.

11 (Condizionale) Se si esegue Sentinel in un ambiente ad alta disponibilità, ripetere questi passaggi in tutti i nodi del cluster.

12 Riavviare Sentinel.

13 Eseguire il login a Sentinel e verificare che vengano visualizzati i dati migrati, ad esempio avvisi, dati di Security Intelligence e così via.

14 Ora i dati in MongoDB sono ridondanti poiché Sentinel 8.3 e versioni successive memorizzerà i dati solo in PostgreSQL. Per liberare spazio su disco, eliminare i dati. Per ulteriori informazioni, consultare "Rimozione dei dati da MongoDB" a pagina 183.

**Per eseguire l'upgrade dell'applicazione mediante Sentinel Appliance Manager:**

1 Avviare l'applicazione Sentinel effettuando una delle seguenti operazioni:

- Eseguire il login a Sentinel e fare clic su **Sentinel Main** > **Applicazione**.
- Specificare l'URL seguente nel browser Web: `https://<Indirizzo_IP>:9443`.

2 Eseguire il login come utente `vaadmin` o `root`.

3 (Condizionale) Effettuare la registrazione per gli aggiornamenti se non è stata effettuata in precedenza. Per ulteriori informazioni, consultare "Registrazione degli aggiornamenti" a pagina 93.

---

**Nota:** Per Sentinel 8.3.1, oltre ai passaggi 4 e 5, è necessario aggiungere il passaggio 6.

---

4 Fare clic su **Aggiornamento online**.

---

**Nota:** Non riavviare il sistema finché non vengono completati tutti i passaggi seguenti.

---

5 Per installare gli aggiornamenti visualizzati, fare clic su **Update Now (Aggiorna ora)** > **OK**.

6 Eseguire il seguente comando dal prompt dei comandi:

---

**Importante:** Ignorare il messaggio/la richiesta di riavvio fino al passaggio 7. È importante avviare Sentinel prima di riavviare il computer.

---

- zypper up
- (Condizionale) Prima dell'upgrade, se è abilitata la visualizzazione degli eventi, dopo aver eseguito l'upgrade a Sentinel 8.4.0.0, Elasticsearch viene arrestato poiché viene abilitato con il plug-in di sicurezza X-Pack; per avviare Elasticsearch, attenersi alla procedura descritta in "Impostazioni in Elasticsearch per la comunicazione cluster sicura" a pagina 184.
- rcsentinel start

7 Per applicare gli aggiornamenti installati, fare clic su **Reboot (Riavvia)**.

8 Eseguire il login a Sentinel e verificare che vengano visualizzati i dati migrati, ad esempio avvisi, dati di Security Intelligence e così via.

9 Ora i dati in MongoDB sono ridondanti poiché Sentinel 8.3 e versioni successive memorizzerà i dati solo in PostgreSQL. Per liberare spazio su disco, è possibile eliminare questi dati. Per ulteriori informazioni, consultare “Rimozione dei dati da MongoDB” a pagina 183.

## Upgrade tramite 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.

**Per eseguire l'upgrade dell'applicazione mediante SMT:**

1 Assicurarsi che l'applicazione sia configurata con SMT.

Per ulteriori informazioni, vedere il “Configurazione dell'applicazione con SMT” a pagina 95.

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 Sentinel).

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).

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 (Condizionale) Prima dell'upgrade, se è abilitata la visualizzazione degli eventi, dopo aver eseguito l'upgrade a Sentinel 8.4.0.0, Elasticsearch viene arrestato poiché viene abilitato con il plug-in di sicurezza X-Pack; per avviare Elasticsearch, attenersi alla procedura descritta in “Impostazioni in Elasticsearch per la comunicazione cluster sicura” a pagina 184.

11 Aprire il file `/etc/sysctl.conf` e cercare `# 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
```

12 Riavviare l'applicazione.

```
rcsentinel restart
```

13 (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
```

14 (Condizionale) Per eseguire l'upgrade dell'istanza di di Collector Manager o di Correlation Engine, procedere come descritto nel Passo 4 fino al Passo 13.

15 (Condizionale) Se si esegue Sentinel in un ambiente ad alta disponibilità, ripetere questi passaggi in tutti i nodi del cluster.

16 Riavviare Sentinel.

17 Eseguire il login a Sentinel e verificare che vengano visualizzati i dati migrati, ad esempio avvisi, dati di Security Intelligence e così via.

18 Ora i dati in MongoDB sono ridondanti poiché Sentinel 8.3 e versioni successive memorizzerà i dati solo in PostgreSQL. Per liberare spazio su disco, è possibile eliminare questi dati. Per ulteriori informazioni, consultare “Rimozione dei dati da MongoDB” a pagina 183.

# Esecuzione di aggiornamenti offline

È possibile eseguire un aggiornamento offline effettuando il download dell'immagine ISO delle patch offline per ciascuna applicazione.

## Aggiornamento dell'applicazione offline in un ambiente sicuro

Durante l'applicazione della patch, in caso di problemi di registro/archivio, è possibile provare a cancellare le voci del registro e dell'archivio nel sistema.

Per ripulire i dettagli del registro e dell'archivio nell'applicazione, eseguire i passaggi seguenti:

1. Eseguire un backup dei file prima di cancellare le voci di registro:
   a. Creare una directory di backup. Ad esempio:

      ```
      mkdir /etc/zypp/backup
      ```

   b. Copiare i seguenti file di registro nella directory di backup. Ad esempio:

```
cp /etc/zypp/credentials.d /etc/zypp/backup
cp /etc/zypp/repos.d/*     /etc/zypp/backup
cp /etc/zypp/services.d/*  /etc/zypp/ backup
```

2. Eliminare i seguenti file di registro:

```
rm -fr /etc/zypp/credentials.d
rm -fr /etc/zypp/repos.d/*
rm -fr /etc/zypp/services.d/*
```

## Applicazione della patch ISO

Eseguire i passaggi seguenti:

1. Effettuare il download dell'immagine ISO delle patch in una directory. Ad esempio: `<nomedirectory>/PatchCD-Sentinel-Server-<versione-numero build>-SLES12-SP5-<dataora>.iso`
2. Creare una directory per il montaggio dell'immagine ISO delle patch utilizzando il comando seguente. Ad esempio:

   ```
   mkdir -p /opt/trial
   ```

3. Montare localmente l'immagine ISO delle patch utilizzando il comando seguente. Ad esempio:

   ```
   mount -o loop <directoryname>/PatchCD-Sentinel-Server-<version-build number>-SLES12-SP5-<datetime>.iso /opt/trial
   ```

4. Aggiungere gli archivi del prodotto e del sistema operativo. Ad esempio:

   ```
   zypper ar -c -t plaindir "/opt/trial/product-repo" "<product repository>"
   zypper ar -c -t plaindir "/opt/trial/osupdate-repo" "<operating system repository>"
   ```

5. (Facoltativo) Confermare se gli archivi sono stati aggiunti correttamente utilizzando il comando seguente:

   ```
   zypper repos
   ```

6. Verificare che le patch siano state integrate nell'immagine ISO delle patch utilizzando il seguente comando:

   ```
   zypper lp
   ```

7. Applicare tutti gli aggiornamenti utilizzando i comandi seguenti:

   ```
   zypper -v patch
   zypper -v update
   ```

8. Ripulire l'elenco degli archivi utilizzando i comandi seguenti:

   ```
   zypper rr "<product repository>"
   zypper rr "<operating system repository>"
   ```

9. Al termine dell'aggiornamento, riavviare il computer utilizzando il seguente comando:

   `reboot`

# Applicazione delle patch del sistema operativo

**Per applicare le patch del sistema operativo:**

1. Avviare l'applicazione Sentinel effettuando una delle seguenti operazioni:
   - Eseguire il login a Sentinel e fare clic su **Sentinel Main** > **Applicazione**.
   - Specificare l'URL seguente nel browser Web: `https://<Indirizzo_IP>:9443`.
2. Eseguire il login come utente `vaadmin` o `root`.
3. Fare clic su **Aggiornamento online**.
   - **3a** (Condizionale) Effettuare la registrazione per gli aggiornamenti se non è stata effettuata in precedenza. Per ulteriori informazioni, consultare "Registrazione degli aggiornamenti" a pagina 93.
   - **3b** Per installare gli aggiornamenti visualizzati per il sistema operativo, fare clic su **Update Now (Aggiorna ora)** > **OK**.
4. Per applicare gli aggiornamenti installati, fare clic su **Reboot (Riavvia)**.

