



# NetIQ® Sentinel™

## Guida all'installazione e alla configurazione

**Febbraio 2015**

## Note legali

NetIQ Sentinel è protetto dal brevetto n° 05829001 rilasciato negli Stati Uniti.

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

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

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

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

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

© 2015 NetIQ Corporation. Tutti i diritti riservati. Per informazioni sui marchi di fabbrica di NetIQ, vedere <http://www.netiq.com/company/legal/>.

---

# Sommario

<b>Informazioni sulla Guida e la raccolta di documentazione</b>	<b>9</b>
<b>Informazioni su NetIQ Corporation</b>	<b>11</b>
<b>Parte I Informazioni su Sentinel</b>	<b>13</b>
<b>1 Cos'è Sentinel?</b>	<b>15</b>
1.1 Sfide da affrontare per rendere sicuro l'ambiente IT	15
1.2 La soluzione Sentinel	16
<b>2 Le funzioni di Sentinel</b>	<b>19</b>
2.1 Origini evento	21
2.2 Evento Sentinel	21
2.2.1 Servizio di mappatura	22
2.2.2 Streaming delle mappe	22
2.2.3 Rilevamento degli exploit (Servizio di mappatura)	22
2.3 Gestione servizi di raccolta	23
2.3.1 Servizi di raccolta	23
2.3.2 Connettori	23
2.4 Gestione agenti	24
2.5 Gestione servizi di raccolta NetFlow	24
2.6 Instradamento e memorizzazione dei dati di Sentinel	24
2.7 Correlazione	25
2.8 Security Intelligence	26
2.9 Contromisure per incidenti	26
2.10 Workflow iTRAC	26
2.11 Azioni e integratori	26
2.12 Esecuzione di ricerche	27
2.13 Rapporti	27
2.14 Controllo delle identità	27
2.15 Analisi evento	27
<b>Parte II Pianificazione dell'installazione di Sentinel</b>	<b>29</b>
<b>3 Elenco di controllo per l'implementazione</b>	<b>31</b>
<b>4 Informazioni sulla licenza</b>	<b>33</b>
4.1 Licenze di Sentinel	35
4.1.1 Licenza di valutazione	35
4.1.2 Licenza gratuita	36
4.1.3 Licenze aziendali	36
<b>5 Requisiti di sistema</b>	<b>37</b>
5.1 Requisiti di sistema relativi al connettore e al servizio di raccolta	37
5.2 Ambiente virtuale	37

<b>6</b>	<b>Considerazioni sull'installazione</b>	<b>39</b>
6.1	Vantaggi delle installazioni distribuite . . . . .	39
6.1.1	Vantaggi apportati dalla presenza di più Gestioni servizi di raccolta . . . . .	40
6.1.2	Vantaggi derivanti dall'uso di istanze aggiuntive del motore di correlazione . . . . .	40
6.1.3	Vantaggi apportati dalla presenza di più istanze di Gestione servizi di raccolta NetFlow . . . . .	41
6.2	Installazione all-in-one . . . . .	41
6.3	Installazione distribuita a un livello . . . . .	42
6.4	Installazione distribuita a un livello con alta disponibilità . . . . .	43
6.5	Installazione distribuita a due e tre livelli . . . . .	44
6.6	Pianificazione delle partizioni per la memorizzazione dei dati . . . . .	45
6.6.1	Utilizzo delle partizioni in installazioni tradizionali . . . . .	46
6.6.2	Utilizzo delle partizioni in installazioni in modalità applicazione . . . . .	46
6.6.3	Best practice per il layout delle partizioni . . . . .	46
6.6.4	Struttura delle directory di Sentinel . . . . .	47
<b>7</b>	<b>Considerazione sull'installazione per la modalità FIPS140-2</b>	<b>49</b>
7.1	Implementazione di FIPS in Sentinel . . . . .	49
7.1.1	Pacchetti NSS di RHEL . . . . .	49
7.1.2	Pacchetti NSS di SLES . . . . .	50
7.2	Componenti di Sentinel che supportano FIPS . . . . .	50
7.3	Elenco di controllo per l'implementazione . . . . .	51
7.4	Scenari di distribuzione . . . . .	51
7.4.1	Scenario 1: raccolta dati esclusivamente in modalità FIPS 140-2 . . . . .	52
7.4.2	Scenario 2: raccolta dati parzialmente in modalità FIPS 140-2 . . . . .	53
<b>8</b>	<b>Porte utilizzate</b>	<b>55</b>
8.1	Porte del server Sentinel . . . . .	56
8.1.1	Porte locali . . . . .	56
8.1.2	Porte di rete . . . . .	56
8.1.3	Porte specifiche per l'applicazione server Sentinel . . . . .	57
8.2	Porte di Gestione servizi di raccolta . . . . .	58
8.2.1	Porte di rete . . . . .	58
8.2.2	Porte specifiche per l'applicazione Gestione servizi di raccolta . . . . .	58
8.3	Porte del motore di correlazione . . . . .	59
8.3.1	Porte di rete . . . . .	59
8.3.2	Porte specifiche per l'applicazione Motore di correlazione . . . . .	59
8.4	Porte di Gestione servizi di raccolta NetFlow . . . . .	60
<b>9</b>	<b>Opzioni di installazione</b>	<b>61</b>
9.1	Installazione tradizionale . . . . .	61
9.2	Installazione in modalità applicazione . . . . .	62

<b>Parte III Installazione di Sentinel</b>	<b>63</b>
<b>10 Panoramica relativa all'installazione</b>	<b>65</b>
<b>11 Elenco di controllo per l'installazione</b>	<b>67</b>
<b>12 Installazione tradizionale</b>	<b>69</b>
12.1 Informazioni sulle opzioni di installazione . . . . .	69
12.2 Installazione interattiva. . . . .	70
12.2.1 Installazione standard . . . . .	70
12.2.2 Installazione personalizzata. . . . .	71
12.3 Installazione in modalità automatica . . . . .	73
12.4 Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione . . . . .	73
12.4.1 Elenco di controllo per l'installazione. . . . .	74
12.4.2 Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione . . . . .	74
12.4.3 Aggiunta di un utente personalizzato ActiveMQ per Gestione servizi di raccolta o il motore di correlazione . . . . .	75
12.5 Installazione di Sentinel come utente non root. . . . .	76
<b>13 Installazione in modalità applicazione</b>	<b>79</b>
13.1 Installazione dell'applicazione Sentinel ISO. . . . .	79
13.1.1 Prerequisiti. . . . .	79
13.1.2 Installazione di Sentinel. . . . .	80
13.1.3 Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione . . . . .	81
13.2 Installazione dell'applicazione Sentinel OVF . . . . .	82
13.2.1 Installazione di Sentinel. . . . .	83
13.2.2 Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione . . . . .	84
13.3 Configurazione dell'applicazione successiva all'installazione . . . . .	84
13.3.1 Configurazione di WebYaST . . . . .	85
13.3.2 Creazione di partizioni . . . . .	85
13.3.3 Registrazione degli aggiornamenti . . . . .	86
13.3.4 Configurazione dell'applicazione con SMT . . . . .	86
13.4 Interruzione e avvio del server mediante WebYaST . . . . .	87
<b>14 Installazione di Gestione servizi di raccolta NetFlow</b>	<b>89</b>
14.1 Elenco di controllo per l'installazione . . . . .	89
14.2 Procedura di installazione di Gestione servizi di raccolta NetFlow . . . . .	89
<b>15 Installazione di servizi di raccolta e connettori aggiuntivi</b>	<b>91</b>
15.1 Installazione di un servizio di raccolta . . . . .	91
15.2 Installazione di un connettore. . . . .	91
<b>16 Verifica dell'installazione</b>	<b>93</b>
<b>Parte IV Configurazione di Sentinel</b>	<b>95</b>
<b>17 Orario di configurazione</b>	<b>97</b>
17.1 L'orario in Sentinel . . . . .	97
17.2 Configurazione dell'orario in Sentinel. . . . .	99

17.3	Configurazione della soglia di ritardo degli eventi	99
17.4	Gestione dei fusi orari	99
<b>18</b>	<b>Modificare la configurazione dopo l'installazione</b>	<b>103</b>
<b>19</b>	<b>Configurazione dei plug-in pronti all'uso</b>	<b>105</b>
19.1	Visualizzazione dei plug-in preinstallati	105
19.2	Configurazione della raccolta di dati	105
19.3	Configurazione dei pacchetti soluzione	105
19.4	Configurazione di azioni e integratori	106
<b>20</b>	<b>Abilitazione della modalità FIPS 140-2 in un'installazione esistente di Sentinel</b>	<b>107</b>
20.1	Abilitazione dell'esecuzione in modalità FIPS 140-2 nel server Sentinel	107
20.2	Abilitazione della modalità FIPS 140-2 in istanze remote di Gestione servizi di raccolta e del motore di correlazione	107
<b>21</b>	<b>Esecuzione di Sentinel in modalità FIPS 140-2</b>	<b>109</b>
21.1	Configurazione del servizio Advisor in modalità FIPS 140-2	109
21.2	Configurazione della ricerca distribuita in modalità FIPS 140-2	109
21.3	Configurazione dell'autenticazione LDAP in modalità FIPS 140-2	111
21.4	Aggiornamento dei certificati del server nelle istanze remote di Gestione servizi di raccolta e del motore di correlazione	111
21.5	Configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2	112
21.5.1	Connettore di Gestione agenti	112
21.5.2	Connettore del database (JDBC)	113
21.5.3	Connettore di collegamento Sentinel	113
21.5.4	Connettore Syslog	114
21.5.5	Connettore degli eventi di Windows (WMI)	115
21.5.6	Integratore di Collegamento Sentinel	116
21.5.7	Integratore LDAP	117
21.5.8	Integratore SMTP	117
21.5.9	Utilizzo di connettori non FIPS con Sentinel in modalità FIPS 140-2	117
21.6	Importazione di certificati nel database di archivio chiavi FIPS	118
21.7	Ripristino di Sentinel nella modalità non FIPS	118
21.7.1	Ripristino del server Sentinel nella modalità non FIPS	118
21.7.2	Ripristino della modalità non FIPS in istanze remote di Gestione servizi di raccolta e del motore di correlazione	119
<b>Parte V</b>	<b>Esecuzione dell'upgrade di Sentinel</b>	<b>121</b>
<b>22</b>	<b>Elenco di controllo per l'implementazione</b>	<b>123</b>
<b>23</b>	<b>Prerequisiti</b>	<b>125</b>
23.1	Prerequisito per l'esecuzione di Sentinel in modalità FIPS	125
23.2	Prerequisito per versioni precedenti a Sentinel 7.1.1	125
<b>24</b>	<b>Upgrade dell'installazione tradizionale di Sentinel</b>	<b>127</b>
24.1	Esecuzione dell'upgrade di Sentinel	127

24.2	Upgrade di Sentinel come utente non root. . . . .	128
24.3	Upgrade di Gestione servizi di raccolta e del motore di correlazione . . . . .	130
<b>25</b>	<b>Esecuzione dell'upgrade dell'applicazione Sentinel</b>	<b>131</b>
25.1	Esecuzione dell'upgrade dell'applicazione mediante Zypper. . . . .	131
25.2	Esecuzione dell'upgrade dell'applicazione mediante WebYaST . . . . .	132
25.3	Esecuzione dell'upgrade dell'applicazione mediante SMT. . . . .	134
<b>26</b>	<b>Esecuzione dell'upgrade dei plug-in di Sentinel</b>	<b>137</b>
<b>Parte VI</b>	<b>Installazione di Sentinel per alta disponibilità</b>	<b>139</b>
<b>27</b>	<b>Concetti</b>	<b>141</b>
27.1	Sistemi esterni . . . . .	141
27.2	Memorizzazione condivisa . . . . .	141
27.3	Monitoraggio dei servizi . . . . .	142
27.4	Fencing . . . . .	142
<b>28</b>	<b>Requisiti di sistema</b>	<b>145</b>
<b>29</b>	<b>Installazione e configurazione</b>	<b>147</b>
29.1	Configurazione iniziale . . . . .	148
29.2	Configurazione della memorizzazione condivisa . . . . .	149
29.2.1	Configurazione delle destinazioni iSCSI . . . . .	150
29.2.2	Configurazione degli iniziatori iSCSI . . . . .	151
29.3	Installazione di Sentinel . . . . .	152
29.3.1	Installazione nel primo nodo . . . . .	152
29.3.2	Installazione in nodi successivi . . . . .	154
29.4	Installazione del cluster . . . . .	155
29.5	Configurazione del cluster . . . . .	155
29.6	Configurazione delle risorse. . . . .	158
29.7	Configurazione della memorizzazione secondaria. . . . .	159
<b>30</b>	<b>Upgrade di Sentinel in configurazione ad alta disponibilità</b>	<b>161</b>
30.1	Prerequisiti . . . . .	161
30.2	Esecuzione dell'upgrade di un'installazione tradizionale ad alta disponibilità di Sentinel . . . . .	161
30.3	Esecuzione dell'upgrade di un'installazione in modalità applicazione ad alta disponibilità di Sentinel . . . . .	163
30.3.1	Esecuzione dell'upgrade dell'applicazione Sentinel ad alta disponibilità mediante Zypper . . . . .	163
30.3.2	Esecuzione dell'upgrade dell'applicazione Sentinel ad alta disponibilità mediante WebYaST. . . . .	165
<b>31</b>	<b>backup e recupero d'emergenza</b>	<b>167</b>
31.1	Backup . . . . .	167
31.2	PlateSpin . . . . .	167
31.2.1	Errore temporaneo. . . . .	167
31.2.2	Danneggiamento dei nodi . . . . .	167
31.2.3	Configurazione dei dati del cluster. . . . .	168

<b>Parte VII</b>	<b>Appendici</b>	<b>169</b>
<b>A</b>	<b>Soluzione dei problemi</b>	<b>171</b>
A.1	Installazione non riuscita a causa di una configurazione della rete non corretta . . . . .	171
A.2	Non viene creato l'UUID per le Gestioni servizi di raccolta o il Motore di raccolta . . . . .	171
A.3	Dopo aver eseguito il login l'interfaccia Web appare vuota in Internet Explorer . . . . .	171
<b>B</b>	<b>Disinstallazione</b>	<b>173</b>
B.1	Elenco di controllo per la disinstallazione. . . . .	173
B.2	Disinstallazione di Sentinel. . . . .	173
B.2.1	Disinstallazione del server Sentinel. . . . .	173
B.2.2	Disinstallazione di Gestione servizi di raccolta e del motore di correlazione. . . . .	174
B.2.3	Disinstallazione di Gestione servizi di raccolta NetFlow . . . . .	174
B.3	Task successivi alla disinstallazione. . . . .	175

---

# Informazioni sulla Guida e la raccolta di documentazione

La *Guida all'installazione e alla configurazione* contiene informazioni introduttive su NetIQ 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 NetIQ Corporation

NetIQ Corporation è una società globale di software per le aziende, focalizzata su tre problematiche costanti dell'ambiente aziendale - cambiamento, complessità e rischio - e che offre soluzioni utili per gestirle.

## Il nostro punto di vista

### **Adattamento al cambiamento e gestione della complessità: sfide ben note**

Fra tutte le sfide da affrontare, queste sono forse le variabili principali che impediscono il controllo necessario a misurare, monitorare e gestire in modo sicuro gli ambienti informatici fisici, virtuali e cloud.

### **Erogazione migliore e più rapida dei servizi aziendali di importanza critica**

Siamo convinti del fatto che le nostre soluzioni per assicurare il massimo controllo possibile alle organizzazioni IT siano il solo percorso verso un'erogazione tempestiva ed economica dei servizi. Il costante processo di cambiamento delle organizzazioni e la maggiore complessità intrinseca delle tecnologie necessarie per gestirlo continueranno ad esercitare pressioni sempre più forti.