# 32 Soluzione dei problemi



## Pulizia dei dati da PostgreSQL in caso di errore di migrazione

Se si riscontrano errori durante la migrazione, è necessario eliminare i dati spostati parzialmente nel database PostgreSQL ed eseguire nuovamente lo script di migrazione.

---

**Avviso:** Non eseguire questa procedura se la migrazione ha esito positivo. Questo script elimina tutti i dati migrati.

---

**Per ripulire i dati parzialmente migrati:**

1. Accertarsi che il database PostgreSQL sia attivo e in esecuzione.
2. Eseguire il login al server Sentinel come utente `novell`.
3. Accedere all'ubicazione in cui è stato estratto il programma di installazione di Sentinel o l'utility di migrazione.
4. Eseguire lo script `./db_migration_failure_cleanup.sh` per eliminare i dati parzialmente migrati.
5. Eseguire il comando `rm db_migration_failure_cleanup.sh` per eliminare il file `db_migration_failure_cleanup.sh`.

   Per continuare con l'upgrade tradizionale, vedere Capitolo 30, “Upgrade dell'installazione tradizionale di Sentinel”, a pagina 157.

   Per continuare con l'upgrade dell'applicazione, eseguire la migrazione dei dati da MongoDB a PostgreSQL. Per informazioni, vedere “Migrazione dei dati da MongoDB a PostgreSQL” a pagina 170.

# Impossibile eseguire lo script di migrazione

È possibile che venga visualizzato il seguente messaggio di errore durante l'esecuzione dello script di migrazione per lo spostamento dei dati a PostgreSQL:

```
8101server:/opt # su novell
novell@8101server:/opt>
novell@8101server:/opt> ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as novell
novell@8101server:/opt>
novell@8101server:/opt> exit
exit
8101server:/opt #
8101server:/opt # ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as root
```

Questo errore potrebbe verificarsi se è stato eseguito l'upgrade dell'applicazione a Sentinel 8.2 da una versione precedente, poiché il file `bashrc` potrebbe essere stato modificato durante un processo di upgrade precedente.

Per evitare questo errore, è necessario aggiornare il file `bashrc`.

**Per aggiornare il file bashrc:**

1. Aprire il file `bashrc`:

   `/home/novell/.bashrc`

2. (Condizionale) Se non sono presenti, aggiungere le seguenti proprietà al file:

   ```
   APP_HOME="/opt/novell/sentinel"
   export PATH="$APP_HOME/bin:$APP_HOME/bin/actions:$PATH"
   ```

3. Eseguire nuovamente lo script di migrazione. Per ulteriori informazioni, consultare “Migrazione dei dati da MongoDB a PostgreSQL” a pagina 170.

# Impossibile connettersi ai server o ad altri componenti tramite applicazione

Le installazioni precedenti di Sentinel possono includere l'indirizzo IP 127.0.0.2 nel file `/etc/hosts` se è stata scelta l'opzione **Assign hostname to loopback address (Assegna nome host a indirizzo loopback)** durante l'installazione. Ciò potrebbe causare problemi di comunicazione con altri server o componenti. È necessario modificare il file e rimuovere l'indirizzo IP.

**Per rimuovere l'indirizzo IP:**

1. Aprire il file `/etc/hosts`.
2. Commentare la voce per l'indirizzo IP 127.0.0.2.
3. Salvare il file.

# Errore durante il processo di upgrade dell'applicazione

Quando si esegue l'upgrade dell'applicazione ed è stato eseguito l'upgrade alla versione 8.2 o successiva da una versione precedente, è possibile che venga visualizzato il seguente messaggio di errore:

```
(104/134) Installing: kernel-default-4.12.14-95.45.1.x86_64
.....................................................................
.............[error]
Installation of kernel-default-4.12.14-95.45.1.x86_64 failed:
Error: Subprocess failed. Error: RPM failed:    installing package kernel-
default-4.12.14-95.45.1.x86_64 needs 4MB on the /boot filesystem
```

Si tratta di un problema noto del sistema operativo SUSE e non di Sentinel. Pertanto, per risolvere il problema, attenersi alla soluzione fornita nella documentazione di SUSE.

# Errore durante l'aggiunta di una password all'archivio chiavi di Elasticsearch in fase di configurazione dell'upgrade

Durante l'esecuzione del seguente comando in fase di configurazione dell'upgrade, viene visualizzato il messaggio di errore `FileAlreadyExistsException`:

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

**Soluzione:**

1. Passare all'utente `novell`:

   ```
   su novell
   ```

2. Eliminare il file `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.keystore.tmp`.
3. Eliminare il certificato `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` ed eseguire il comando seguente per rigenerarlo:

   ```
   <sentinel_installation_path>/opt/novell/sentinel/bin/javacert.sh --
   generateES <sentinel_installation_path>/opt/novell/sentinel/3rdparty/
   elasticsearch/config/http.pks <password> <keyalias>
   ```

4. Eseguire il comando seguente in `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` per aggiungere la password per il certificato creato nel passaggio precedente per l'archivio chiavi di Elasticsearch:

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.http.ssl.keystore.secure_password
   ```

5. Fare riferimento alla sezione “Abilitazione della visualizzazione degli eventi in Sentinel” a pagina 109 ed eseguire i passaggi da 5 a 11 per configurare Elasticsearch.

6. Riavviare Sentinel:

   ```
   rcsentinel restart
   ```

# Impossibile visualizzare gli avvisi meno recenti nelle viste dashboard e avvisi dopo la configurazione di Elasticsearch

Dopo aver configurato Elasticsearch, il dashboard degli avvisi e i grafici nella vista degli avvisi non aggiornano o visualizzano gli avvisi meno recenti. Tuttavia, nella tabella della vista avvisi vengono visualizzati i nuovi avvisi generati. Questo problema può verificarsi a causa di un indice degli avvisi danneggiato.

**Soluzione:** eseguire i seguenti passaggi:

1. Accedere alla directory <percorso_di_installazione_di_sentinel>/var/opt/novell/sentinel/bin.
2. Per passare all'utente novell, eseguire il comando seguente:

   ```
   su novell
   ```

3. Per avviare il processo di sincronizzazione degli avvisi, eseguire il comando seguente:

   ```
   ./reSyncAlert.sh
   ```

# 33 Configurazioni di post-upgrade

In questo capitolo sono descritte le configurazioni di post-upgrade.



## Rimozione dei dati da MongoDB

Al termine del processo di upgrade di Sentinel, i dati memorizzati in MongoDB non saranno più necessari. È possibile eliminare questi dati per liberare spazio su disco.

**Per ripulire lo spazio di memorizzazione:**

1. Eseguire il login al server Sentinel come utente `root`.
2. Accedere a *<percorso_di_installazione_di_sentinel>*`/opt/novell/sentinel/bin`.
3. Eseguire lo script seguente:

   `./mongoDB_cleanup. sh`

## Sincronizzazione del file postgresql.conf

Durante l'upgrade, il file `postgresql.conf` proveniente da una versione precedente viene rinominato `postgresql.conf_old`. Viene creato un nuovo file `postgresql.conf` per la versione 8.3. Il nuovo file `postgresql.conf` contiene configurazioni che consentono di migliorare le prestazioni del dashboard di Security Intelligence. È pertanto necessario mantenere tale file. Nel caso in cui le personalizzazioni non siano incluse nel nuovo file, modificare il nuovo file `postgres.sql`. Entrambi i file si trovano nella seguente ubicazione: `/var/opt/novell/sentinel/3rdparty/postgresql/data/`

# 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 42.

# Impostazioni in Elasticsearch per la comunicazione cluster sicura

A partire da Sentinel 8.4.0.0 sono incluse funzioni di sicurezza avanzate pronte all'uso, per le quali sono necessarie alcune configurazioni post-installazione/upgrade. A partire dalla versione 8.4.0.0, Sentinel comunica con Elasticsearch in modo sicuro (tramite SSL) e di default integra il plug-in X-Pack di Elasticsearch. In questo modo l'amministratore di Sentinel avrà la possibilità di configurare tutte le comunicazioni Elasticsearch da **nodo** a **nodo** in modo sicuro tramite SSL. In questo modo sarà possibile memorizzare i dati nei nodi Elasticsearch in diverse aree geografiche, consentendo comunque che i dati siano trasmessi e visualizzati in modo sicuro da un server Sentinel. Grazie a questa funzione, gli utenti possono ora unirsi a tutti i cluster Elasticsearch distribuiti in tutto il mondo e possono comunque visualizzare e accumulare i risultati in modo sicuro da un'unica console di ricerca di Sentinel.

---

**Importante:** Per il completamento del processo di upgrade, l'esecuzione dei passaggi seguenti è obbligatoria. I dettagli presenti in questa pagina sono applicabili solo se la funzione di visualizzazione degli eventi è abilitata prima dell'upgrade alle versioni 8.4 o 8.5 di Sentinel da una versione precedente di Sentinel.

Pertanto se si sta eseguendo l'upgrade da Sentinel 8.4 a Sentinel 8.5, non eseguire i passaggi seguenti.

Se non vengono eseguiti i passaggi descritti, l'upgrade a Sentinel 8.4.0.0 o versione successiva da una versione precedente sarà incompleto e si verificano i seguenti problemi:

- Elasticsearch non verrà avviato automaticamente.
- Se Elasticsearch non viene riavviato manualmente, gli avvisi e gli eventi presenti non verranno visualizzati correttamente durante la ricerca in Sentinel.

---

**Abilitazione della comunicazione sicura tra il server Sentinel ed Elasticsearch preintegrato quando non è presente alcuna configurazione del cluster Elasticsearch esterno**

Questa sezione è necessaria per i casi in cui non è associato alcun cluster Elasticsearch esterno a Sentinel. In questo caso, è necessario solo abilitare la comunicazione sicura tra Sentinel ed Elasticsearch preintegrato.

1. Arrestare il servizio Elasticsearch interno utilizzando il comando seguente:

   ```
   rcsentinel stopES
   ```

2. Passare all'utente `novell`:

   ```
   su novell
   ```

   Se la versione java è 292, eseguire i passaggi 3 e 4. Per individuare la versione Java a livello di sistema operativo, eseguire `java -version` dal prompt dei comandi.

3. (Condizionale) Impostare `JAVA_HOME` al JDK di Sentinel integrato:

   ```
   JAVA_HOME=/opt/novell/sentinel/jdk
   ```

4. (Condizionale) Impostare PATH per Java all'ubicazione del JDK di Sentinel:

   ```
   PATH=$JAVA_HOME/bin:$PATH
   ```

5. Generare un'autorità di certificazione (CA) per il cluster nel nodo Sentinel. Eseguire il comando seguente nella home directory di Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

   ```
   ./bin/elasticsearch-certutil ca
   ```

   Viene richiesto di specificare il nome file e la password del certificato CA. Il nome file di default è `elastic-stack-ca.p12`.

6. Generare i certificati e le chiavi private per il nodo Elasticsearch preintegrato di Sentinel. A tal scopo, eseguire il comando seguente nella home directory di Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

   ```
   ./bin/elasticsearch-certutil cert --ca <CA certificate filename>.p12 --out config/certs/node-1.p12
   ```

   Viene richiesto di immettere la password per il certificato CA. Viene inoltre richiesto di creare una password per il certificato generato.

7. Aggiungere le seguenti impostazioni al file `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.yml` nel nodo Sentinel:

   - `xpack.security.transport.ssl.enabled: true`
   - `xpack.security.transport.ssl.keystore.path: certs/node-1.p12`
   - `xpack.security.transport.ssl.truststore.path: certs/node-1.p12`
   - `xpack.security.transport.ssl.verification_mode: certificate`

8 Memorizzare la password del file del certificato dell'`archivio attendibilità` e dell'`archivio chiavi` generata in precedenza nell'archivio chiavi di Elasticsearch. A tal scopo, eseguire i comandi seguenti nella home directory di Elasticsearch: `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.truststore.secure_password
```

9 Avviare il servizio Elasticsearch utilizzando il comando seguente:

```
rcsentinel startES
```

**Abilitazione della comunicazione sicura tra i nodi Elasticsearch esterni e tra Sentinel e il cluster Elasticsearch in presenza di una configurazione del cluster Elasticsearch esterno**

L'ultima versione di Sentinel consente la comunicazione sicura tra il server Sentinel e il cluster Elasticsearch esterno e tra i diversi nodi del cluster Elasticsearch. In questa sezione viene illustrata la procedura per abilitare tali impostazioni sicure nei casi in cui al server Sentinel sia connesso un cluster Elasticsearch esterno.

1 **Passaggi da seguire per proteggere la comunicazione all'interno del cluster tra i nodi Elasticsearch:**

1. Arrestare Elasticsearch su tutti i nodi.
2. Passare all'utente `novell`:

   ```
   su novell
   ```

   Se la versione java è 292, eseguire i passaggi 3 e 4. Per individuare la versione Java a livello di sistema operativo, eseguire `java -version` dal prompt dei comandi.
3. (Condizionale) Impostare JAVA_HOME al JDK di Sentinel integrato:

   ```
   JAVA_HOME=/opt/novell/sentinel/jdk
   ```
4. (Condizionale) Impostare PATH per Java all'ubicazione del JDK di Sentinel:

   ```
   PATH=$JAVA_HOME/bin:$PATH
   ```
5. Generare un'autorità di certificazione (CA) per il cluster nel nodo Sentinel. Eseguire il comando seguente nella home directory di Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

   ```
   ./bin/elasticsearch-certutil ca
   ```

   Viene richiesto di specificare il nome file e la password del certificato CA. Il nome file di default è `elastic-stack-ca.p12`.
6. Generare i certificati e le chiavi private per il nodo Elasticsearch preintegrato di Sentinel. A tal scopo, eseguire il comando seguente nella home directory di Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

```
./bin/elasticsearch-certutil cert --ca <CA certificate
filename>.p12 --out config/certs/node-1.p12
```

Viene richiesto di immettere la password per il certificato CA. Viene inoltre richiesto di creare una password per il certificato generato.

7. Aggiungere le seguenti impostazioni al file `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.yml` nel nodo Sentinel:
   - `xpack.security.transport.ssl.enabled: true`
   - `xpack.security.transport.ssl.keystore.path: certs/node-1.p12`
   - `xpack.security.transport.ssl.truststore.path: certs/node-1.p12`
   - `xpack.security.transport.ssl.verification_mode: certificate`
8. Memorizzare la password del file del certificato dell'`archivio attendibilità` e dell'`archivio chiavi` generata in precedenza nell'archivio chiavi di Elasticsearch. A tal scopo, eseguire i comandi seguenti nella home directory di Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.keystore.secure_password
   ```

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.truststore.secure_password
   ```

9. Generare i certificati per tutti i nodi Elasticsearch esterni nel cluster. È possibile creare prima tutti i certificati Elasticsearch esterni nel nodo Sentinel stesso e quindi copiarli nei rispettivi nodi Elasticsearch. A tal scopo, eseguire innanzitutto il comando seguente nella home directory di Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch` dell'istanza di Sentinel:

   ```
   ./bin/elasticsearch-certutil cert --ca <CA certificate
   filename>.p12 --out config/certs/newNode.p12
   ```

   Viene richiesto di immettere la password per il certificato CA. Viene inoltre richiesto di creare una password per il certificato generato.

10. Copiare i certificati nei rispettivi nodi Elasticsearch esterni. Ad esempio, copiare il file `newNode.p12` nella directory `/etc/elasticsearch/certs/` di `newNode` del cluster Elasticsearch esterno. Fornire le autorizzazioni di lettura/scrittura ai certificati sui nuovi computer utilizzando il comando `chmod`.