## La nostra filosofia

### **Vendiamo soluzioni intelligenti e non semplice software**

Al fine di poter garantire un controllo affidabile, prima di tutto ci dedichiamo a comprendere le situazioni reali in cui le organizzazioni IT operano quotidianamente. Questo approccio è il solo che consenta di sviluppare soluzioni IT pratiche e intelligenti, capaci di garantire risultati misurabili e comprovati, e che ci gratifica molto di più della semplice vendita di software.

### **Il successo degli utenti è il nostro stimolo**

Il fulcro attorno al quale ruota la nostra attività aziendale è il successo degli utenti. Dall'ideazione del prodotto alla sua installazione, non dimentichiamo mai l'esigenza di poter contare su soluzioni IT funzionanti e che si integrino alla perfezione con i prodotti esistenti, fornendovi supporto costante e formazione successiva all'installazione oltre che, tanto per cambiare, essendo un partner con cui è veramente facile collaborare. In sintesi: il successo degli utenti è il nostro successo.

## Le nostre soluzioni

- ◆ Governance di identità e accessi
- ◆ Gestione degli accessi
- ◆ Gestione sicurezza
- ◆ Gestione di sistemi e applicazioni

- ♦ Gestione dei carichi di lavoro
- ♦ Gestione servizio

## Contattare l'assistenza alle vendite

Per informazioni su prodotti, prezzi e funzionalità, rivolgersi al partner locale. In caso d'impossibilità, contattare il team di assistenza alle vendite.

<b>Sedi globali:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>Stati Uniti e Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Sito Web:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contattare il supporto tecnico

Per problemi specifici del prodotto, rivolgersi al team del supporto tecnico.

<b>Sedi globali:</b>	<a href="http://www.netiq.com/support/contactinfo.asp">www.netiq.com/support/contactinfo.asp</a>
<b>Nord e Sud America:</b>	1-713-418-5555
<b>Europa, Medio Oriente e Africa:</b>	+353 (0) 91-782 677
<b>Email:</b>	<a href="mailto:support@netiq.com">support@netiq.com</a>
<b>Sito Web:</b>	<a href="http://www.netiq.com/support">www.netiq.com/support</a>

## Contattare il supporto per la documentazione

NetIQ desidera fornire tutta la documentazione necessaria per indicare le soluzioni più appropriate alle esigenze degli utenti. Per inviare suggerimenti di miglioramento, fare clic su **comments on this topic** (commenti su questo argomento) in fondo a qualsiasi pagina nelle versioni in HTML della documentazione pubblicata sul sito Web [www.netiq.com/documentation](http://www.netiq.com/documentation). È inoltre possibile inviare un'e-mail a [Documentation-Feedback@netiq.com](mailto:Documentation-Feedback@netiq.com). La collaborazione degli utenti è una fonte preziosa e saremo lieti di ricevere qualsiasi suggerimento.

## Contattare la comunità online di utenti

La comunità online di NetIQ, Qmunity, è una rete collaborativa che unisce utenti ed esperti di NetIQ. È una risorsa che contribuisce ad acquisire la conoscenza approfondita necessaria a sfruttare a pieno il potenziale degli investimenti IT fondamentali, in quanto offre informazioni più immediate, collegamenti e risorse utili e accesso agli esperti di NetIQ. Per ulteriori informazioni, visitare il sito <http://community.netiq.com>.

---

# Informazioni su Sentinel

In questa sezione sono descritte dettagliatamente le caratteristiche di Sentinel e come questa soluzione consenta di gestire gli eventi all'interno dell'organizzazione.

- ◆ [Capitolo 1, "Cos'è Sentinel?", a pagina 15](#)
- ◆ [Capitolo 2, "Le funzioni di Sentinel", a pagina 19](#)



# 1 Cos'è Sentinel?

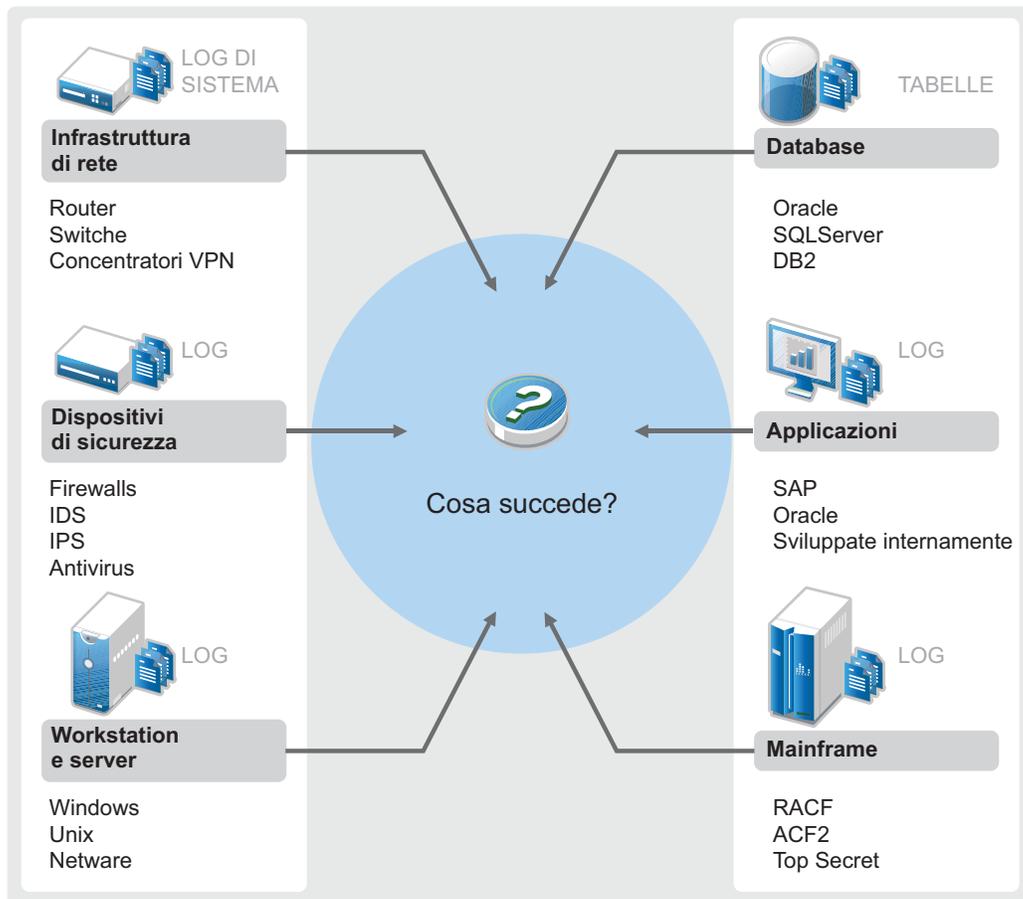
Sentinel è una soluzione SIEM (Security, Information and Event Management) e di monitoraggio della conformità. che monitora automaticamente gli ambienti IT più complessi e garantisce la sicurezza necessaria per proteggerli.

- ♦ Sezione 1.1, "Sfide da affrontare per rendere sicuro l'ambiente IT", a pagina 15
- ♦ Sezione 1.2, "La soluzione Sentinel", a pagina 16

## 1.1 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. Numerose applicazioni, database, mainframe, workstation e server di vario tipo generano log specifici degli eventi. A questi si aggiungono i dispositivi di sicurezza e quelli dell'infrastruttura di rete, ognuno dei quali fornisce log relativi a quanto avviene nell'ambiente IT.

*Figura 1-1 Eventi dell'ambiente IT*



Le sfide derivano dai fattori elencati di seguito:

- ♦ Nell'ambiente IT sono presenti numerosi dispositivi.
- ♦ I log sono in formati diversi.
- ♦ I log sono memorizzati in silos.
- ♦ I log generano una grande quantità di informazioni.
- ♦ Per individuare i responsabili dei vari eventi è necessario analizzare tutti i log manualmente.

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

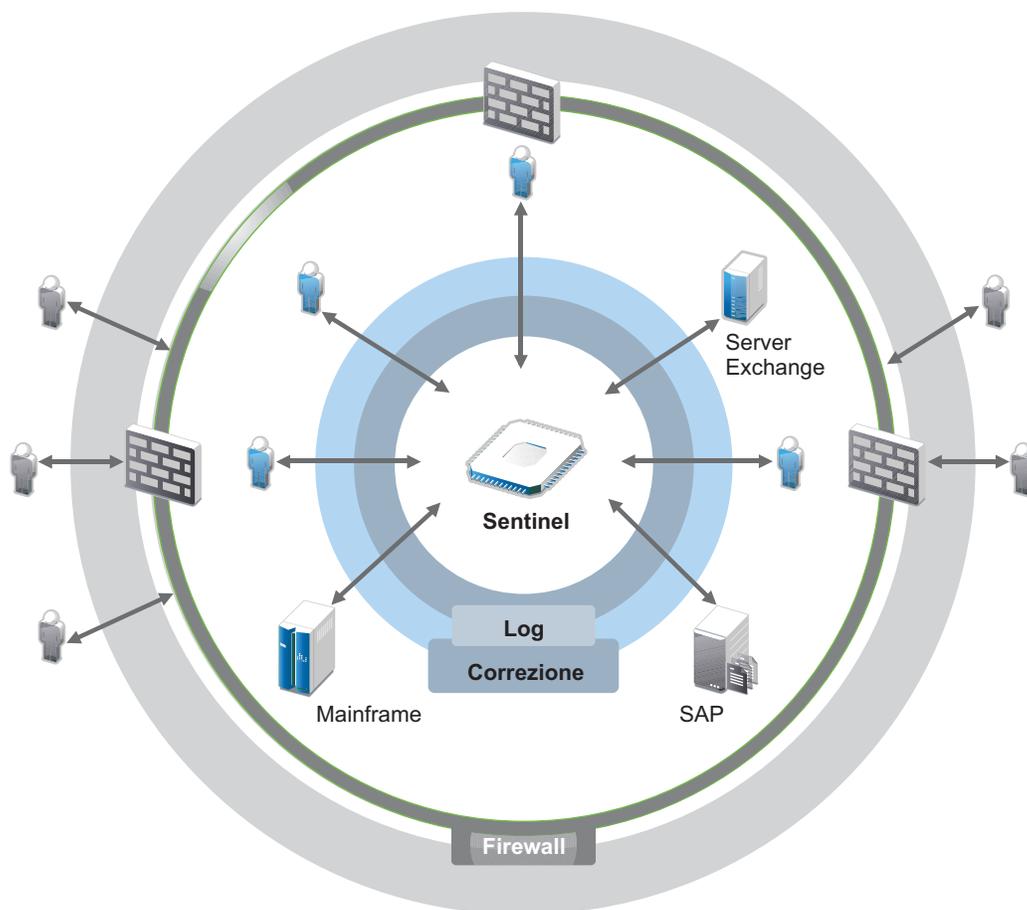
- ♦ Raccogliere i dati.
- ♦ Consolidare i dati.
- ♦ Standardizzazione di dati di tipo diverso in eventi facilmente confrontabili.
- ♦ Mappare gli eventi a normative standard.
- ♦ Analizzare i dati.
- ♦ Confrontare gli eventi di più sistemi per stabilire se sussistono problemi per la sicurezza.
- ♦ Inviare 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 le sfide da affrontare per rendere sicuro l'ambiente IT, è necessario stabilire come rendere sicura l'azienda per gli utenti ma anche come proteggerla da essi senza trattarli come malintenzionati o sovraccaricarli al punto da azzerarne la produttività. Sentinel vi offre la soluzione.

## 1.2 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 e 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 preciso momento e avere la possibilità di collegare le azioni intraprese sulle risorse alle persone che le intraprendono. In questo modo potrete conoscere i comportamenti degli utenti e monitorare efficacemente il controllo. A prescindere dal fatto che l'utente sia un interno o un esterno, è possibile raggruppare tutte le azioni che svolge e quindi individuare le attività non autorizzate prima che arrechino danni.

Sentinel svolge queste funzioni senza gravare eccessivamente sui costi poiché:

- ◆ Offre un'unica soluzione per gestire i controlli IT in funzione di normative diverse..
- ◆ Colma il gap cognitivo fra ciò che le norme prevedono e quello che effettivamente avviene nell'ambiente di rete.
- ◆ Dimostra ai revisori e ai funzionari che l'organizzazione documenta, monitora e genera rapporti sui controlli di sicurezza.
- ◆ Include programmi di monitoraggio della conformità e di reportistica pronti all'uso.
- ◆ Consente di acquisire la visibilità e il controllo necessari per verificare costantemente la conformità dell'organizzazione e i programmi di sicurezza.

Sentinel automatizza i processi di raccolta dei log, analisi e generazione dei rapporti affinché i controlli IT soddisfino efficacemente le esigenze di rilevamento delle minacce e revisione. Sentinel fornisce un monitoraggio automatizzato degli eventi di sicurezza, degli eventi di conformità e dei controlli IT, consentendo di intervenire tempestivamente qualora si produca una violazione alla sicurezza o un evento di non conformità. Inoltre, Sentinel permette di raccogliere facilmente le informazioni di riepilogo relative all'ambiente, affinché sia possibile comunicare alle principali parti interessate la condizione generale rispetto alla sicurezza.

---

# 2 Le funzioni di Sentinel

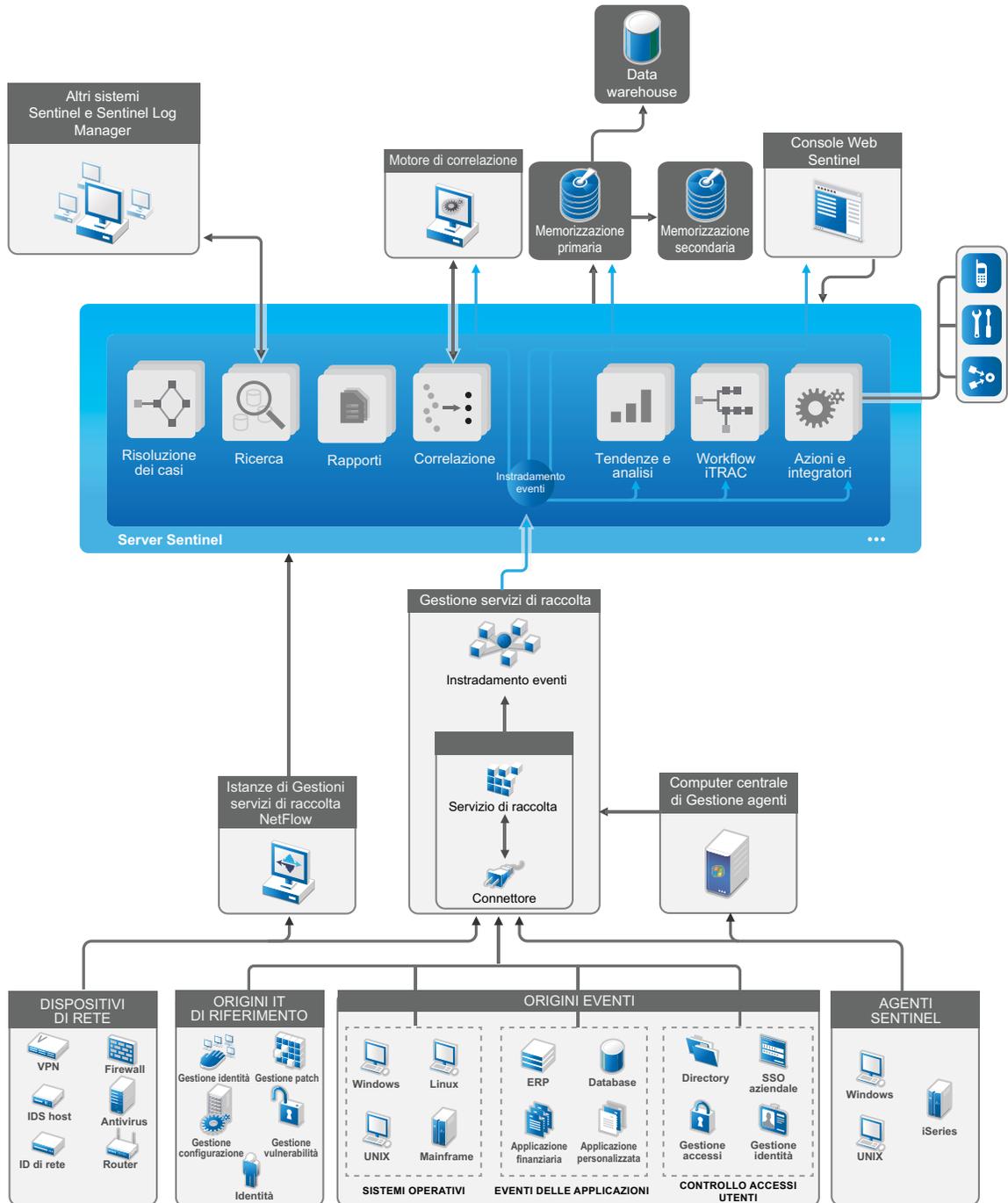
Sentinel gestisce costantemente le informazioni e gli eventi relativi alla sicurezza sfruttando l'ambiente IT dell'utente per fornire una soluzione di monitoraggio completa.