    **Nota:** Se la directory `certs` non è presente, è necessario crearla.

11. Dopo aver generato e copiato i certificati in tutti i nodi Elasticsearch esterni, aggiungere le seguenti impostazioni nel file `/etc/elasticsearch/elasticsearch.yml` di tutti i nodi Elasticsearch esterni:
    - `xpack.security.enabled: true`
    - `xpack.security.transport.ssl.enabled: true`
    - `xpack.security.transport.ssl.keystore.path: certs/newNode.p12`
    - `xpack.security.transport.ssl.truststore.path: certs/newNode.p12`
    - `xpack.security.transport.ssl.verification_mode: certificate`

12. In ciascun nodo Elasticsearch esterno, memorizzare la password per il file del certificato dell'`archivio chiavi` e dell'`archivio attendibilità` generato nell'archivio chiavi di Elasticsearch. A tal scopo, eseguire i comandi seguenti nella home directory di Elasticsearch `/usr/share/elasticsearch` di tutti i nodi Elasticsearch esterni:

    ```
    ./bin/elasticsearch-keystore add
    xpack.security.transport.ssl.keystore.secure_password
    ```

    ```
    ./bin/elasticsearch-keystore add
    xpack.security.transport.ssl.truststore.secure_password
    ```

**2 Passaggi da seguire per proteggere le comunicazioni tra Sentinel e il cluster Elasticsearch:**

1. Passare all'utente `novell`:

    ```
    su novell
    ```

2. Eseguire il comando seguente per generare un certificato `http` per un nodo Elasticsearch esterno dal computer Sentinel:

    ```
    <sentinel_installation_path>/opt/novell/sentinel/bin/javacert.sh --
    generateES <provide path where the http certificate should be
    generated, example /opt/http.pks> <http certificate password>
    <keyalias>
    ```

3. Copiare il certificato `http` nel nodo Elasticsearch. Ad esempio, copiare il file `http.pks` nella directory ES_PATH_CONF`/certs/` del nodo Elasticsearch. Fornire le autorizzazioni di lettura/scrittura ai certificati sui nuovi computer.

    **Nota:** Se la directory `certs` non è presente, è necessario crearla.

4. Aggiungere le seguenti impostazioni al file ES_PATH_CONF`/elasticsearch.yml` in tutti i nodi Elasticsearch esterni:
    - `xpack.security.http.ssl.enabled: true`
    - `xpack.security.http.ssl.keystore.path: certs/http.pks`
5. Eseguire il comando seguente nella home directory di Elasticsearch `/usr/share/elasticsearch` di tutti i nodi Elasticsearch esterni per salvare la password del certificato `http` nell'archivio chiavi di Elasticsearch:

    ```
    ./bin/elasticsearch-keystore add
    xpack.security.http.ssl.keystore.secure_password
    ```

6. Avviare il servizio Elasticsearch in ciascuno dei nodi Elasticsearch esterni:

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

**3 (Condizionale) Se si è in modalità FIPS, dopo aver eseguito i due passaggi descritti in precedenza, è necessario eseguire i passaggi seguenti:**

1. Aggiungere il certificato `http` Elasticsearch interno generato durante l'installazione di Sentinel nell'archivio chiavi FIPS del server Sentinel utilizzando il comando:

    ```
    ./convert_to_fips.sh -i <sentinel_installation_path>/opt/novell/
    sentinel/3rdparty/elasticsearch/config/http.pks
    ```

2. Dopo il passaggio precedente verrà richiesto di riavviare Sentinel. Selezionare **No**.

3. Copiare i certificati `http` di tutti i nodi Elasticsearch esterni generati nel passaggio 2 e aggiungerli all'archivio chiavi FIPS del server Sentinel utilizzando il comando seguente:

   ```
   ./convert_to_fips.sh -i <location of the copied http certificate>/
   <name of the certificate>
   ```

4. Assicurarsi che tutti i certificati `http` dei nodi Elasticsearch esterni siano presenti nell'archivio chiavi FIPS del server Sentinel eseguendo il seguente comando:

   ```
   certutil -L -d sql:<sentinel_installation_path>/etc/opt/novell/
   sentinel/3rdparty/nss
   ```

5. Copiare il certificato`http` Elasticsearch interno (`<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` nel server Sentinel) generato durante l'installazione di Sentinel e aggiungerlo a tutti gli archivi chiavi FIPS di Remote Collector Manager (RCM) utilizzando il seguente comando:

   ```
   ./convert_to_fips.sh -i <location of the copied http certificate>/
   http.pks
   ```

6. Dopo il passaggio precedente verrà richiesto di riavviare Sentinel. Selezionare **No**.
7. Copiare i certificati `http` di tutti i nodi Elasticsearch esterni generati nel passaggio 2 e aggiungerli all'archivio chiavi FIPS di tutti gli RCM utilizzando il comando seguente:

   ```
   ./convert_to_fips.sh -i <location of the copied http certificate>/
   <name of the certificate>
   ```

8. Assicurarsi che tutti i certificati `http` dei nodi Elasticsearch esterni siano presenti nell'archivio chiavi FIPS di RCM eseguendo il seguente comando:

   ```
   certutil -L -d sql:<rcm_installation_path>/etc/opt/novell/sentinel/
   3rdparty/nss
   ```

4 **Riavviare Sentinel e tutti gli RCM:**

```
rcsentinel restart
```

# Aggiunta del certificato http.pks in modalità FIPS

A partire da Sentinel 8.4.0.0, la comunicazione tra Elasticsearch e Sentinel è protetta, pertanto è necessario aggiungere il certificato `http` all'archivio chiavi FIPS del server Sentinel e alle istanze remote di Collector Manager (RCM).

**Se la visualizzazione degli eventi non è abilitata, eseguire i passaggi seguenti:**

1 Aggiungere il certificato `http` Elasticsearch interno generato durante l'installazione di Sentinel nell'archivio chiavi FIPS del server Sentinel utilizzando il seguente comando:

```
./convert_to_fips.sh -i <sentinel_installation_path>/opt/novell/
sentinel/3rdparty/elasticsearch/config/http.pks
```

2 Copiare il certificato `http` Elasticsearch interno (`<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks`) in tutti gli RCM e importarli nell'archivio chiavi FIPS utilizzando il seguente comando:

```
./convert_to_fips.sh -i <path of the certificate copied above>/http.pks
```

# Configurazione della raccolta dati del flusso IP

Sentinel si avvale delle istanze di ArcSight SmartConnector che consentono di controllare la rete aziendale tramite la raccolta dati del flusso IP. Le istanze di SmartConnector raccolgono i dati del flusso IP come eventi e vengono pertanto considerati per il conteggio EPS. Ciò consente di:

- Utilizzare le istanze esistenti di Collector Manager per raccogliere i dati del flusso IP.
- 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.

La funzionalità di flusso IP è ora abilitata per default. È necessario installare e configurare ArcSight SmartConnector per la raccolta dei dati del flusso IP.

Sentinel non include più le funzioni di NetFlow, tra cui le visualizzazioni. Tramite le istanze di SmartConnector che raccolgono i dati del flusso IP come eventi, è possibile utilizzare le istanze di Collector Manager esistenti per la raccolta dei dati NetFlow. Non sarà quindi più necessario utilizzare istanze di NetFlow Collector Manager per raccogliere i dati NetFlow. Pertanto, è possibile disinstallare eventuali istanze esistenti di NetFlow Collector Manager.


- “Configurazione delle istanze di SmartConnector per la raccolta dei dati del flusso IP” a pagina 190
- “Disinstallazione delle istanze di NetFlow Collector Manager esistenti” a pagina 190


## Configurazione delle istanze di SmartConnector per la raccolta dei dati del flusso IP

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.

## Disinstallazione delle istanze di NetFlow Collector Manager esistenti

**Per disinstallare le istanze di NetFlow Collector Manager esistenti:**

1 Eseguire il login al computer di NetFlow Collector Manager con la stessa autorizzazione utente utilizzata per installare 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 disinstalla completamente Collector Manager.

# 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 93.

# 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.

---

# Aggiornamento delle autorizzazioni per gli utenti che inviano i dati da altri prodotti integrati a Sentinel

In Sentinel 8.2 SP1 e versioni successive è disponibile una nuova autorizzazione, Invia eventi e allegati, che consente solo agli utenti designati di inviare eventi e allegati da Change Guardian o Secure Configuration Manager a Sentinel. Quando si esegue l'upgrade a Sentinel 8.2 SP1 e versioni successive, quest'autorizzazione viene assegnata automaticamente agli utenti con ruolo di amministratore. Per gli utenti non amministratori che inviano eventi o allegati a Sentinel, è necessario assegnare manualmente l'autorizzazione. Se non si assegna tale autorizzazione, Sentinel non riceverà più eventi o allegati da Change Guardian o Secure Configuration Manager.

L'aggiornamento di questa autorizzazione è applicabile solo se Sentinel è integrato con Change Guardian o Secure Configuration Manager. Per ulteriori informazioni, vedere Creating Roles (Creazione dei ruoli) nella Sentinel Administration Guide (Guida all'amministrazione di Sentinel).

# Aggiornamento della password dell'archivio chiavi

Lo script `chg_keystore_pass.sh` consente di cambiare le password dell'archivio chiavi. Come best practice di sicurezza, modificare le password dell'archivio chiavi subito dopo l'upgrade di Sentinel.

---

**Nota:** Non eseguire questa procedura se il server Sentinel è in modalità FIPS.

---

**Per modificare le password dell'archivio chiavi:**

1. Eseguire il login al server di Sentinel come utente root.
2. Passare all'utente `novell`.
3. Passare alla directory `/opt/novell/sentinel/bin`.
4. Eseguire lo script `chg_keystore_pass.sh` e seguire le istruzioni visualizzate per cambiare le password di dell'archivio chiavi.

# 34 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.

# 35 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 36, “Migrazione dei dati”, a pagina 201.

# 36 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 Capitolo 18, “Configurazione di Elasticsearch per la visualizzazione degli eventi”, a pagina 109.

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.

---

# 37 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.

# 38 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 SP5
  - 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 12 SP5 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.

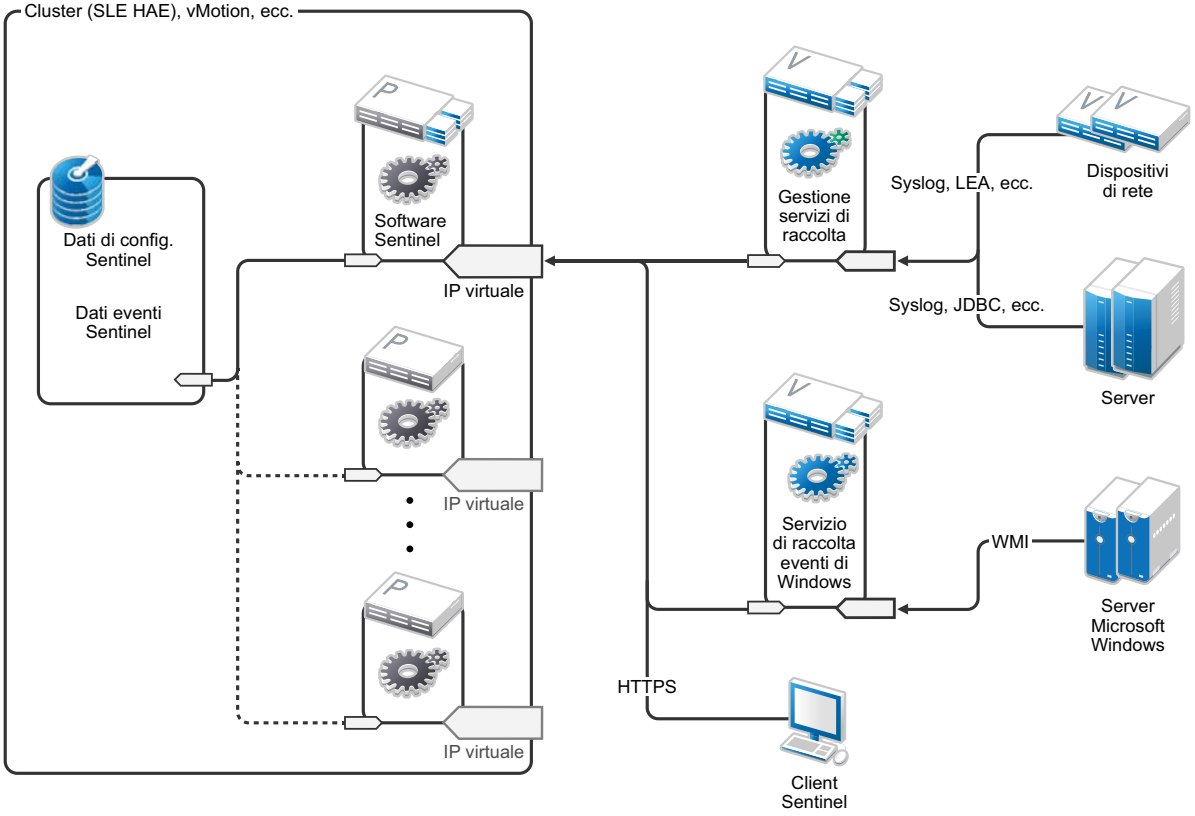
per iSCSI si deve utilizzare l'unità MTU (Message Transfer Unit) più grande supportata dall'hardware in uso. L'uso di unità MTU di grandi dimensioni migliora le prestazioni di memorizzazione. Nel caso in cui la latenza e la larghezza di banda verso l'unità di memorizzazione siano più lente dei valori 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.

# 39 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 57, 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`.<br>◆ Accertarsi di non aver assegnato un nome host a un indirizzo IP di loopback.<br>◆ 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 88.
- 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=<file size> bs=<bit size>
```

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 214
- "Configurazione degli iniziatori iSCSI" a pagina 216


## 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 12 SP1 e versione successiva, selezionare **Servizi di rete** > **Destinazione iSCSI LIO**.

  ---

  **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 12 SP1 e versione successiva: `iscsiliotarget RPM`

9 (Condizionale) Se si utilizza SLES 12, effettuare i passaggi seguenti in 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.

---

**Nota:** Micro Focus consiglia di utilizzare una password diversa per la destinazione e l'iniziatore iSCSI.

---

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 Lasciare le altre opzioni ai valori di default e fare clic su **Avanti**.

17 (Condizionale) Se si utilizza SLES 12, 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.

Non è necessario aggiungere il nome dell'iniziatore client per SLES 15 e versioni successive.

18 (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.

19 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.

20 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 214 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 otterrà 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 218
- "Installazione dell'applicazione Sentinel ad alta disponibilità" a pagina 219


### 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.
   - **3c** Se si abilita la modalità FIPS, aggiungere il percorso del certificato `http` Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando viene richiesto il certificato esterno.
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`.
   - **3d** Se si abilita la modalità FIPS, aggiungere il percorso del certificato `http` Elasticsearch `<percorso_di_installazione_di_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks` quando viene richiesto il certificato esterno.
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/sentinel/* /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/sentinel
```

```
umount /var/opt/novell/sentinel
```

### Configurazione dell'applicazione con SMT

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-HA-8-OS-Updates sle-12-x86_64
```

```
smt-repos -e Sentinel-Server-HA-8-Prod-Updates sle-12-x86_64
```

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

## Installazione in nodi successivi


- "Installazione tradizionale ad alta disponibilità" a pagina 220
- "Installazione dell'applicazione Sentinel ad alta disponibilità" a pagina 221


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/sentinel/*
   ```

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.

## Connessione di RCM/RCE in modalità ad alta disponibilità

### Tradizionale ad alta disponibilità

**Eseguire i seguenti passaggi per connettere RCM/RCE in modalità tradizionale ad alta disponibilità sia per la nuova configurazione che per quella esistente:**

1. Aggiungere una voce al file `/etc/hosts` come indicato di seguito nella casella RCM/RCE prima di installare/configurare RCM/RCE.

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   Ad esempio: 164.99.87.27 primo_host_attivo.nome.dom primo_host_attivo

   ---

   **Importante:** Assicurarsi che questa voce corrisponda sempre al primo nome host del nodo attivo corretto nell'ambiente ad alta disponibilità specificato nel file`/etc/hosts` prima di eseguire `configure.sh`

   ---

2. Alla richiesta visualizzata durante la connessione di RCM/RCE al server, fornire l'IP virtuale.

   ---

   **Importante:** Sebbene il primo nodo attivo corretto sia inattivo e l'altro nodo sia attualmente attivo, utilizzare comunque il nome del primo nodo attivo corretto con l'IP virtuale nel file `/etc/hosts`.