Le funzioni di Sentinel sono:

- ♦ Raccolta di log, eventi e informazioni sulla sicurezza da tutte le diverse origini degli eventi presenti nell'ambiente IT.
- ♦ Standardizzazione in un unico formato di log, eventi e informazioni sulla sicurezza.
- ♦ Memorizzazione degli eventi in un datastore basato su file, con policy di permanenza dei dati flessibili e personalizzabili.
- ♦ Raccolta di dati del flusso della rete per facilitare il monitoraggio dettagliato delle attività di rete.
- ♦ Collegamento gerarchico di più sistemi Sentinel, incluso Sentinel Log Manager.
- ♦ Ricerca di eventi non solo nel server Sentinel locale, ma anche in altri 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 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.

La figura seguente illustra in che modo Sentinel svolge queste funzioni:

Figura 2-1 Architettura di Sentinel



Nelle sezioni seguenti si descrivono dettagliatamente i componenti di Sentinel:

- ◆ Sezione 2.1, "Origini evento", a pagina 21
- ◆ Sezione 2.2, "Evento Sentinel", a pagina 21
- ◆ Sezione 2.3, "Gestione servizi di raccolta", a pagina 23
- ◆ Sezione 2.4, "Gestione agenti", a pagina 24

- ♦ Sezione 2.5, “Gestione servizi di raccolta NetFlow”, a pagina 24
- ♦ Sezione 2.6, “Instradamento e memorizzazione dei dati di Sentinel”, a pagina 24
- ♦ Sezione 2.7, “Correlazione”, a pagina 25
- ♦ Sezione 2.8, “Security Intelligence”, a pagina 26
- ♦ Sezione 2.9, “Contromisure per incidenti”, a pagina 26
- ♦ Sezione 2.10, “Workflow iTRAC”, a pagina 26
- ♦ Sezione 2.11, “Azioni e integratori”, a pagina 26
- ♦ Sezione 2.12, “Esecuzione di ricerche”, a pagina 27
- ♦ Sezione 2.13, “Rapporti”, a pagina 27
- ♦ Sezione 2.14, “Controllo delle identità”, a pagina 27
- ♦ Sezione 2.15, “Analisi evento”, a pagina 27

## 2.1 Origini evento

Sentinel raccoglie informazioni ed eventi relativi alla sicurezza da diverse origini all'interno del vostro ambiente IT. Tali origini sono denominate origini degli eventi. e possono essere numerosi elementi diversi presenti sulla rete.

**Perimetro di sicurezza:** dispositivi di sicurezza di tipo hardware e software utilizzati per creare un perimetro di sicurezza intorno all'ambiente, fra i quali firewall, IDS e VPN.

**Sistemi operativi:** eventi di diversi sistemi operativi utilizzati nella rete.

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

**Eventi delle applicazioni:** eventi generati dalle applicazioni installate nella rete.

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

Per ulteriori informazioni sulla raccolta e le origini degli eventi, vedere [“Configurazione della raccolta dati senza agenti”](#).

## 2.2 Evento Sentinel

Sentinel riceve le informazioni dai dispositivi, le normalizza in una struttura denominata evento che, successivamente, categorizza e invia per l'elaborazione. Grazie all'aggiunta di informazioni categorizzate (tassonomia) agli eventi, questi possono essere comparati più semplicemente tra i sistemi che li segnalano secondo modalità distinte. Ad esempio, gli errori relativi all'autenticazione. Gli eventi vengono elaborati dal motore di correlazione con visualizzazione in tempo reale, dai dashboard e dal server di back-end.

Un evento contiene oltre 200 campi. I campi di un evento sono di vario tipo e vengono utilizzati per diversi scopi. Esistono alcuni campi predefiniti come, ad esempio, quelli che fanno riferimento alla gravità, la criticità, l'IP di destinazione e la porta di destinazione. Sono presenti due set di campi configurabili: i campi riservati, solo per uso interno di Sentinel, consentono espansioni future, mentre i campi personalizzati sono concepiti per permettere le estensioni dei clienti.

Lo scopo dei campi può comunque essere modificato mediante la loro ridenominazione. L'origine di un campo può essere esterna, vale a dire configurata esplicitamente dal dispositivo o dal servizio di raccolta corrispondente, oppure può essere referenziale. 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 definito come il codice di costruzione della struttura contenente la risorsa menzionata come l'IP di destinazione di un evento. Ad esempio, un campo può essere calcolato dal servizio di mappatura mediante una mappatura definita dal cliente che utilizza l'IP di destinazione dell'evento.

- ♦ [Sezione 2.2.1, “Servizio di mappatura”, a pagina 22](#)
- ♦ [Sezione 2.2.2, “Streaming delle mappe”, a pagina 22](#)
- ♦ [Sezione 2.2.3, “Rilevamento degli exploit \(Servizio di mappatura\)”, a pagina 22](#)

## 2.2.1 Servizio di mappatura

Il servizio di mappatura consente di elaborare un meccanismo complesso per propagare i dati aziendali rilevanti in tutto il sistema. Tali dati possono arricchire gli eventi con informazioni referenziali, fornendo il contesto necessario affinché gli analisti siano in grado di adottare le decisioni in modo più efficace, redattare rapporti più utili e scrivere regole di correlazioni più razionali.

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. Tali informazioni aggiuntive possono essere utilizzate per eseguire correlazioni o generare rapporti avanzati. Oltre a quelle personalizzate definite dall'utente, il sistema supporta diverse mappature incorporate.

Le mappature definite in Sentinel vengono memorizzate in due modi:

- ♦ Le mappature incorporate sono memorizzate nel database, vengono aggiornate mediante le API nel codice del servizio di raccolta 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 Gestione servizi di raccolta e applicate localmente. Questa elaborazione distribuita assicura che l'attività di mappatura non sovraccarichi il server principale.

## 2.2.2 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. L'importanza della capacità di streaming è particolarmente rilevante in un sistema in tempo reale mission-critical, ad esempio quello di Sentinel dove è necessario un movimento costante, prevedibile e veloce dell'indipendenza dei dati di qualsiasi carico transitorio sul sistema.

## 2.2.3 Rilevamento degli exploit (Servizio di mappatura)

Sentinel consente di creare riferimenti incrociati tra le firme dei dati relativi agli eventi e i dati della scansione delle vulnerabilità. Ciò consente di inviare una notifica immediata e automatica agli utenti quando un attacco cerca di penetrare in un sistema vulnerabile. Tale funzionalità è garantita da:

- ♦ feed di dati di Advisor
- ♦ rilevamento delle intrusioni
- ♦ scansione delle vulnerabilità
- ♦ Firewall

In Advisor è incluso un riferimento incrociato tra le firme dei dati relativi agli eventi e i dati relativi alla scansione delle vulnerabilità. Il feed di dati Advisor contiene informazioni relative alle vulnerabilità e alle minacce oltre che una normalizzazione delle firme eventi e dei plug-in di vulnerabilità. Per ulteriori informazioni su Advisor, vedere “[Detecting Vulnerabilities and Exploits](#)” (Rilevamento di vulnerabilità ed exploit) nella *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

## 2.3 Gestione servizi di raccolta

Gestione servizi di raccolta gestisce la raccolta dei dati, monitora i messaggi di stato del sistema e applica i filtri agli eventi in base secondo necessità. Le funzioni principali di Gestione servizi di raccolta sono:

- ◆ Trasformazione degli eventi.
- ◆ Aggiunta di pertinenza aziendale agli eventi mediante il servizio di mappatura.
- ◆ Instradamento degli eventi.
- ◆ Distinzione fra dati in tempo reale, vulnerabilità, risorse e dati non in tempo reale.
- ◆ Invio di un messaggio di stato al server Sentinel.

### 2.3.1 Servizi di raccolta

I servizi di raccolta raccolgono e standardizzano le informazioni provenienti dai connettori. Sono scritti in Javascript e definiscono la logica per:

- ◆ Ricezione dei dati non elaborati dai servizi di raccolta.
- ◆ Analisi sintattica e normalizzazione dei dati.
- ◆ Applicazione della logica di ripetibilità ai dati.
- ◆ Conversione dei dati specifici del dispositivo in dati specifici di Sentinel.
- ◆ Formattazione degli eventi.
- ◆ Passaggio dei dati normalizzati, analizzati sintatticamente e formattati a Gestione servizi di raccolta.
- ◆ Filtraggio degli eventi in base al dispositivo.

Per ulteriori informazioni sui servizi di raccolta, visitare il [sito Web dei plug-in di Sentinel](#).

### 2.3.2 Connettori

I connettori hanno la funzione di stabilire le connessioni fra le origini degli eventi e il sistema Sentinel. Per raccogliere gli eventi utilizzano protocolli standard del settore, quali Syslog, JDBC per leggere dalle tabelle dei database, WMI per leggere dai log degli eventi di Windows e così via. Le funzioni dei connettori sono:

- ◆ Trasporto dei dati evento non elaborati dalle origini evento al servizio di raccolta.
- ◆ Connessione per il filtraggio specifico.
- ◆ Connessione per la gestione degli errori.

## 2.4 Gestione agenti

Mediante Gestione agenti è possibile effettuare la raccolta dati basata sull'host, completando quella senza agenti al fine 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.

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

## 2.5 Gestione servizi di raccolta NetFlow

Gestione servizi di raccolta NetFlow raccoglie i dati del flusso di rete (NetFlow, IPFIX e così via) da dispositivi di rete quali router, switch e firewall. I dati del flusso di rete forniscono informazioni di base su tutte le connessioni di rete fra gli host, inclusi pacchetti e byte trasmessi, e sono utili per visualizzare il comportamento dei singoli host o dell'intera rete.

Le funzionalità di Gestione servizi di raccolta NetFlow sono:

- ♦ Raccolta dei dati del flusso di rete in byte, flussi e pacchetti dai dispositivi di rete supportati.
- ♦ Aggregazione e invio dei dati raccolti al server Sentinel per la visualizzazione e l'analisi delle attività di rete all'interno dell'ambiente.

Per ulteriori informazioni sulla visualizzazione e l'analisi dei dati del flusso di rete, vedere [“Visualizing and Analyzing Network Flow Data”](#) (Visualizzazione e analisi dei dati del flusso di rete) nella [NetIQ Sentinel User Guide](#) (Guida dell'utente di NetIQ Sentinel).

## 2.6 Instradamento e memorizzazione dei dati di Sentinel

In Sentinel sono disponibili numerose opzioni per instradare, memorizzare ed estrarre i dati raccolti. Per default, Sentinel riceve da Gestione servizi di raccolta due flussi di dati separati ma correlati: i dati degli eventi analizzati sintatticamente e i dati non elaborati. Questi ultimi vengono immediatamente memorizzati in partizioni protette per registrare una sequenza sicura di evidenze. I dati degli eventi analizzati sintatticamente vengono instradati in base alle regole definite dall'utente e possono essere filtrati, inviati alla memorizzazione e alla funzionalità di analisi in tempo reale, nonché instradati a sistemi esterni. Tutti i dati degli eventi che vengono inviati alla memorizzazione sono sottoposti a un'ulteriore analisi di corrispondenza rispetto alle policy di conservazione stabilite dall'utente, che determinano la partizione in cui risiedono i dati e definiscono inoltre la policy di pulizia per la conservazione dei dati degli eventi e la loro eliminazione.

La memorizzazione dei dati in Sentinel si basa su una struttura a tre livelli:

<b>Memorizzazione online</b>	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.
<b>Nota:</b> 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.		
<b>Memorizzazione offline</b>	Memorizzazione di archiviazione	Quando le partizioni sono chiuse, è possibile eseguirne il backup in una partizione offline come Amazon Glacier o simili. Se necessario, è possibile anche reimportare temporaneamente le partizioni per l'analisi forense 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, consultare [“Configurazione della memorizzazione dei dati”](#) nella *NetIQ Sentinel Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

## 2.7 Correlazione

Anche se un solo evento può sembrare irrilevante, in combinazione con altri eventi potrebbe informare sulla presenza di un problema potenziale. Sentinel consente di eseguire la correlazione di tali eventi nel Motore di correlazione grazie alle regole create e distribuite dall'utente, permettendo di intervenire nel modo più appropriato e attenuare tali problemi.

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

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

## 2.8 Security Intelligence

La funzione di correlazione di Sentinel consente di conoscere i modelli di attività, sia 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 alle serie di tempi, al fine di consentire agli analisti d'individuare e analizzare le deviazioni (anomalie) sia tramite un motore statistico automatico che mediante la rappresentazione visiva dei dati statistici per l'interpretazione manuale. Per ulteriori informazioni, vedere [“Analisi di tendenze nei dati”](#) nella *NetIQ Sentinel User Guide (Guida per l'utente di NetIQ Sentinel 7.0.1)*.

## 2.9 Contromisure per incidenti

Grazie alla gestione automatica delle risposte ai casi, Sentinel consente di documentare e formalizzare il processo di controllo, escalation e risposta ai casi e alle violazioni della sicurezza e garantisce una doppia integrazione con i sistemi di richiesta di assistenza. Sentinel consente di reagire tempestivamente e risolvere i casi in modo efficiente. Per ulteriori informazioni, vedere [“Configuring Incidents”](#) (Configurazione dei casi) nella *NetIQ Sentinel User Guide* (Guida dell'utente di NetIQ Sentinel 7.1).

## 2.10 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 agli incidenti. iTRAC sfrutta il sistema degli incidenti di Sentinel per controllare la sicurezza o i problemi del sistema dall'identificazione (mediante regole di correzione o identificazione manuale) fino alla risoluzione.

I workflow possono essere creati utilizzando procedure manuali o automatiche. Sono supportate funzioni avanzate quali diramazione, riassegnazione in base al tempo e variabili locali. L'integrazione con script e plug-in esterni consente l'interazione flessibile con sistemi di terze parti. I rapporti completi permettono agli amministratori di comprendere e ottimizzare i processi di risposta agli incidenti. Per ulteriori informazioni, vedere [“Configuring iTRAC Workflows \(Configurazione dei workflow di iTRAC\)”](#) in *NetIQ Sentinel User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

## 2.11 Azioni e integratori

In Sentinel le azioni eseguono manualmente o automaticamente operazioni di vario genere, come ad esempio l'invio di e-mail. Le azioni possono essere avviate 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 *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.1).

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

## 2.12 Esecuzione di ricerche

In Sentinel è disponibile un'opzione per effettuare ricerche degli eventi. È possibile effettuare la ricerca nell'ubicazione della memorizzazione primaria o secondaria. 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 [“Performing a Search”](#) (Esecuzione di una ricerca) nella *NetIQ Sentinel User Guide* (Guida dell'utente di NetIQ Sentinel).