   ---

### Alta disponibilità dell'applicazione

**Eseguire i seguenti passaggi per connettere RCM/RCE in modalità ad alta disponibilità dell'applicazione per la nuova configurazione:**

- Utilizzare solo il nome host del primo nodo attivo corretto nel cluster ad alta disponibilità.

**Eseguire i seguenti passaggi per connettere RCM/RCE in modalità ad alta disponibilità dell'applicazione per la configurazione esistente:**

1. Aggiungere una voce al file `/etc/hosts` come indicato di seguito nella casella RCM/RCE prima di installare/configurare RCM/RCE.

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   Ad esempio: 164.99.87.27 primo_host_attivo.nome.dom primo_host_attivo

   ---

   **Importante:** Assicurarsi che questa voce corrisponda sempre al primo nome host del nodo attivo corretto nell'ambiente ad alta disponibilità specificato nel file`/etc/hosts` prima di eseguire `configure.sh`

   ---

2. Alla richiesta visualizzata durante la connessione di RCM/RCE al server, fornire l'IP virtuale.

   ---

   **Importante:** Sebbene il primo nodo attivo corretto sia inattivo e l'altro nodo sia attualmente attivo, utilizzare comunque il nome del primo nodo attivo corretto con l'IP virtuale nel file `/etc/hosts`.

   ---

# 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 227.

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 (Condizionale) Se non è stata abilitata l'autenticazione, selezionare **Sicurezza** dal pannello sinistro, deselezionare **Enable Security Auth (Abilita autenticazione sicurezza)**.

22 Per completare la configurazione, selezionare **Fine**.

23 Uscire da YaST.

24 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` ed eseguire 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.

# 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 è diverso da quello della soluzione consigliata, è possibile modificare il file `resources.cli` (nella stessa directory) e modificare le definizioni delle primitive. 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.

# 40 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 <watchdog driver name>`

## Upgrade dell'installazione tradizionale di Sentinel ad alta disponibilità

La procedura descritta in questa sezione consente di eseguire l'upgrade dell'installazione tradizionale di Sentinel ad alta disponibilità e del sistema operativo.

A partire da Sentinel versione 8.3.00, viene utilizzato PostgreSQL anziché MongoDB per memorizzare i dati di Security Intelligence e degli avvisi.

---

**Importante:** Se si esegue l'upgrade da versioni precedenti di Sentinel 8.3.0.0, i passaggi seguenti sono applicabili.

---

Il processo di upgrade esegue le seguenti operazioni sul nodo attivo:

- Esegue la migrazione dei dati di Security Intelligence, degli avvisi e così via da MongoDB a PostgreSQL.

  Ora Sentinel memorizza i dati di Security Intelligence e degli avvisi in PostgreSQL anziché in MongoDB. Il processo di upgrade eseguirà la migrazione dei dati a PostgreSQL e, in caso di esito positivo, proseguirà automaticamente con il processo di upgrade. Se la migrazione dei dati ha esito negativo, non sarà possibile eseguire l'upgrade di Sentinel.
- Genera uno script di pulizia che è possibile utilizzare per rimuovere i dati e gli RPM relativi a MongoDB.

I dati memorizzati in MongoDB vengono conservati come backup ed è possibile eliminarli al termine del processo di upgrade di Sentinel.


- "Upgrade di Sentinel ad alta disponibilità" a pagina 232
- "Upgrade del sistema operativo" a pagina 234


## 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:

   ```
   rcpacemaker 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 <install_filename>
   ```

   **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:

   ```
   rcpacemaker start
   ```

Ripetere dal Passo 3a a pagina 232 al Passo 3e a pagina 232 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 Sentinel).

**4b** Arrestare lo stack del cluster:

```
rcpacemaker 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 <install_filename>
```

**4e** Nella directory in cui risiedono i file di installazione estratti, eseguire il comando seguente:

```
./install-sentinel
```

---

**4f** **Importante:** Se si esegue l'upgrade da versioni precedenti di Sentinel 8.3.0.0, i passaggi seguenti sono applicabili.

---

**4f1** Selezionare l'opzione di migrazione desiderata.

---

**Avviso:** Accertarsi di selezionare l'opzione appropriata poiché non è possibile ripetere la procedura dopo il completamento del processo di upgrade.

---

Se la migrazione dei dati ha esito positivo, il processo di upgrade continuerà automaticamente.

Il processo di upgrade mantiene i dati memorizzati in MongoDB come backup.

**4f2** (Condizionale) Se la migrazione dei dati non viene eseguita correttamente:

**4f2a** Ripulire i dati di cui non è stata eseguita la migrazione. Per ulteriori informazioni, vedere "Pulizia dei dati da PostgreSQL in caso di errore di migrazione" a pagina 179.

**4f2b** (Condizionale) Avviare Sentinel, se non viene avviato automaticamente:

```
rcsentinel start
```

**4f2c** (Condizionale) Prima dell'upgrade, se è abilitata la visualizzazione degli eventi, dopo aver eseguito l'upgrade a Sentinel 8.4.0.0, Elasticsearch viene arrestato poiché viene abilitato con il plug-in di sicurezza X-Pack; per avviare Elasticsearch, attenersi alla procedura descritta in "Impostazioni in Elasticsearch per la comunicazione cluster sicura" a pagina 184.

**4g** Al termine dell'upgrade, avviare lo stack del cluster:

```
rcpacemaker start
```

**4h** Rimuovere gli script di avvio automatico affinché il cluster possa gestire il prodotto.

```
cd /
insserv -r sentinel
```

**4i** 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
```

8 Eseguire il login a Sentinel e verificare che vengano visualizzati i dati migrati, ad esempio avvisi, dati di Security Intelligence e così via.

9 Ora i dati in MongoDB sono ridondanti poiché Sentinel 8.3 e versioni successive memorizzerà i dati solo in PostgreSQL. Per liberare spazio su disco, eliminare i dati. Per ulteriori informazioni, consultare “Rimozione dei dati da MongoDB” a pagina 183.

## 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 235
- “Configurazione delle destinazioni iSCSI” a pagina 235
- “Configurazione degli iniziatori iSCSI” a pagina 237
- “Configurazione del cluster ad alta disponibilità” a pagina 238

## 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 arrestare lo stack del cluster:

     ```
     rcpacemaker stop
     ```

     Arrestando 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 il sistema operativo di tutti i nodi del cluster sia lo stesso.

## 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.

Per configurare le destinazioni iSCSI:

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:

- Selezionare **Servizi di rete** > **iSCSI LIO Target** (Destinazione LIO iSCSI).

  **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:

iscsiliotarget RPM

9 (Condizionale) Effettuare i passaggi seguenti in 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` (Configurazione client di destinazione iSCSI).

10 Fare clic su **Service** (Servizio) e selezionare l'opzione **When Booting** (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 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.

**Nota:** Micro Focus consiglia di utilizzare una password diversa per la destinazione e l'iniziatore iSCSI.

12 Fare clic su **Targets** (Destinazioni) e successivamente su **Add** (Aggiungi) per aggiungere una nuova destinazione.

13 Fare clic su **Aggiungi** per aggiungere un nuovo LUN.

14 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`.

15 Ripetere i passaggi 13 e 14, ma questa volta aggiungere LUN 1 e selezionare `/networkdata`.

16 Non modificare i valori di default delle altre opzioni. Fare clic su **Avanti**.

17 (Condizionale) Se si utilizza SLES 12, 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.

Non è necessario aggiungere il nome dell'iniziatore client per SLES 15 e versioni successive.

18 (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.

19 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.

20 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 235 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 a Sentinel da Sentinel 8.2 o versioni successive. È possibile eseguire l'upgrade di Sentinel e del sistema operativo SLES tramite Sentinel Appliance Manager o Zypper (Appliance Update Channel, canale di aggiornamento dell'applicazione).

A partire da Sentinel versione 8.3.00, viene utilizzato PostgreSQL anziché MongoDB per memorizzare i dati di Security Intelligence e degli avvisi. Prima di eseguire l'upgrade dell'applicazione sul nodo attivo, è necessario eseguire la migrazione dei dati da MongoDB a PostgreSQL. L'utente sarà in grado di eseguire l'upgrade dell'applicazione solo se i dati sono stati migrati correttamente a PostgreSQL.

- È necessario avere installato SLES 12 SP3 o SLES 12 SP4.
  1. (Condizionale) Se si utilizza SLES 11 SP4 con Sentinel 8.2.0.0, si consiglia di ottenere tutti gli aggiornamenti del canale su SLES 11. Eseguire quindi l'upgrade del sistema operativo a SLES 12 SP3. Per ulteriori informazioni sul processo di upgrade del sistema operativo SLES, vedere “Upgrade del sistema operativo a SLES 12 SP3” a pagina 168. Effettuare il download ed eseguire l'utility post-upgrade dal sito WebMicro Focus Patch Finder.
  2. (Condizionale) Se si utilizza SLES 12 SP3 con Sentinel 8.2.0.0 ed è stata eseguita l'utility post upgrade `sentinel_sles_iso_os_post_upgrade-release-73.tar.gz`, è necessario effettuare il download ed eseguire l'utility post-upgrade `sentinel_sles_iso_os_post_upgrade-release-85.tar.gz` dal sito Web Micro Focus Patch Finder.
  3. (Condizionale) Se si utilizza SLES 12 SP3 con Sentinel 8.2.0.0 ed è stata eseguita l'utility post-upgrade `sentinel_sles_iso_os_post_upgrade-release-85.tar.gz` dal sito Web Micro Focus Patch Finder, seguire la procedura riportata in “Esecuzione dell'upgrade dell'applicazione” a pagina 171.
- “Esecuzione dell'upgrade mediante la patch Zypper” a pagina 239
- “Esecuzione dell'upgrade tramite la console di gestione dell'applicazione Sentinel” a pagina 241

## Esecuzione dell'upgrade mediante la patch 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 93. 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.

```
rcpacemaker stop
```

Arrestando lo stack del cluster le risorse rimangono inaccessibili e si evita il fencing dei nodi.

**3b** Soddisfare i prerequisiti 1 e 2 elencati in "Prerequisiti per il processo di upgrade dell'applicazione" a pagina 167

**3c** Effettuare il download degli aggiornamenti per Sentinel:

---

**Nota:** Per Sentinel 8.3.1, sono necessari i comandi `zypper -v patch` e `zypper up` poiché per l'applicazione sono richiesti sia gli rpm aggiornati che quelli nuovi.

---

- `zypper -v patch`

  ---

  **Nota:** Dopo avere applicato la patch, viene visualizzato un messaggio che invita a riavviare il sistema. Ignorare il riavvio fino al completamento del passaggio successivo `zypper up`.

  ---

- `zypper up`

**3d** Al termine dell'upgrade, avviare lo stack del cluster.

```
rcpacemaker 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 Sentinel).

**5b** Arrestare lo stack del cluster.

```
rcpacemaker stop
```

Arrestando lo stack del cluster le risorse rimangono inaccessibili e si evita il fencing dei nodi.

**5c** Soddisfare i prerequisiti elencati in "Prerequisiti per il processo di upgrade dell'applicazione" a pagina 167.

**5d** Effettuare il download degli aggiornamenti per Sentinel.

Per eseguire l'upgrade di Sentinel, eseguire i comandi seguenti dal prompt dei comandi:

- `zypper -v patch`

**Nota:** Una volta eseguito tale comando, viene visualizzato un messaggio che invita a riavviare il sistema. Ignorare il riavvio finché al completamento del Passo 8 a pagina 241.

- `zypper up`
- (Condizionale) Prima dell'upgrade, se è abilitata la visualizzazione degli eventi, dopo aver eseguito l'upgrade a Sentinel 8.4.0.0, Elasticsearch viene arrestato poiché viene abilitato con il plug-in di sicurezza X-Pack; per avviare Elasticsearch, attenersi alla procedura descritta in "Impostazioni in Elasticsearch per la comunicazione cluster sicura" a pagina 184.

**5e** Al termine dell'upgrade:

- (Condizionale) Se Sentinel non viene avviato automaticamente, avviare il database di Sentinel:

  ```
  rcsentinel startdb
  ```

- Avviare lo stack del cluster:

  ```
  rcpacemaker start
  ```

**5f** 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 sia stato eseguito correttamente:

```
rcsentinel version
```

**9** Riavviare il sistema in base al messaggio `zypper patch` illustrato al passaggio 5d.

**10** Eseguire il login a Sentinel e verificare che vengano visualizzati i dati di cui è stata eseguita la migrazione, ad esempio avvisi, dashboard di Security Intelligence e così via.

**11** Ora i dati in MongoDB sono ridondanti poiché Sentinel 8.3 e versioni successive memorizzerà i dati solo in PostgreSQL. Per liberare spazio su disco, eliminare i dati. Per ulteriori informazioni, consultare "Rimozione dei dati da MongoDB" a pagina 183.

## Esecuzione dell'upgrade tramite la console di gestione dell'applicazione Sentinel

**Per eseguire l'upgrade tramite la console di gestione dell'applicazione Sentinel:**

**1** Per abilitare la modalità di manutenzione, eseguire il comando seguente sul nodo attivo o su un nodo passivo del 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.

**2** 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.

**3** Eseguire prima l'upgrade di tutti i nodi passivi del cluster:

**3a** Eseguire il comando seguente per arrestare lo stack del cluster:

```
rcpacemaker stop
```

Arrestando lo stack del cluster le risorse rimangono inaccessibili e si evita il fencing dei nodi.

**3b** Eseguire il comando seguente per verificare che la porta 9443 sia in ascolto sul nodo attivo per accedere all'applicazione:

```
netstat –na | grep 9443
```

**3c** (Condizionale) Se la porta 9443 non è in ascolto, eseguire il comando seguente:

```
systemctl restart vabase vabase-jetty vabase-datamodel
```

**3d** Soddisfare i prerequisiti 1 e 2 elencati in "Prerequisiti per il processo di upgrade dell'applicazione" a pagina 167

**3e** Avviare l'applicazione effettuando una delle seguenti operazioni:

- Eseguire il login a Sentinel e fare clic su **Sentinel Main** > **Applicazione**.
- Specificare l'URL seguente nel browser Web: `https://<Indirizzo_IP>:9443`.

**3f** (Condizionale) Se non è possibile avviare la console di gestione dell'applicazione Sentinel:

**3f1** Accedere a `/var/opt/novell` nel nodo attivo e copiare i seguenti file in `/var/opt/novell/` in ciascun nodo passivo:

- `datamodel-service`
- `ganglia`
- `Jetty`
- `python`
- `va`

**3f2** In ogni nodo passivo, impostare l'autorizzazione del file su `vabase-jetty` per i file nella cartella `jetty`:

1. Accedere a `/var/opt/novell/jetty`.
2. Eseguire il comando seguente:

```
chown -R vabase-jetty:vabase-jetty *
```

**3f3** Per riavviare i servizi vabase, eseguire il comando seguente:

```
systemctl start vabase-jetty vabase-datamodel vabase
```

**3f4** Per verificare che la porta 9443 sia in ascolto in tutti i nodi disponibili, eseguire il comando seguente:

```
netstat -na | grep 9443
```

**3g** Eseguire il login come utente `vaadmin`.

**3h** Fare clic su **Aggiornamento online**.

**3h1** (Condizionale) Effettuare la registrazione per gli aggiornamenti se non è stata effettuata in precedenza. Per ulteriori informazioni, consultare "Registrazione degli aggiornamenti" a pagina 93.

---

**Nota:** Viene visualizzato un messaggio che invita a riavviare il sistema dopo il passo 5h2 ma ignorarlo fino al completamento del passaggio 5h3.

---

**3h2** Per installare gli aggiornamenti visualizzati per Sentinel e il sistema operativo, fare clic su **Update Now (Aggiorna ora)** > **OK**.

---

**3h3** **Nota:** Per Sentinel 8.3.1, oltre al passaggio 5h2, è necessario anche il comando`zypper up` poiché per l'applicazione sono richiesti sia gli rpm aggiornati che quelli nuovi.