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

## 2.13 Rapporti

Sentinel vi consente di creare rapporti sui dati raccolti. Viene fornito con un set completo di rapporti personalizzabili. Alcuni rapporti sono flessibili e consentono di specificare le colonne da visualizzare nei risultati.

È possibile eseguire, pianificare e inviare tramite 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 sui risultati. I rapporti possono anche essere eseguiti sui server Sentinel distribuiti in diverse ubicazioni geografiche. Per ulteriori informazioni, vedere [“Reporting \(Generazione di rapporti\)”](#) in *NetIQ Sentinel User Guide (Guida dell'utente di NetIQ Sentinel 7.0.1)*.

## 2.14 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. Visualizzando le informazioni relative alle persone che hanno avviato una determinata azione o a quelle che ne hanno subito gli effetti è possibile ridurre i tempi di risposta ed eseguire l'analisi basata sui comportamenti. Per ulteriori informazioni, vedere [“Leveraging Identity Information”](#) (Utilizzo delle informazioni sulle identità) nella *NetIQ Sentinel User Guide* (Guida dell'utente di NetIQ Sentinel).

## 2.15 Analisi evento

Sentinel offre un potente set di strumenti che facilitano il reperimento e l'analisi di dati evento critici. Il sistema è configurato e ottimizzato affinché possa offrire la massima efficienza per ogni tipo specifico di analisi. È dotato, inoltre, di metodi che consentono la transizione semplificata e lineare tra i vari tipi di analisi.

L'esame degli eventi in Sentinel spesso inizia con la visualizzazione in tempo reale di Active Views. Sebbene siano disponibili molti altri strumenti avanzati, Active Views visualizza i flussi evento filtrati insieme a grafici di riepilogo che possono essere utilizzati per un'analisi semplice e approssimativa delle tendenze dei dati, dei dati evento e dell'identificazione di eventi specifici. Familiarizzando con il prodotto, l'utente sarà in grado di creare filtri configurati per classi specifici di dati, come gli output provenienti dalla correlazione. Active Views può essere utilizzato come un dashboard in cui viene visualizzata un'attitudine relativa alla sicurezza e operatività generica.

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 o su un sistema particolare. 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 dei rapporti offerte da Sentinel forniscono un controllo personalizzato del layout degli eventi, consentendo la visualizzazione di ampi volumi di dati. Sentinel rende la transizione più semplice in quanto consente di trasferire le ricerche interattive create nell'interfaccia di ricerca, in un modello di generazione dei rapporti in grado di creare all'istante un rapporto, in cui vengono visualizzati gli stessi dati, ma in un formato organizzato meglio e concepito per numero di eventi elevato.

A tale scopo, Sentinel include numerosi modelli. Alcuni sono configurati per consentire la visualizzazione di particolari tipi di informazioni, come i dati di autenticazione o la creazione di utenti, mentre altri sono di tipo più generico e consentono di personalizzare i gruppi e le colonne del rapporto in modo interattivo.

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

---

# II Pianificazione dell'installazione di Sentinel

In questa sezione sono illustrati i fattori da prendere in esame prima di installare Sentinel. Se si desidera installare una configurazione non descritta nelle sezioni che seguono o per eventuali chiarimenti, rivolgersi al [supporto tecnico di NetIQ](#).

- ♦ [Capitolo 3, "Elenco di controllo per l'implementazione"](#), a pagina 31
- ♦ [Capitolo 4, "Informazioni sulla licenza"](#), a pagina 33
- ♦ [Capitolo 5, "Requisiti di sistema"](#), a pagina 37
- ♦ [Capitolo 6, "Considerazioni sull'installazione"](#), a pagina 39
- ♦ [Capitolo 7, "Considerazione sull'installazione per la modalità FIPS140-2"](#), a pagina 49
- ♦ [Capitolo 8, "Porte utilizzate"](#), a pagina 55
- ♦ [Capitolo 9, "Opzioni di installazione"](#), a pagina 61



# 3 Elenco di controllo per l'implementazione

Per eseguire pianificazione, installazione e configurazione di Sentinel, utilizzare l'elenco di controllo seguente:

<input type="checkbox"/> Task	Vedere
<input type="checkbox"/> Esaminare le informazioni relative all'architettura del prodotto per acquisire familiarità con i componenti di Sentinel.	<a href="#">Parte I, "Informazioni su Sentinel," a pagina 13.</a>
<input type="checkbox"/> Esaminare le condizioni di licenza di Sentinel per stabilire se è necessario utilizzare la licenza di valutazione o Enterprise.	<a href="#">Capitolo 4, "Informazioni sulla licenza", a pagina 33.</a>
<input type="checkbox"/> 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.	<a href="#">Capitolo 5, "Requisiti di sistema", a pagina 37.</a>
<input type="checkbox"/> Esaminare gli eventi al secondo (EPS) di Gestione servizi di raccolta e del motore di correlazione e i record al secondo (RPS) di Gestione servizi di raccolta NetFlow.  Stabilire il numero di istanze di Gestione servizi di raccolta, del motore di correlazione e di Gestione servizi di raccolta NetFlow che è necessario installare per migliorare le prestazioni e bilanciare il carico.	<a href="#">Sezione 6.1, "Vantaggi delle installazioni distribuite", a pagina 39.</a>
<input type="checkbox"/> Esaminare le note di rilascio di Sentinel per informazioni sulle nuove funzionalità e i problemi noti.	<a href="#">Note di rilascio di Sentinel</a>
<input type="checkbox"/> Installare Sentinel.	<a href="#">Parte III, "Installazione di Sentinel," a pagina 63.</a>
<input type="checkbox"/> Accertarsi di aver configurato l'orario nel server Sentinel.	<a href="#">Capitolo 17, "Orario di configurazione", a pagina 97.</a>
<input type="checkbox"/> Quando si esegue l'installazione di Sentinel, per default vengono installati i plug-in disponibili al momento della release. Configurare i plug-in pronti all'uso per la raccolta dati e la generazione di rapporti.	<a href="#">Capitolo 19, "Configurazione dei plug-in pronti all'uso", a pagina 105.</a>
<input type="checkbox"/> In Sentinel sono incluse regole di correlazione pronte all'uso. Alcune regole di correlazione sono configurate di default per eseguire un'azione che invia un'e-mail quando la regola viene attivata, come ad esempio l'azione di notifica all'amministratore della sicurezza. È quindi necessario configurare il server di posta nel server Sentinel impostando l'integratore SMTP e l'azione Invia e-mail.	<a href="#">Documentazione sull'integratore SMTP e l'azione Send Email sul <a href="#">sito Web dei plug-in di Sentinel</a>.</a>
<input type="checkbox"/> Installare i connettori e i servizi di raccolta in base alle esigenze del proprio ambiente.	<a href="#">Capitolo 15, "Installazione di servizi di raccolta e connettori aggiuntivi", a pagina 91.</a>

---

☐	Task	Vedere
☐	Installare istanze aggiuntive di Gestione servizi di raccolta e del motore di correlazione in base alle esigenze del proprio ambiente.	<a href="#">Sezione 12.4, "Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione", a pagina 73.</a>

---

---

# 4 Informazioni sulla licenza

Poiché i clienti hanno esigenze diverse, la piattaforma Sentinel include un'ampia gamma di funzionalità e NetIQ offre diverse tipologie di licenze per soddisfarle.

Prima di Sentinel 7.3 la piattaforma di base era suddivisa in due prodotti principali: Sentinel e Sentinel Log Manager. A partire da Sentinel 7.3, NetIQ fornisce i due prodotti sotto forma di piattaforma singola unitaria per migliorare l'erogazione di nuove funzioni, patch, documentazione e supporto e per consentire ai clienti di selezionare le funzionalità della soluzione che meglio soddisfano le loro esigenze.

La piattaforma Sentinel è composta da due soluzioni principali:

- ♦ **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 7.3 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 7.3, vedere il documento sulle domande frequenti disponibile all'indirizzo <https://www.netiq.com/products/sentinel/frequently-asked-questions/slm122-to-slm73-upgrade-faqs.html>.

NetIQ fornisce licenze separate per ciascuna di queste soluzioni. A seconda della chiave di licenza immessa, viene abilitata la soluzione corrispondente. Altri elementi del sistema di licenza di Sentinel, quali il valore di EPS, le autorizzazioni per i dispositivi e i plug-in, rendono necessaria una licenza aggiuntiva. Per ulteriori dettagli, vedere il contratto di licenza con l'utente finale.

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

Tabella 4-1 Servizi e funzioni di Sentinel

Servizi e funzioni	Sentinel Enterprise	Sentinel for Log Management
<b>Funzionalità principali</b>	Si	Si
<ul style="list-style-type: none"> <li>◆ Raccolta eventi di base</li> <li>◆ Raccolta di dati diversi dagli eventi (risorse, vulnerabilità, identità)</li> <li>◆ Analisi sintattica e normalizzazione</li> <li>◆ Classificazione tassonomica dei dati degli eventi</li> <li>◆ Mappatura contestuale in linea</li> <li>◆ Raccolta e memorizzazione NetFlow</li> <li>◆ Visualizzazione NetFlow in tempo reale</li> <li>◆ Visualizzazione NetFlow in base agli eventi</li> <li>◆ Ricerca di eventi (locale)</li> <li>◆ Generazione di rapporti sugli eventi</li> <li>◆ Filtro degli eventi</li> <li>◆ Visualizzazione degli eventi in tempo reale</li> <li>◆ Memorizzazione degli eventi</li> <li>◆ Policy di permanenza dei dati</li> <li>◆ Non rifiuto della memorizzazione eventi</li> <li>◆ Abilitazione FIPS</li> <li>◆ Azioni attivate manualmente</li> <li>◆ Creazione e gestione manuali dei casi</li> <li>◆ Azioni e workflow dei casi</li> <li>◆ Workflow iTRAC</li> </ul>		
<b>Azioni</b>	Si	Si
<ul style="list-style-type: none"> <li>◆ Azioni attivate da correlazioni (soltanto se la correlazione è abilitata)</li> <li>◆ Azioni attivate da regole di instradamento (soltanto se le regole sono abilitate)</li> <li>◆ Azioni attivate manualmente</li> </ul>		
<b>Regole di instradamento</b>	Si	Si
<ul style="list-style-type: none"> <li>◆ Instradamento degli eventi (esterni)</li> <li>◆ Azioni attivate da regole di instradamento (soltanto se le azioni sono abilitate)</li> </ul>		
Collegamento Sentinel	Si	Si

Servizi e funzioni	Sentinel Enterprise	Sentinel for Log Management
<b>Correlazione</b>	Si	No
<ul style="list-style-type: none"> <li>◆ Correlazione di modelli in tempo reale</li> <li>◆ Azioni attivate da regole di correlazione (soltanto se le azioni sono abilitate)</li> <li>◆ Valutazione degli avvisi</li> <li>◆ Dashboard degli avvisi</li> </ul>		
Sincronizzazione dei dati	Si	Si
Ripristino dei dati degli eventi dall'archivio	Si	Si
Federazione di dati (ricerca distribuita)	Si	Si
<b>Security Intelligence</b>	Si	No
<ul style="list-style-type: none"> <li>◆ Regole di anomalie</li> <li>◆ Analisi statistica in tempo reale</li> </ul>		
Analisi statistica in tempo reale	Si	No
Scadenza della licenza	Mai	Mai
Limite EPS	Illimitato	Illimitato

## 4.1 Licenze di Sentinel

In questa sezione vengono fornite informazioni sulle varie licenze di Sentinel.

- ◆ [Sezione 4.1.1, “Licenza di valutazione”, a pagina 35](#)
- ◆ [Sezione 4.1.2, “Licenza gratuita”, a pagina 36](#)
- ◆ [Sezione 4.1.3, “Licenze aziendali”, a pagina 36](#)

### 4.1.1 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 si esegue il ripristino nel sistema di eventi di vecchia data, Sentinel aggiorna di conseguenza la data di scadenza.

Quando la licenza di valutazione scade, il sistema viene eseguito con una chiave di licenza base che consente l'utilizzo di un numero limitato di funzioni e una frequenza eventi limitata a 25 EPS. La licenza base è detta anche licenza gratuita.

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.

## 4.1.2 Licenza gratuita

La licenza gratuita consente l'utilizzo di un numero limitato di funzioni e una frequenza eventi limitata a 25 EPS. La licenza gratuita non ha scadenza.

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:** NetIQ non fornisce supporto tecnico e aggiornamenti del prodotto per la versione gratuita di Sentinel.

---

## 4.1.3 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 abilita alcune funzionalità, frequenze di raccolta dati e origini eventi. 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, vedere [Adding a License Key](#) (Aggiunta di una chiave di licenza) nella [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel).

---

# 5 Requisiti di sistema

L'implementazione di Sentinel può variare a seconda delle esigenze dell'ambiente specifico e, pertanto, prima di stabilire l'architettura definitiva è necessario rivolgersi a NetIQ Consulting Services o a un partner NetIQ Sentinel.

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

- ♦ [Sezione 5.1, "Requisiti di sistema relativi al connettore e al servizio di raccolta", a pagina 37](#)
- ♦ [Sezione 5.2, "Ambiente virtuale", a pagina 37](#)

## 5.1 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](#).

## 5.2 Ambiente virtuale

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

Per ulteriori informazioni sui consigli relativi al computer fisico, vedere il [Capitolo 5, "Requisiti di sistema", a pagina 37](#).



---

# 6 Considerazioni sull'installazione

L'architettura di Sentinel è scalabile e può essere ampliata in modo da gestire il carico necessario. In Sentinel è possibile gestire diversi tipi di carico. In questo capitolo sono riportate le principali considerazioni da effettuare al fine di definire la scala dell'installazione di Sentinel. Per progettare in modo più accurato il sistema nell'ambito del proprio ambiente specifico è possibile rivolgersi a un professionista di [NetIQ Services](#) o a un [partner di NetIQ Services](#).

- ♦ [Sezione 6.1, "Vantaggi delle installazioni distribuite", a pagina 39](#)
- ♦ [Sezione 6.2, "Installazione all-in-one", a pagina 41](#)
- ♦ [Sezione 6.3, "Installazione distribuita a un livello", a pagina 42](#)
- ♦ [Sezione 6.4, "Installazione distribuita a un livello con alta disponibilità", a pagina 43](#)
- ♦ [Sezione 6.5, "Installazione distribuita a due e tre livelli", a pagina 44](#)
- ♦ [Sezione 6.6, "Pianificazione delle partizioni per la memorizzazione dei dati", a pagina 45](#)

## 6.1 Vantaggi delle installazioni distribuite

Nel server Sentinel sono inclusi di default i componenti seguenti:

- ♦ **Gestione servizi di raccolta:** flessibile punto di raccolta dei dati utilizzato da Sentinel. Il programma di installazione di Sentinel installa per default anche un'istanza di Gestione servizi di raccolta.
- ♦ **Motore di correlazione:** elabora gli eventi contenuti nel flusso in tempo reale per stabilire se devono attivare una o più delle regole di correlazione.
- ♦ **Gestione servizi di raccolta NetFlow:** Gestione servizi di raccolta NetFlow raccoglie i dati del flusso di rete (NetFlow, IPFIX e così via) da dispositivi di rete quali router, switch e firewall. I dati del flusso di rete forniscono informazioni di base su tutte le connessioni di rete fra gli host, inclusi pacchetti e byte trasmessi, e sono utili per visualizzare il comportamento dei singoli host o dell'intera rete.

---

**Importante:** per gli ambienti di produzione, NetIQ Corporation consiglia di configurare un'installazione distribuita poiché isola i componenti di raccolta dati in un computer separato e consente quindi la gestione dei picchi e di altre anomalie preservando la massima stabilità del sistema.

---

In questa sezione sono descritti i vantaggi delle installazioni distribuite.

- ♦ [Sezione 6.1.1, "Vantaggi apportati dalla presenza di più Gestioni servizi di raccolta", a pagina 40](#)
- ♦ [Sezione 6.1.2, "Vantaggi derivanti dall'uso di istanze aggiuntive del motore di correlazione", a pagina 40](#)
- ♦ [Sezione 6.1.3, "Vantaggi apportati dalla presenza di più istanze di Gestione servizi di raccolta NetFlow", a pagina 41](#)

## 6.1.1 Vantaggi apportati dalla presenza di più Gestioni servizi di raccolta

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

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

- ♦ **Miglioramento della prestazione del sistema:** le istanze aggiuntive di Gestione servizi di raccolta 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 Gestioni servizi di raccolta vengono posizionate insieme alle origini evento, i processi di filtraggio, cifratura e compressione dei dati possono essere elaborati su lato origine.
- ♦ **Memorizzazione dei file nella cache:** le istanze aggiuntive di Gestione servizi di raccolta 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 Gestione servizi di raccolta in ubicazioni appropriate della rete. Le istanze remote di Gestione servizi di raccolta 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 Gestione servizi di raccolta, vedere la [Sezione 12.4](#), "Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione", a pagina 73.

---

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

---

## 6.1.2 Vantaggi derivanti dall'uso di istanze aggiuntive del motore di correlazione

È possibile installare istanze multiple del motore di correlazione, 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, potrebbe essere opportuno installare più istanze del motore di correlazione e ridistribuire alcune regole sulle nuove istanze. Le istanze multiple del motore di correlazione 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 del motore di correlazione, vedere [Sezione 12.4](#), "Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione", a pagina 73.

---

**Nota:** in un sistema è possibile installare un solo motore di correlazione. Le istanze aggiuntive del motore di correlazione possono essere installate in sistemi remoti e successivamente connesse al server Sentinel.

---

### 6.1.3 Vantaggi apportati dalla presenza di più istanze di Gestione servizi di raccolta NetFlow

Gestione servizi di raccolta NetFlow raccoglie i dati del flusso di rete dai dispositivi di rete. Invece di eseguire Gestione servizi di raccolta NetFlow nel server Sentinel è necessario installare delle istanze aggiuntive e liberare risorse di sistema per altre funzioni importanti, quali la memorizzazione e le ricerche di eventi.

Negli scenari seguenti è possibile installare istanze aggiuntive di Gestione servizi di raccolta NetFlow:

- ♦ Negli ambienti in cui sono presenti numerosi dispositivi di rete e con frequenze elevate dei dati di flusso, è possibile installare più istanze di Gestione servizi di raccolta NetFlow al fine di distribuire il carico.
- ♦ Se si utilizza un ambiente con più tenant, è necessario installare un'istanza separata di Gestione servizi di raccolta NetFlow per ciascun tenant, al fine di raccogliere separatamente i dati del flusso della rete.

Per ulteriori informazioni sull'installazione di istanze aggiuntive di Gestione servizi di raccolta NetFlow, vedere il [Capitolo 14, "Installazione di Gestione servizi di raccolta NetFlow"](#), a pagina 89.

## 6.2 Installazione all-in-one

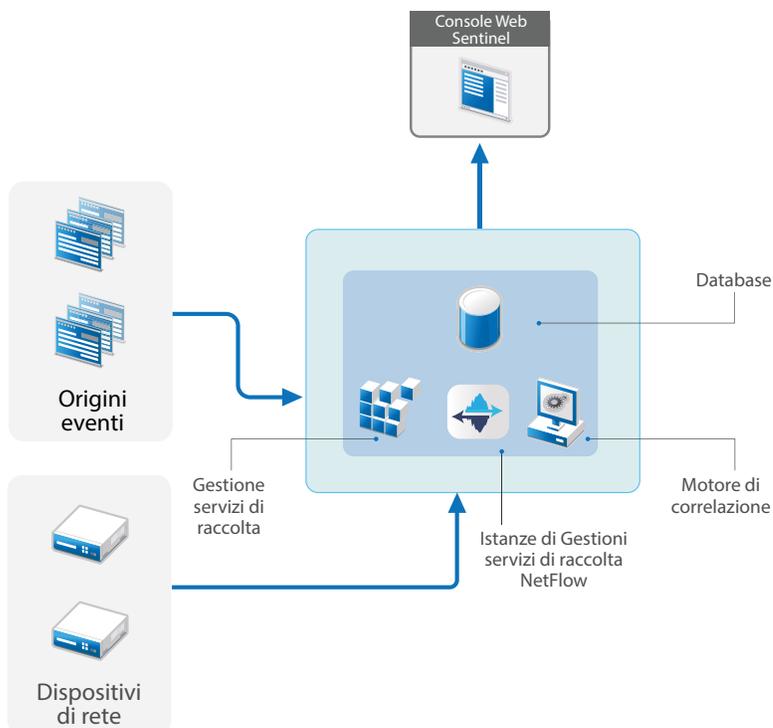
L'opzione d'installazione di base prevede un sistema all-in-one che include tutti i componenti di Sentinel installati in un solo computer. L'installazione all-in-one è adeguata soltanto se il carico del sistema è relativamente basso e non è necessario monitorare computer Windows. In numerosi ambienti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

---

**Importante:** per gli ambienti di produzione, NetIQ Corporation consiglia di configurare un'installazione distribuita poiché isola i componenti di raccolta dati in un computer separato e consente quindi la gestione dei picchi e di altre anomalie preservando la massima stabilità del sistema.

---

Figura 6-1 Installazione all-in-one

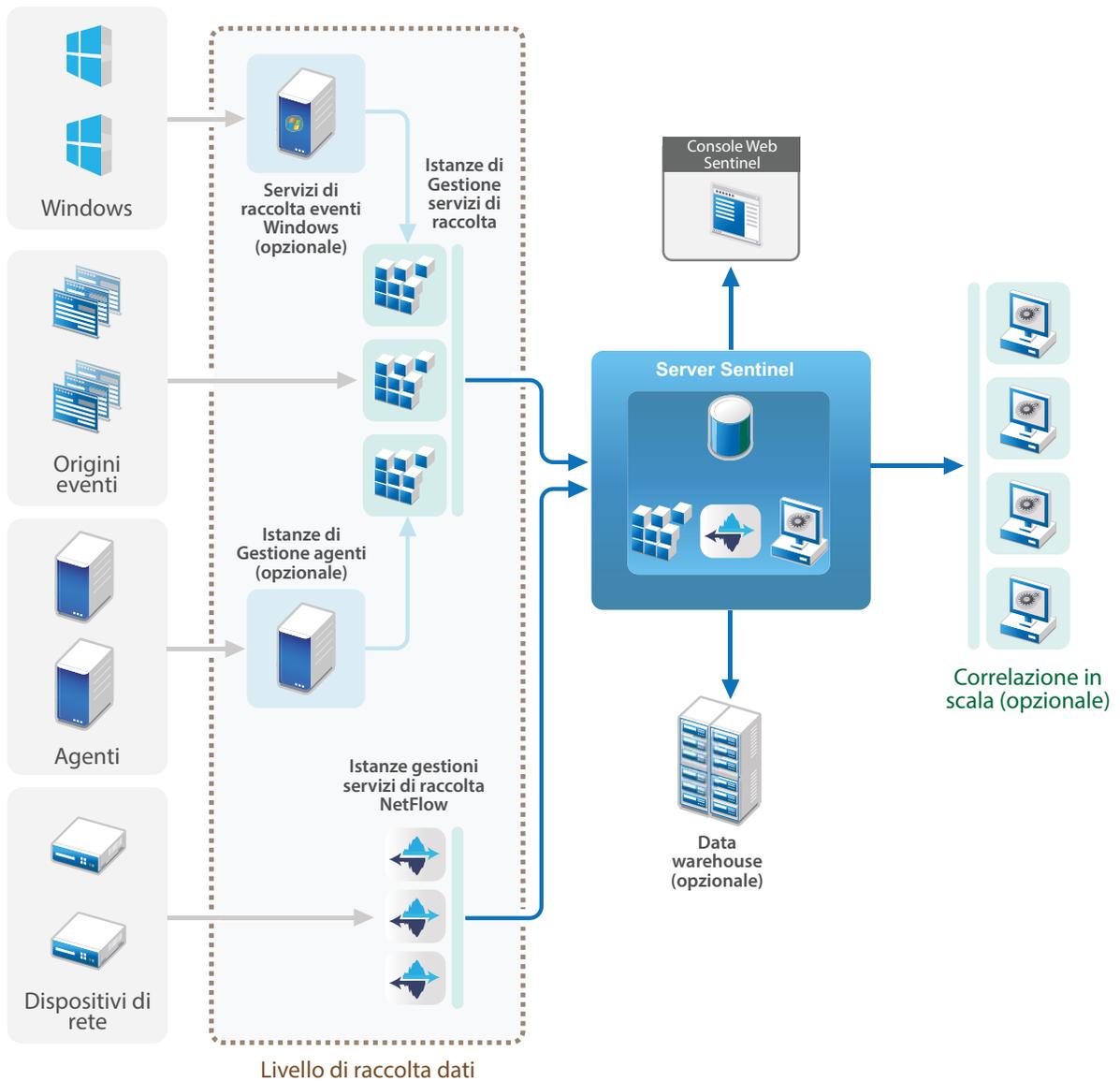


## 6.3 Installazione distribuita a un livello

L'installazione a un livello include un'ulteriore funzionalità per il monitoraggio dei computer Windows, oltre a consentire la gestione di un carico superiore rispetto a quella all-in-one. La raccolta dei dati e la correlazione può essere ampliata aggiungendo computer con istanze di Gestione servizi di raccolta, Gestione servizi di raccolta NetFlow e del motore di correlazione, che riducono il carico di elaborazione nel server Sentinel centrale. Oltre alla gestione dei carichi di eventi, regole di correlazione e dati del flusso di rete, le istanze remote di Gestione servizi di raccolta, del motore di correlazione e di Gestione servizi di raccolta NetFlow contribuiscono anche a liberare risorse nel server Sentinel centrale, 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.

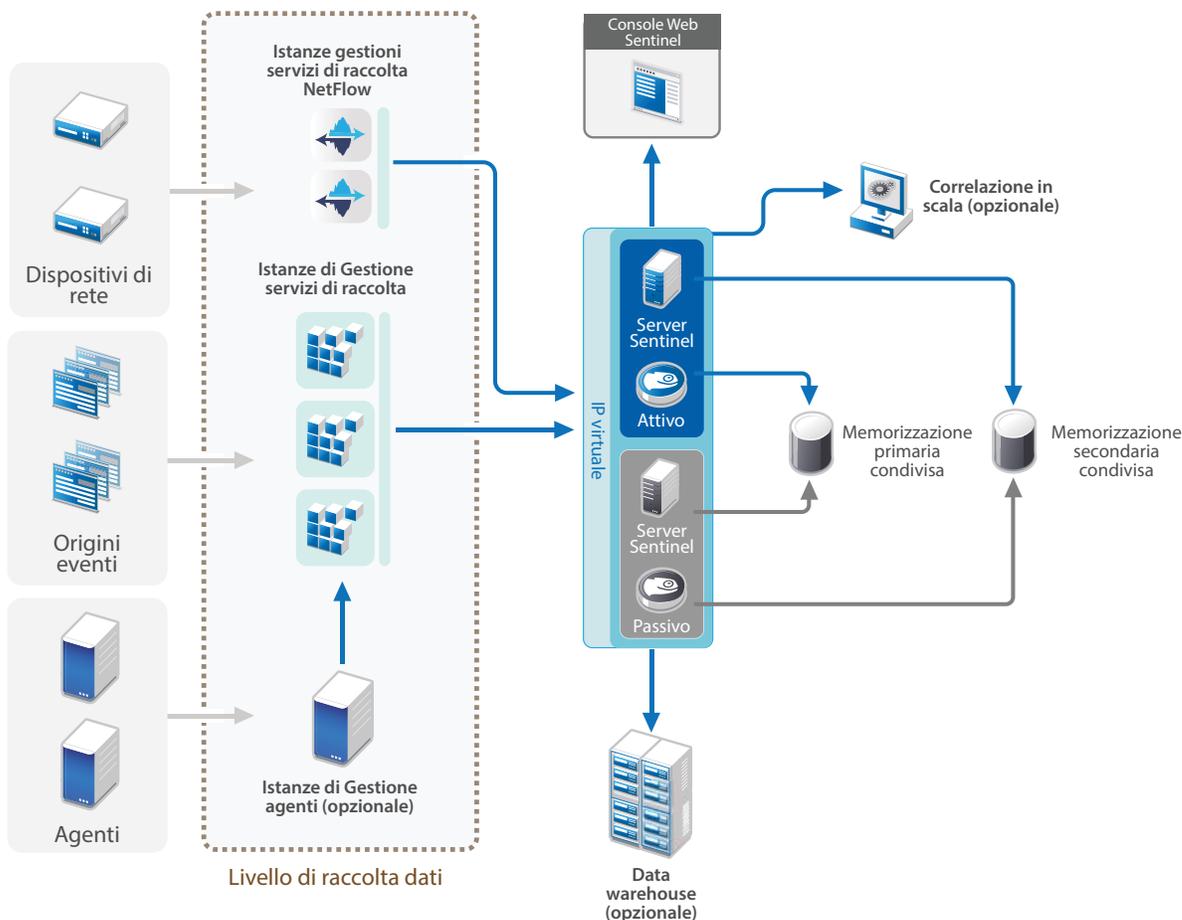
Figura 6-2 Installazione distribuita a un livello



## 6.4 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 VI, "Installazione di Sentinel per alta disponibilità,"](#) a pagina 139.

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

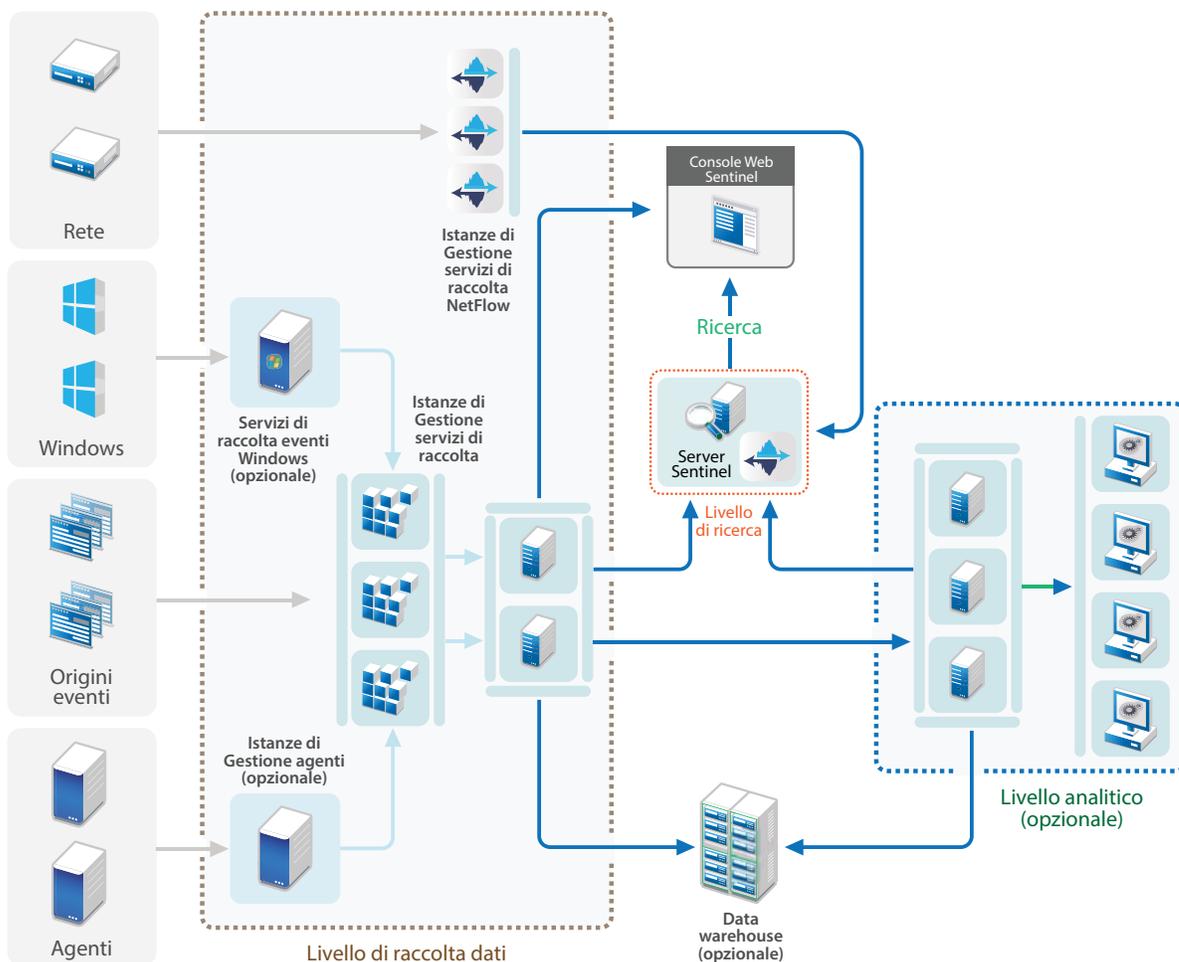


## 6.5 Installazione distribuita a due e tre livelli

Questo tipo d'installazione consente di migliorare le capacità di gestione del carico di un solo server Sentinel centrale e di condividere il carico di elaborazione con più istanze di Sentinel mediante le funzionalità Collegamento Sentinel e Ricerca distribuita. Il carico della raccolta dati viene bilanciato su più server Sentinel, ognuno dei quali prevede varie istanze di Gestione servizi di raccolta, 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 costituisce un pratico punto di accesso singolo per effettuare ricerche in tutti i livelli dei sistemi utilizzando la funzione Ricerca distribuita. Poiché la richiesta di ricerca viene federata fra numerose istanze di Sentinel, questo tipo d'installazione offre anche proprietà di bilanciamento del carico delle ricerche, utili per la gestione distribuita di carichi di ricerca elevati.