---

Eseguire il seguente comando dal prompt dei comandi per eseguire l'upgrade completo dell'rpm:

```
zypper up
```

**3h4** Per applicare gli aggiornamenti installati, fare clic su **Reboot (Riavvia)**.

**3h5** Dopo il riavvio, controllare la versione nell'angolo in alto a destra dello schermo per verificare che l'upgrade abbia avuto esito positivo.

**3i** Al termine dell'upgrade, riavviare lo stack del cluster.

```
rcpacemaker start
```

**4** Eseguire l'upgrade del nodo attivo del cluster.

**4a** Soddisfare i prerequisiti elencati in "Prerequisiti per il processo di upgrade dell'applicazione" a pagina 167.

**4b** Ripetere i passaggi da 5h1 a 5h3 per il nodo attivo del cluster.

**4c** (Condizionale) Avviare Sentinel, se non viene avviato automaticamente:

```
rcsentinel start
```

**4d** Al termine dell'upgrade, riavviare lo stack del cluster:

```
rcpacemaker start
```

**5** Per disabilitare la modalità di manutenzione, eseguire il comando seguente sul nodo attivo o su un nodo passivo del cluster:

```
crm configure property maintenance-mode=false
```

**6** Per verificare che la modalità di manutenzione non sia attiva, eseguire il comando seguente sul nodo attivo o su un nodo passivo del cluster:

```
crm status
```

7 (Condizionale) Prima dell'upgrade, se è abilitata la visualizzazione degli eventi, dopo aver eseguito l'upgrade a Sentinel 8.4.0.0, Elasticsearch viene arrestato poiché viene abilitato con il plug-in di sicurezza X-Pack; per avviare Elasticsearch, attenersi alla procedura descritta in "Impostazioni in Elasticsearch per la comunicazione cluster sicura" a pagina 184.

8 Ora riavviare il sistema in base al messaggio `zypper patch` illustrato al passaggio 5h2.

9 Dopo il riavvio, controllare la versione nell'angolo in alto a destra dello schermo per verificare che l'upgrade abbia avuto esito positivo.

10 Eseguire il login a Sentinel e verificare che vengano visualizzati i dati di cui è stata eseguita la migrazione, ad esempio avvisi, dashboard di Security Intelligence e così via.

11 Ora i dati in MongoDB sono ridondanti poiché Sentinel 8.3 e versioni successive memorizzerà i dati solo in PostgreSQL. Per liberare spazio su disco, eliminare i dati. Per ulteriori informazioni, consultare "Rimozione dei dati da MongoDB" a pagina 183.

# 41 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 Sentinel) 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 Sentinel) 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.



## La proprietà cluster Default-Resource-Stickiness è obsoleta

**Problema:** L'uso del comando `crm` per impostare o modificare la proprietà di configurazione (ad esempio: `crm configure property maintenance-mode=true`), mostra il seguente messaggio:

```
ERROR: DEBUG: Cluster properties: cib-bootstrap-options-default-resource-
stickiness: moving default-resource-stickiness under rsc_defaults as
resource-stickiness unless already defined there
WARNING: cib-bootstrap-options: unknown attribute 'default-resource-
stickiness'
```

**Correzione:** Tale messaggio viene visualizzato se è stato eseguito l'upgrade della versione precedente di SLE HAE alla nuova versione nel prodotto Sentinel, in genere da SLES 12 SP3 a SLES 12 SP5 o versioni successive. Questa modifica non ha alcun impatto sulla funzionalità. Per ulteriori informazioni, fare riferimento al seguente articolo della Knowledge Base di SUSE.

# Impossibile configurare RCM/RCE utilizzando l'IP virtuale nella configurazione ad alta disponibilità

## Problema:

Impossibile configurare RCM/RCE utilizzando l'IP virtuale. L'host non è raggiungibile tramite nome host.

## Correzione:

### Tradizionale ad alta disponibilità

**Eseguire i seguenti passaggi per connettere RCM/RCE in modalità tradizionale ad alta disponibilità sia per la nuova configurazione che per quella esistente:**

1. Aggiungere una voce al file `/etc/hosts` come indicato di seguito nella casella RCM/RCE prima di installare/configurare RCM/RCE.

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   Ad esempio: 164.99.87.27 primo_host_attivo.nome.dom primo_host_attivo

   ---

   **Importante:** Assicurarsi che questa voce corrisponda sempre al primo nome host del nodo attivo corretto nell'ambiente ad alta disponibilità specificato nel file`/etc/hosts` prima di eseguire `configure.sh`

   ---

2. Alla richiesta visualizzata durante la connessione di RCM/RCE al server, fornire l'IP virtuale.

   ---

   **Importante:** Sebbene il primo nodo attivo corretto sia inattivo e l'altro nodo sia attualmente attivo, utilizzare comunque il nome del primo nodo attivo corretto con l'IP virtuale nel file `/etc/hosts`.

   ---

### Alta disponibilità dell'applicazione

**Eseguire i seguenti passaggi per connettere RCM/RCE in modalità ad alta disponibilità dell'applicazione per la nuova configurazione:**

- Utilizzare solo il nome host del primo nodo attivo corretto nel cluster ad alta disponibilità.

**Eseguire i seguenti passaggi per connettere RCM/RCE in modalità ad alta disponibilità dell'applicazione per la configurazione esistente:**

1. Aggiungere una voce al file `/etc/hosts` come indicato di seguito nella casella RCM/RCE prima di installare/configurare RCM/RCE.

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   Ad esempio: 164.99.87.27 primo_host_attivo.nome.dom primo_host_attivo

   ---

   **Importante:** Assicurarsi che questa voce corrisponda sempre al primo nome host del nodo attivo corretto nell'ambiente ad alta disponibilità specificato nel file`/etc/hosts` prima di eseguire `configure.sh`

   ---

2. Alla richiesta visualizzata durante la connessione di RCM/RCE al server, fornire l'IP virtuale.

   ---

   **Importante:** Sebbene il primo nodo attivo corretto sia inattivo e l'altro nodo sia attualmente attivo, utilizzare comunque il nome del primo nodo attivo corretto con l'IP virtuale nel file `/etc/hosts`.

   ---

# In ambiente DHCP, l'icona dell'interfaccia utente Web del server Sentinel dalla pagina dell'applicazione server Sentinel reindirizza a una pagina vuota

**Problema:** l'icona dell'interfaccia utente Web del server Sentinel dalla pagina dell'applicazione server Sentinel apre una pagina bloccata vuota nell'ambiente DHCP.

**Soluzione:** eseguire i passaggi seguenti:

1. Accedere al menu **YaST**.
2. Passare a **System > Network Settings > IPv6 protocol Setting** (Sistema > Impostazioni di rete > Impostazione protocollo IPv6).
3. Disabilitare IPv6 e salvare.
4. Riavviare il computer.

# Impossibile connettersi a Transformation Hub (T-Hub) dopo aver specificato l'indirizzo IP/il nome host corretto

Nel caso in cui il server Sentinel non sia in grado di comunicare con T-Hub anche se T-Hub è raggiungibile e tutti i certificati di T-Hub sono stati copiati sul server Sentinel, eseguire i passaggi seguenti:

1. Accedere alla directory `/etc/opt/novell/sentinel/intelligence` nel server Sentinel.
2. Eliminare il file `avro-schema-file-V1.json`
3. Riavviare il server Sentinel:

   ```
   rcsentinel restart
   ```

Il riavvio del server Sentinel rigenera il file dello schema e l'utente sarà in grado di stabilire una connessione corretta a T-Hub.

# 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/*;
   ```

to

```
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
```

# 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 si chiude 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 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"
   ```

   to

   ```
   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 di Sentinel

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 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).

# Task successivi alla disinstallazione di Sentinel

La disinstallazione del server Sentinel non include la rimozione dell'utente amministratore di Sentinel dal sistema operativo. L'operazione deve essere eseguita manualmente.

Dopo aver disinstallato Sentinel, alcune impostazioni di sistema rimangono invariate. È necessario rimuovere le impostazioni prima di eseguire una nuova installazione di Sentinel, soprattutto se si sono verificati errori durante la disinstallazione di Sentinel.

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.