I dati del flusso di rete vengono memorizzati in un livello di ricerca per facilitare la navigazione dai risultati di ricerca all'analisi contestuale del traffico di rete.

Figura 6-4 Installazione distribuita a due e tre livelli



## 6.6 Pianificazione delle partizioni per la memorizzazione dei dati

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 [Sezione 6.6.4, "Struttura delle directory di Sentinel"](#), a pagina 47.

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"](#).

## 6.6.1 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 dettagliatamente in [Sezione 6.6.4, "Struttura delle directory di Sentinel", a pagina 47](#). 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`.
- 

## 6.6.2 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 [Sezione 13.3.2, "Creazione di partizioni", a pagina 85](#).

## 6.6.3 Best practice per il layout delle partizioni

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

---

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

---

partizione	Punto di montaggio	Dimensioni	Note
Temp	/tmp	30 GB	Ubicazione del sistema operativo e dei file temporanei di Sentinel; ubicandoli in una partizione separata è possibile proteggere i dati dell'applicazione da danneggiamenti nel caso in cui un processo con eccessivo tempo di esecuzione riempia lo spazio temporaneo.
Memorizzazione primaria	/var/opt/novell/sentinel	Eeguire il calcolo utilizzando le <a href="#">informazioni sulle dimensioni del sistema</a> .	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.	Eeguire il calcolo utilizzando le <a href="#">informazioni sulle dimensioni del sistema</a> .	Area della memorizzazione secondaria che può essere montata localmente come mostrato o in remoto.
Memorizzazione di archiviazione	Sistema remoto	Eeguire il calcolo utilizzando le <a href="#">informazioni sulle dimensioni del sistema</a> .	Questa memorizzazione è riservata ai dati archiviati.

## 6.6.4 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 di configurazione risiedono nella directory seguente: `/etc/opt/novell/sentinel`
- ♦ Il file ID processo (PID) risiede nella directory `/var/run/sentinel/server.pid`

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



---

# 7 Considerazione sull'installazione per la modalità FIPS140-2

Sentinel può essere facoltativamente 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 Gestione servizi di raccolta, le istanze remote del motore di correlazione, l'interfaccia utente Web, Sentinel Control Center e il servizio Advisor utilizzino la cifratura convalidata da FIPS 140-2.

- ♦ [Sezione 7.1, "Implementazione di FIPS in Sentinel", a pagina 49](#)
- ♦ [Sezione 7.2, "Componenti di Sentinel che supportano FIPS", a pagina 50](#)
- ♦ [Sezione 7.3, "Elenco di controllo per l'implementazione", a pagina 51](#)
- ♦ [Sezione 7.4, "Scenari di distribuzione", a pagina 51](#)

## 7.1 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 ha ottenuto la convalida FIPS 140-2. Il modulo di cifratura NSS incluso in SLES 11 SP3 non è stato ancora ufficialmente convalidato come conforme a FIPS 140-2, ma le procedure di convalida del modulo SUSE 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 FIPS 140-2 di RHEL 6.2, vedere [Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules](#) (Moduli di cifratura con convalida FIPS 140-1 e FIPS 140-2).

### 7.1.1 Pacchetti NSS di RHEL

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

- ♦ nspr-4.9-1.el6.x86\_64
- ♦ nss-sysinit-3.13.3-6.el6.x86\_64
- ♦ nss-util-3.13.3-2.el6.x86\_64
- ♦ nss-softokn-freebl-3.12.9-11.el6.x86\_64
- ♦ nss-softokn-3.12.9-11.el6.x86\_64
- ♦ nss-3.13.3-6.el6.x86\_64
- ♦ nss-tools-3.13.3-6.el6.x86\_64

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

## 7.1.2 Pacchetti NSS di SLES

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

- ◆ libfreebl3-3.13.1-0.2.1
- ◆ mozilla-nspr-4.8.9-1.2.2.1
- ◆ mozilla-nss-3.13.1-0.2.1
- ◆ mozilla-nss-tools-3.13.1-0.2.1

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

## 7.2 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 Gestione agenti 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

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 112.](#)

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'uso dei connettori con Sentinel in modalità FIPS 140-2, vedere [“Utilizzo di connettori non FIPS con Sentinel in modalità FIPS 140-2” a pagina 117.](#)

- ◆ 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.

- ◆ NetIQ 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. Nel caso in cui si utilizzino questi integratori con Sentinel in modalità FIPS 140-2, è comunque 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](#).

## 7.3 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.	<a href="#">Sezione 7.4, "Scenari di distribuzione", a pagina 51.</a>
Stabilire se si desidera abilitare la modalità FIPS 140-2 durante l'installazione di Sentinel o se si preferisce farlo successivamente.  Per abilitare la modalità FIPS 140-2 di Sentinel durante l'installazione, è necessario selezionare l'installazione personalizzata o quella in modalità automatica.	<a href="#">Sezione 12.2.2, "Installazione personalizzata", a pagina 71.</a>  <a href="#">Sezione 12.3, "Installazione in modalità automatica", a pagina 73</a>  <a href="#">Capitolo 20, "Abilitazione della modalità FIPS 140-2 in un'installazione esistente di Sentinel", a pagina 107</a>
Configurare i plug-in di Sentinel affinché vengano eseguiti in modalità FIPS 140-2.	<a href="#">Sezione 21.5, "Configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2", a pagina 112.</a>
Importare i certificati nell'archivio chiavi FIPS di Sentinel.	<a href="#">Sezione 21.6, "Importazione di certificati nel database di archivio chiavi FIPS", a pagina 118</a>

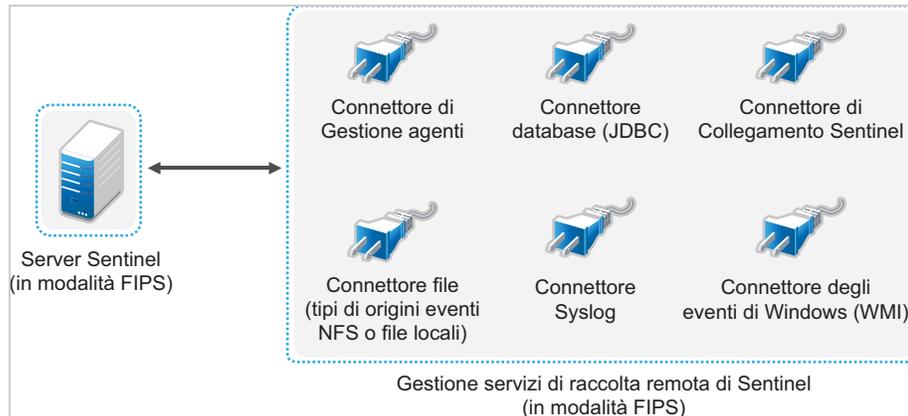
**Nota:** prima di avviare la conversione alla modalità FIPS, NetIQ consiglia di eseguire un backup dei sistemi Sentinel in uso. Se fosse necessario ripristinare il server alla modalità non FIPS, il solo metodo supportato è il ripristino da backup. Per ulteriori informazioni sul ripristino della modalità non FIPS, vedere ["Ripristino di Sentinel nella modalità non FIPS" a pagina 118](#).

## 7.4 Scenari di distribuzione

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

## 7.4.1 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 Gestione servizi di raccolta. Le istanze remote di Gestione servizi di raccolta 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 107.

---

- 2 È necessario che un'istanza remota di Gestione servizi di raccolta Sentinel sia in esecuzione in modalità FIPS 140-2.

---

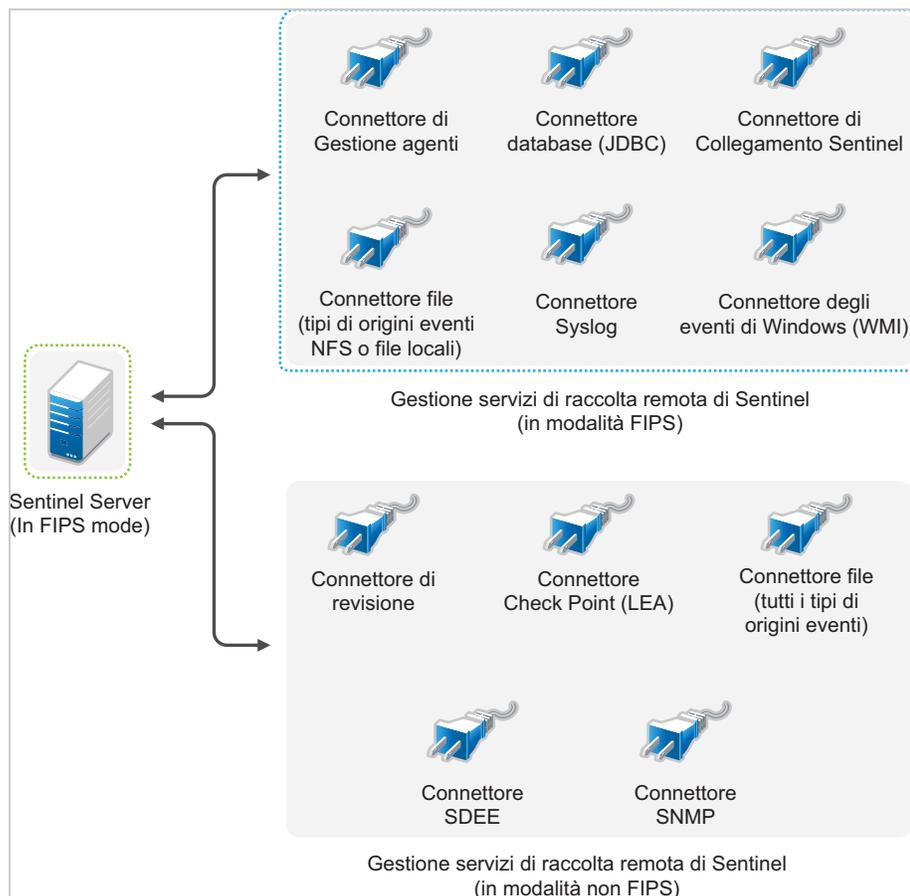
**Nota:** se subito dopo l'installazione o l'upgrade, l'istanza remota di Gestione servizi di raccolta non è in modalità FIPS, abilitare FIPS nell'istanza remota di Gestione servizi di raccolta. Per ulteriori informazioni, vedere il [“Abilitazione della modalità FIPS 140-2 in istanze remote di Gestione servizi di raccolta e del motore di correlazione”](#) a pagina 107.

---

- 3 Accertarsi che il server FIPS e le istanze remote di Gestione servizi di raccolta comunichino fra di loro.
- 4 Se sono presenti istanze remote del motore di correlazione, configurarle affinché vengano eseguite in modalità FIPS. Per ulteriori informazioni, vedere il [“Abilitazione della modalità FIPS 140-2 in istanze remote di Gestione servizi di raccolta e del motore di correlazione”](#) a pagina 107.
- 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 112.

## 7.4.2 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. Le istruzioni che seguono presuppongono che l'ambiente includa un server Sentinel e che i dati vengano raccolti mediante un'istanza remota di Gestione servizi di raccolta. Le istanze remote di Gestione servizi di raccolta 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 Gestione servizi di raccolta, 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 soltanto nel caso in cui per la raccolta dati dalle origini eventi si utilizzino sia connettori che supportano la modalità FIPS 140-2 sia connettori che ancora 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 107.

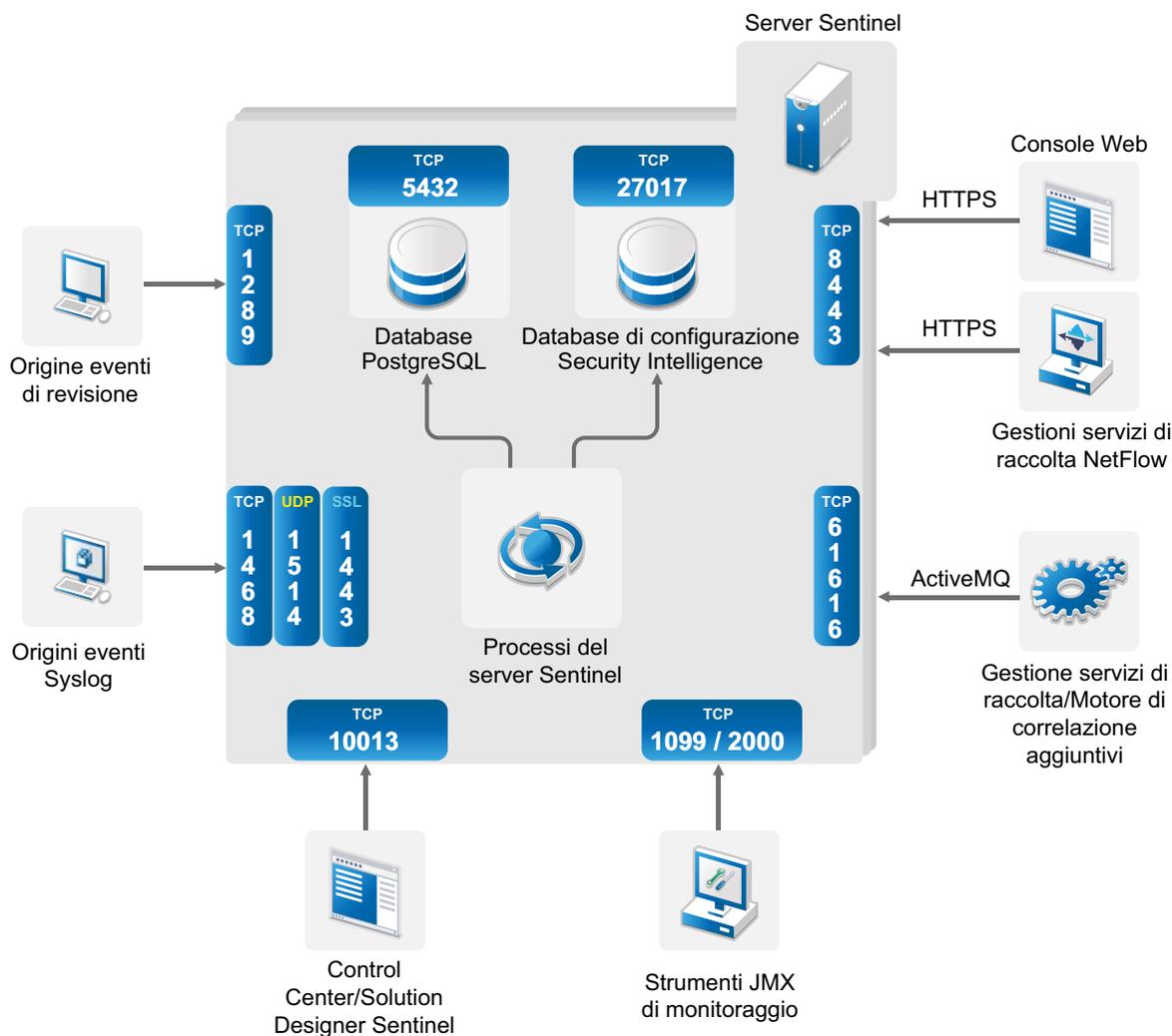
---

- 2 Verificare che un'istanza remota di Gestione servizi di raccolta sia in modalità FIPS 140-2 e che un'altra istanza remota sia in modalità non FIPS.
  - 2a Se non si dispone di un'istanza remota di Gestione servizi di raccolta in modalità FIPS 140-2, abilitare FIPS nell'istanza remota di Gestione servizi di raccolta. Per ulteriori informazioni, vedere il [“Abilitazione della modalità FIPS 140-2 in istanze remote di Gestione servizi di raccolta e del motore di correlazione”](#) a pagina 107.
  - 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 Gestione servizi di raccolta e del motore di correlazione”](#) a pagina 111.
- 3 Verificare che le due istanze remote di Gestione servizi di raccolta comunichino con il server Sentinel abilitato per la modalità FIPS 140-2.
- 4 Se sono presenti istanze remote del motore di correlazione, configurarle affinché vengano eseguite in modalità FIPS. Per ulteriori informazioni, vedere il [“Abilitazione della modalità FIPS 140-2 in istanze remote di Gestione servizi di raccolta e del motore di correlazione”](#) a pagina 107.
- 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 112.
  - 5a Installare i connettori che supportano la modalità FIPS 140-2 nell'istanza remota di Gestione servizi di raccolta in modalità FIPS.
  - 5b Installare i connettori che non supportano la modalità FIPS 140-2 nell'istanza remota di Gestione servizi di raccolta 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. Nella figura seguente sono illustrate le porte utilizzate in Sentinel:

Figura 8-1 Porte utilizzate in Sentinel



- ◆ Sezione 8.1, "Porte del server Sentinel", a pagina 56
- ◆ Sezione 8.2, "Porte di Gestione servizi di raccolta", a pagina 58
- ◆ Sezione 8.3, "Porte del motore di correlazione", a pagina 59
- ◆ Sezione 8.4, "Porte di Gestione servizi di raccolta NetFlow", a pagina 60

## 8.1 Porte del server Sentinel

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

### 8.1.1 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 l'interfaccia Web del database 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.

### 8.1.2 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 <a href="#">Sentinel Plug-in SDK</a> (SDK per i plug-in di Sentinel).
TCP 1099 e 2000	In entrata	Facoltativo	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 e le connessioni in entrata dalle istanze di Gestione di servizi di raccolta NetFlow.
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 Gestione servizi di raccolta e del motore di correlazione.
TCP 10013	In entrata	Obbligatoria	Utilizzata da Sentinel Control Center e Solution Designer.
TCP 1468	In entrata	Facoltativo	Utilizzata per i messaggi syslog.

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 10014	In entrata	Facoltativo	Utilizzata dalle Gestioni servizi di raccolta remota per connettersi al server mediante il proxy SSL. Tale procedura, tuttavia, non è comune. Infatti, per connettersi al server le Gestioni servizi di raccolta remota utilizzano la porta SSL 61616 per default.
TCP 443	In uscita	Facoltativo	Se si utilizza Advisor, la porta avvia una connessione al servizio Advisor via Internet verso l' <a href="https://secure-www.novell.com/sentinel/download/advisor/">URL degli aggiornamenti di Advisor (https://secure-www.novell.com/sentinel/download/advisor/)</a> .
TCP 8443	In uscita	Facoltativo	Se si utilizza la ricerca distribuita, la porta attiva la connessione ad altri sistemi Sentinel per effettuare la ricerca distribuita.
TCP 389 o 636	In uscita	Facoltativo	Se si utilizza l'autenticazione LDAP, la porta attiva la connessione con il server LDAP.
TCP/UDP 111 e TCP/UDP 2049	In uscita	Facoltativo	Se la memorizzazione secondaria è configurata per l'uso del protocollo NFS.
TCP 137, 138, 139, 445	In uscita	Facoltativo	Se la memorizzazione secondaria è configurata per l'uso del protocollo CIFS.
TCP JDBC (a seconda del database)	In uscita	Facoltativo	Se si utilizza la sincronizzazione dei dati, la porta avvia la connessione con il database di destinazione mediante JDBC. La porta utilizzata varia a seconda del database di destinazione.
TCP 25	In uscita	Facoltativo	Avvia una connessione con il server e-mail.
TCP 1290	In uscita	Facoltativo	Quando Sentinel inoltra gli eventi a un altro sistema Sentinel, la porta avvia una connessione con tale sistema tramite Collegamento Sentinel.
UDP 162	In uscita	Facoltativo	Quando Sentinel inoltra gli eventi al sistema che riceve i trap SNMP, la porta invia un pacchetto al destinatario.
UDP 514 o TCP 1468	In uscita	Facoltativo	La porta viene utilizzata quando Sentinel inoltra gli eventi al sistema che riceve i messaggi Syslog. Se la porta è UDP, invia un pacchetto al destinatario. Se la porta è TCP, avvia una connessione con il destinatario.

### 8.1.3 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 dalla console di gestione dell'applicazione Sentinel (WebYaST). Utilizzata anche dall'applicazione Sentinel per il servizio di aggiornamento.

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
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 NetIQ, 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).

## 8.2 Porte di Gestione servizi di raccolta

Gestione servizi di raccolta comunica con gli altri componenti mediante le porte seguenti.

### 8.2.1 Porte di rete

Per il funzionamento ottimale di Gestione servizi di raccolta 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	Facoltativo	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.

### 8.2.2 Porte specifiche per l'applicazione Gestione servizi di raccolta

In aggiunta a quelle riportate precedentemente, per l'applicazione Gestione servizi di raccolta 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 dalla console di gestione dell'applicazione Sentinel (WebYaST). 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	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	In uscita	Obbligatoria	Avvia una connessione con l'archivio degli aggiornamenti software per l'applicazione NetIQ, 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).

## 8.3 Porte del motore di correlazione

Il motore di correlazione comunica con gli altri componenti mediante le porte seguenti.

### 8.3.1 Porte di rete

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

Porte	Direzione	Necessaria/ Facoltativa	Descrizione
TCP 1099 e 2000	In entrata	Facoltativo	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.

### 8.3.2 Porte specifiche per l'applicazione Motore di correlazione

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

<b>Porte</b>	<b>Direzione</b>	<b>Necessaria/ Facoltativa</b>	<b>Descrizione</b>
TCP 22	In entrata	Obbligatoria	Utilizzata per l'accesso shell sicuro a Sentinel Appliance.
TCP 4984	In entrata	Obbligatoria	Utilizzata dalla console di gestione dell'applicazione Sentinel (WebYaST). 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 NetIQ, 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).

## 8.4 Porte di Gestione servizi di raccolta NetFlow

Gestione servizi di raccolta NetFlow comunica con gli altri componenti mediante le porte seguenti:

<b>Porte</b>	<b>Direzione</b>	<b>Necessaria/ Facoltativa</b>	<b>Descrizione</b>
HTTPS 8443	In uscita	Obbligatoria	Avvia una connessione con il server Sentinel.
3578	In entrata	Obbligatoria	Utilizzata per ricevere i dati del flusso di rete dai dispositivi di rete.

# 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.

## 9.1 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 [Sezione 12.2, "Installazione interattiva"](#), a pagina 70.

- ♦ **Modalità automatica:** se si desidera installare più server Sentinel nella propria distribuzione, è possibile registrare le opzioni di installazione in un file di configurazione durante l'installazione standard o personalizzata e, successivamente, utilizzare tale file per eseguire un'installazione in modalità automatica. Per ulteriori informazioni sull'installazione in modalità automatica, vedere la [Sezione 12.3, "Installazione in modalità automatica"](#), a pagina 73.

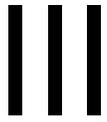
## 9.2 Installazione in modalità applicazione

Con l'installazione in modalità applicazione si installa sia il sistema operativo SLES 11 SP3 a 64 bit che Sentinel.

L'applicazione Sentinel è disponibile nei seguenti formati:

- ♦ Immagine dell'applicazione OVF
- ♦ Immagine di soluzione hardware integrata Live DVD direttamente installata in un server hardware

Per ulteriori informazioni sull'installazione in modalità applicazione, vedere il [Capitolo 13](#), "Installazione in modalità applicazione", a pagina 79.



# Installazione di Sentinel

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

- ♦ [Capitolo 10, "Panoramica relativa all'installazione", a pagina 65](#)
- ♦ [Capitolo 11, "Elenco di controllo per l'installazione", a pagina 67](#)
- ♦ [Capitolo 12, "Installazione tradizionale", a pagina 69](#)
- ♦ [Capitolo 13, "Installazione in modalità applicazione", a pagina 79](#)
- ♦ [Capitolo 14, "Installazione di Gestione servizi di raccolta NetFlow", a pagina 89](#)
- ♦ [Capitolo 15, "Installazione di servizi di raccolta e connettori aggiuntivi", a pagina 91](#)
- ♦ [Capitolo 16, "Verifica dell'installazione", a pagina 93](#)



---

# 10 Panoramica relativa all'installazione

Con questo tipo di installazione di Sentinel si installano nel server Sentinel i componenti seguenti:

- ♦ **Processo del server Sentinel:** componente principale di Sentinel. 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.
- ♦ **Server Web:** Sentinel utilizza Jetty come server Web per consentire la connessione sicura all'interfaccia Web di Sentinel.
- ♦ **Database PostgreSQL:** Sentinel è dotato di un database integrato in cui sono memorizzate le informazioni relative alla sua configurazione, i dati sulle risorse e le vulnerabilità, le informazioni sulle identità, gli stati dei casi e dei workflow e così via.
- ♦ **Database MongoDB:** memorizza i dati di Security Intelligence.
- ♦ **Gestione servizi di raccolta:** flessibile punto di raccolta dei dati utilizzato da Sentinel. Il programma di installazione di Sentinel installa per default anche un'istanza di Gestione servizi di raccolta.
- ♦ **Gestione servizi di raccolta NetFlow:** Gestione servizi di raccolta NetFlow raccoglie i dati del flusso di rete (NetFlow, IPFIX e così via) da dispositivi di rete quali router, switch e firewall. I dati del flusso di rete forniscono informazioni di base su tutte le connessioni di rete fra gli host, inclusi pacchetti e byte trasmessi, e sono utili per visualizzare il comportamento dei singoli host o dell'intera rete.
- ♦ **Motore di correlazione:** elabora gli eventi contenuti nel flusso in tempo reale per stabilire se devono attivare una o più delle regole di correlazione.
- ♦ **Advisor:** Advisor di Security Nexus è un servizio facoltativo di sottoscrizione dati che fornisce una correlazione a livello di dispositivi tra gli eventi in tempo reale provenienti da sistemi di prevenzione e rilevamento delle intrusioni e da risultati di scansioni delle vulnerabilità aziendali. Per ulteriori informazioni su Advisor, vedere "[Detecting Vulnerabilities and Exploits](#)" (Rilevamento di vulnerabilità ed exploit) nella [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel).
- ♦ **Plug-in di Sentinel:** Sentinel supporta una serie di plug-in per ampliare e migliorare le funzionalità del sistema. Alcuni di questi plug-in sono preinstallati. È possibile effettuare il download di plug-in aggiuntivi e aggiornamenti dal [sito Web dei plug-in di Sentinel](#). I plug-in di Sentinel includono:
  - ♦ Servizi di raccolta
  - ♦ Connettori
  - ♦ Regole di correlazione e azioni
  - ♦ Rapporti
  - ♦ Workflow iTRAC
  - ♦ Pacchetti soluzione

ma, grazie all'eccellente scalabilità della soluzione, è possibile distribuirli tra più computer e ottenere così prestazioni ottimali del sistema. Per gli ambienti di produzione, NetIQ Corporation consiglia di configurare un'installazione distribuita poiché isola i componenti di raccolta dati in un computer

separato e consente quindi la gestione dei picchi e di altre anomalie preservando la massima stabilità del sistema. Per ulteriori informazioni, vedere il [Sezione 6.1, “Vantaggi delle installazioni distribuite”](#), a pagina 39.

---

# 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 173.
- Se si prevede di installare la versione con licenza, richiedere la chiave di licenza al [servizio di assistenza clienti NetIQ](#).
- Assicurarsi che le porte elencate in [Capitolo 8, "Porte utilizzate"](#), a pagina 55 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 6. Per Sentinel sono necessarie le versioni a 64 bit dei seguenti RPM:

- ◆ bash
- ◆ bc
- ◆ coreutils
- ◆ gettext
- ◆ glibc
- ◆ grep
- ◆ libgcc
- ◆ libstdc
- ◆ lsof
- ◆ net-tools
- ◆ openssl
- ◆ python-libs

- ◆ sed
- ◆ zlib

---

# 12 Installazione tradizionale

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

- ♦ [Sezione 12.1, “Informazioni sulle opzioni di installazione”, a pagina 69](#)
- ♦ [Sezione 12.2, “Installazione interattiva”, a pagina 70](#)
- ♦ [Sezione 12.3, “Installazione in modalità automatica”, a pagina 73](#)
- ♦ [Sezione 12.4, “Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione”, a pagina 73](#)
- ♦ [Sezione 12.5, “Installazione di Sentinel come utente non root”, a pagina 76](#)

## 12.1 Informazioni sulle opzioni di installazione

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

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

## 12.2 Installazione interattiva

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

- ♦ [Sezione 12.2.1, "Installazione standard", a pagina 70](#)
- ♦ [Sezione 12.2.2, "Installazione personalizzata", a pagina 71](#)

### 12.2.1 Installazione standard

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 NetIQ](#):
  - 1a Nel campo **Product or Technology** (Prodotto o tecnologia) sfogliare e selezionare **SIEM-Sentinel**.
  - 1b Fare clic su **Cerca**.
  - 1c Fare clic sul pulsante nella colonna **Download** in corrispondenza di **Sentinel Evaluation**.
  - 1d Fare clic su **proceed to download** (procedi con il download), quindi specificare il nome e la password cliente.
  - 1e Fare clic su **download** per la versione di installazione compatibile con la piattaforma in uso.

- 2 Per estrarre il file di installazione, specificare il comando seguente nella riga di comando.

```
tar zxvf <install_filename>
```

Sostituire *<nomefile\_installazione>* con il nome attuale del file di installazione.

- 3 Passare alla directory in cui è stato estratto il programma di installazione:

```
cd <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 Web di Sentinel, specificare l'URL seguente nel browser Web:

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

<Indirizzo\_IP\_server\_Sentinel> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

## 12.2.2 Installazione personalizzata

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

- 1 Effettuare il download del file di installazione di Sentinel dal [sito Web dei download di NetIQ](#):
  - 1a Nel campo **Product or Technology** (Prodotto o tecnologia) sfogliare e selezionare **SIEM-Sentinel**.
  - 1b Fare clic su **Cerca**.
  - 1c Fare clic sul pulsante nella colonna **Download** in corrispondenza di **Sentinel 7.2 Evaluation**.
  - 1d Fare clic su **proceed to download** (procedi con il download), quindi specificare il nome e la password cliente.
  - 1e Fare clic su **download** per la versione di installazione compatibile con la piattaforma in uso.
- 2 Per estrarre il file di installazione, specificare il comando seguente nella riga di comando.

```
tar zxvf <install_filename>
```

Sostituire <nomefile\_installazione> con il nome attuale del file di installazione.

- 3 Per installare Sentinel, specificare il comando seguente nella radice della directory estratta:

```
./install-sentinel
```

oppure

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

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

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

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

- 5 Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.
- 6 Immettere `yes` o `y` per accettare il contratto di licenza e continuare l'installazione.

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

- 7 Specificare 2 per elaborare una configurazione personalizzata di Sentinel.
- 8 Immettere 1 per utilizzare la chiave 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**, premere `s`.
  - 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 Se si desidera inserire nel database dell'archivio chiavi dei certificati esterni per stabilire l'attendibilità, premere `s` e specificare il percorso del file del certificato. In caso contrario, premere `n`.
- 15c Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel [Capitolo 21, "Esecuzione di Sentinel in modalità FIPS 140-2", a pagina 109.](#)

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

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

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

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

## 12.3 Installazione in modalità automatica

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

Per eseguire un'installazione in modalità automatica, assicurarsi di aver registrato i parametri di installazione in un file. Per ulteriori informazioni sulla creazione del file di risposta, fare riferimento a [Sezione 12.2.1, "Installazione standard", a pagina 70](#) o [Sezione 12.2.2, "Installazione personalizzata", a pagina 71](#).

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

- ◆ ENABLE\_FIPS\_MODE
- ◆ NSS\_DB\_PASSWORD

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

- 1 Effettuare il download dei file di installazione dal [sito Web dei download di NetIQ](#).
- 2 Effettuare il login come utente `root` al server in cui si desidera installare Sentinel.
- 3 Specificare il seguente comando per estrarre i file di installazione dal file `.tar`:

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

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

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

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

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

- 5 **(Condizionale) Se si è scelto di abilitare la modalità FIPS 140-2**, Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel [Capitolo 21, "Esecuzione di Sentinel in modalità FIPS 140-2", a pagina 109](#).

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.

## 12.4 Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione

Per default viene eseguita l'installazione di un'istanza di Gestione servizi di raccolta e di un'istanza del motore di correlazione. Per gli ambienti di produzione, NetIQ Corporation consiglia di configurare un'installazione distribuita poiché isola i componenti di raccolta dati in un computer separato e consente quindi la gestione dei picchi e di altre anomalie preservando la massima stabilità del sistema. Per informazioni sui vantaggi derivanti dall'installazione di componenti aggiuntivi, vedere la [Sezione 6.1, "Vantaggi delle installazioni distribuite", a pagina 39](#).

---

**Importante:** l'istanza aggiuntiva di Gestione servizi di raccolta o del motore di correlazione deve essere installata in sistemi separati. Tale istanza non deve risiedere nello stesso sistema in cui è installato il server Sentinel.

---

- ◆ [Sezione 12.4.1, “Elenco di controllo per l'installazione”, a pagina 74](#)
- ◆ [Sezione 12.4.2, “Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione”, a pagina 74](#)
- ◆ [Sezione 12.4.3, “Aggiunta di un utente personalizzato ActiveMQ per Gestione servizi di raccolta o il motore di correlazione”, a pagina 75](#)

## 12.4.1 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 una Gestione servizi di raccolta è necessaria la connettività di rete alla porta bus messaggi (61616) nel server di Sentinel. Prima di iniziare il processo di installazione della Gestione servizi di raccolta, assicurarsi che a tutti i firewall e impostazioni di rete sia permesso comunicare su questa porta.

## 12.4.2 Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione

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

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

<Indirizzo\_IP\_server\_Sentinel> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

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

- 2 Nella barra degli strumenti, fare clic su **Download**.
- 3 Fare clic su **Download del programma di installazione** in corrispondenza dell'installazione desiderata.
- 4 Fare clic su **Salva file** per salvare il programma di installazione nell'ubicazione desiderata.
- 5 Per estrarre il file di installazione, immettere il comando seguente.

```
tar zxvf <install_filename>
```

Sostituire <nomefile\_installazione> con il nome attuale del file di installazione.

- 6 Passare alla directory in cui è stato estratto il programma di installazione.
- 7 Per installare Gestione servizi di raccolta o il motore di correlazione, specificare il comando seguente:

**Per Gestione servizi di raccolta:**

```
./install-cm
```

**Per il motore di correlazione:**

```
./install-ce
```

- 8 Immettere il numero relativo alla lingua che si desidera utilizzare per l'installazione.  
Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.
- 9 Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.
- 10 Immettere `yes` o `y` per accettare il contratto di licenza e continuare l'installazione.  
Il processo di installazione potrebbe richiedere alcuni secondi per effettuare l'upload dei pacchetti di installazione e richiedere il tipo di configurazione che si desidera utilizzare.
- 11 Una volta richiesto, immettere `1` per procedere con la configurazione standard.
- 12 Immettere il nome host di default di Communication Server o l'indirizzo IP del computer in cui è installato Sentinel.  
Viene visualizzato il certificato del server Sentinel.
- 13 Specificare le credenziali utente di ActiveMQ per Gestione servizi di raccolta o il motore di correlazione.  
Le credenziali utente di ActiveMQ sono memorizzate nel file `<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties`, che risiede nel server Sentinel.
- 14 Quando viene richiesto di accettare il certificato, verificarne la validità utilizzando il comando seguente:  

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

  
Confrontare l'output del certificato con quello del server Sentinel visualizzato mediante la procedura del [Passo 12](#).
- 15 Se l'output del certificato corrisponde a quello del server Sentinel, accettarlo.
- 16 Immettere `yes` o `y` per abilitare la modalità FIPS 140-2 in Sentinel e continuare con la configurazione FIPS.
- 17 Continuare l'installazione seguendo le istruzioni visualizzate fino al termine della procedura.

### 12.4.3 Aggiunta di un utente personalizzato ActiveMQ per Gestione servizi di raccolta o il motore di correlazione

Per l'istanza remota di Gestione servizi di raccolta e del motore di correlazione, si consiglia di utilizzare i nomi utente ActiveMQ di default. Tuttavia, se sono state installate più istanze remote di Gestione servizi di raccolta e si desidera identificarle separatamente, è possibile creare nuovi utenti ActiveMQ:

- 1 Eseguire il login al server come utente Sentinel che dispone dei diritti di accesso ai file di installazione.
- 2 Aprire il file `activemqgroups.properties`.  
Questo file risiede nella directory `<dir_installazione>/etc/opt/novell/sentinel/config/`.
- 3 Aggiungere i nuovi nomi utente ActiveMQ separati da una virgola come illustrato di seguito:  
**Per Gestione servizi di raccolta, aggiungere i nuovi nomi utente nella sezione `cm`. Ad esempio:**  

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

  
**Per il motore di correlazione, aggiungere i nuovi nomi utente nella sezione `admins`. Ad esempio:**

```
admins=system,correlationengine,ceuser1,ceuser2,...
```

4 Salvare e chiudere il file.

5 Aprire il file `activemqusers.properties`.

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

6 Aggiungere la password per l'utente ActiveMQ creato nel [Passo 3](#).

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

**Per gli utenti di Gestione servizi di raccolta:**

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

**Per gli utenti del motore di correlazione:**

```
system=c7f34372ecd20d831cceb29e754e5ac9
correlationengine=68790d7a
ceuser1=69700c6d
ceuser2=70701b5c
```

7 Salvare e chiudere il file.

8 Riavviare il server Sentinel.

## 12.5 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`. NetIQ Corporation non supporta le installazioni eseguite come utenti non root diversi dall'utente `novell`, anche se il processo ha esito positivo.

1 Effettuare il download dei file di installazione dal [sito Web dei download di NetIQ](#).

2 Nella riga di comando, specificare il comando seguente per estrarre i file di installazione dal file `tar`:

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

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

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

4 Immettere il comando seguente:

```
./bin/root_install_prepare
```

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

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

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

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

**5** Accettare l'elenco dei comandi.

Vengono eseguiti i comandi visualizzati.

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

```
su novell
```

**7** (Condizionale) Per eseguire un'installazione interattiva:

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

Componente	Comando
Server Sentinel	<b>ubicazione di default:</b> <code>./install-sentinel</code> <b>ubicazione diversa da quella di default:</b> <code>./install-sentinel --location=/foo</code>
Gestione servizi di raccolta	<b>ubicazione di default:</b> <code>./install-cm</code> <b>ubicazione diversa da quella di default:</b> <code>./install-cm --location=/foo</code>
Motore di correlazione	<b>ubicazione di default:</b> <code>./install-ce</code> <b>ubicazione diversa da quella di default:</b> <code>./install-cm --location=/foo</code>
Gestione servizi di raccolta NetFlow	<b>ubicazione di default:</b> <code>./install-netflow</code> <b>ubicazione diversa da quella di default:</b> <code>./install-netflow --location=/foo</code>

**7b** Continuare con [Passo 9](#).

**8** (Condizionale) Per eseguire un'installazione in modalità automatica, assicurarsi di aver registrato i parametri di installazione in un file. Per ulteriori informazioni sulla creazione del file di risposta, fare riferimento a [Sezione 12.2.1, "Installazione standard"](#), a [pagina 70](#) o [Sezione 12.2.2, "Installazione personalizzata"](#), a [pagina 71](#).

Per eseguire un'installazione in modalità automatica:

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

Componente	Comando
Server Sentinel	<b>ubicazione di default:</b> <code>./install-sentinel -u &lt;file_risposta&gt;</code> <b>ubicazione diversa da quella di default:</b> <code>./install-sentinel --location=/foo -u &lt;file_risposta&gt;</code>
Gestione servizi di raccolta	<b>ubicazione di default:</b> <code>./install-cm -u &lt;file_risposta&gt;</code> <b>ubicazione diversa da quella di default:</b> <code>./install-cm --location=/foo -u &lt;file_risposta&gt;</code>
Motore di correlazione	<b>ubicazione di default:</b> <code>./install-ce -u &lt;file_risposta&gt;</code> <b>ubicazione diversa da quella di default:</b> <code>./install-ce --location=/foo -u &lt;file_risposta&gt;</code>
Gestione servizi di raccolta NetFlow	<b>ubicazione di default:</b> <code>./install-netflow -u &lt;file_risposta&gt;</code> <b>ubicazione diversa da quella di default:</b> <code>./install-netflow --location=/foo -u &lt;file_risposta&gt;</code>

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

**8b** Continuare con la [Passo 12](#).

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

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

**10** Leggere la licenza con l'utente finale e immettere `yes` o `y` per accettare la licenza e continuare con l'installazione.

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

**11** Viene richiesto di specificare la modalità di installazione.

- ◆ Se si sceglie di procedere con la configurazione standard, continuare con [Passo 8](#) mediante [Passo 10](#) in [Sezione 12.2.1, "Installazione standard"](#), a pagina 70.
- ◆ Se si sceglie di procedere con la configurazione personalizzata, continuare con [Passo 7](#) mediante [Passo 14](#) in [Sezione 12.2.2, "Installazione personalizzata"](#), a pagina 71.

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

```
./bin/root_install_finish
```

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

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

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

<Indirizzo\_IP\_server\_Sentinel> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

---

# 13 Installazione in modalità applicazione

L'applicazione Sentinel è un'applicazione software pronta per l'esecuzione creata su SUSE Studio. 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 incrementare gli investimenti realizzati dal cliente. Prima d'installare l'applicazione Sentinel, esaminare le nuove funzionalità e i problemi noti illustrati nelle [Note di rilascio](#) del sistema SLES supportato.

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

- ♦ [Sezione 13.1, "Installazione dell'applicazione Sentinel ISO", a pagina 79](#)
- ♦ [Sezione 13.2, "Installazione dell'applicazione Sentinel OVF", a pagina 82](#)
- ♦ [Sezione 13.3, "Configurazione dell'applicazione successiva all'installazione", a pagina 84](#)
- ♦ [Sezione 13.4, "Interruzione e avvio del server mediante WebYaST", a pagina 87](#)

## 13.1 Installazione dell'applicazione Sentinel ISO

In questa sezione sono riportate le informazioni necessarie per l'installazione di Sentinel e delle istanze di Gestione servizi di raccolta e del motore di correlazione 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.

- ♦ [Sezione 13.1.1, "Prerequisiti", a pagina 79](#)
- ♦ [Sezione 13.1.2, "Installazione di Sentinel", a pagina 80](#)
- ♦ [Sezione 13.1.3, "Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione", a pagina 81](#)

### 13.1.1 Prerequisiti

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

- ♦ (Condizionale) Se si esegue l'installazione dell'applicazione Sentinel in formato ISO nell'hardware fisico, effettuare il download dell'immagine disco ISO dell'applicazione dal sito del supporto, decomprimere il file e creare un DVD.
- ♦ Affinché sia possibile completare l'installazione, verificare che nel sistema in cui si desidera installare l'immagine disco ISO la memoria disponibile sia di almeno 4,5 GB.
- ♦ Affinché il programma d'installazione possa presentare la proposta di partizione automatica, verificare che lo spazio sul disco rigido sia di almeno 50 GB.

## 13.1.2 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 NetIQ](#).
- 2 (Condizionale) Se si utilizza un Hypervisor:  
Configurare la macchina virtuale utilizzando l'immagine ISO virtuale dell'applicazione e accenderla.  
oppure  
Copiare l'immagine ISO su un DVD, configurare la macchina virtuale utilizzando il DVD e accenderla.
- 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 Eseguire l'immagine dell'applicazione Live DVD selezionando la voce collocata nella parte superiore del menu di avvio.  
  
L'installazione controlla prima la quantità di memoria e lo spazio su disco disponibili. Se la quantità di memoria disponibile è inferiore a 2.5 GB, il processo di installazione viene automaticamente terminato. Se la quantità di memoria disponibile è superiore a 2.5 GB ma inferiore a 6.7 GB, l'installazione visualizza un messaggio per notificare che la quantità di memoria a disposizione è inferiore a quella consigliata. Immettere y in caso affermativo oppure n se non si desidera continuare.
- 4 Selezionare la lingua che si desidera, quindi fare clic su **Avanti**.
- 5 Selezionare la configurazione della tastiera e fare clic su **Avanti**.
- 6 Leggere e accettare il contratto di licenza di SUSE Enterprise Server Software. Fare clic su **Avanti**
- 7 Leggere e accettare il contratto di licenza con l'utente finale di NetIQ Sentinel. Fare clic su **Avanti**
- 8 Nella pagina Nome host e nome dominio, specificare il nome host e il nome del dominio. Deselezionare **Assegnare il nome host all'IP di loopback**.
- 9 Fare clic su **Avanti**.
- 10 Scegliere una delle seguenti opzioni di impostazione della connessione:
  - ♦ Per utilizzare le impostazioni della connessione di rete attuali, selezionare **Utilizzare la configurazione seguente** nella pagina Configurazione di rete II.
  - ♦ Per modificare le impostazioni della connessione di rete, fare clic su **Cambia** e apportare le modifiche desiderate.
- 11 Fare clic su **Avanti**.
- 12 Impostare l'ora e la data, quindi fare clic su **Avanti**.  
  
Per modificare la configurazione NTP una volta completata l'installazione, utilizzare YaST dalla riga di comando dell'applicazione. È possibile utilizzare WebYaST per modificare le impostazioni di data e ora ma non la configurazione NTP.  
  
Se immediatamente dopo aver completato l'installazione, l'ora visualizzata non è sincronizzata, eseguire il comando seguente e riavviare NTP:

```
rcntp restart
```

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

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

Per installare l'applicazione nel server fisico, verificare che l'opzione **Installare l'applicazione Sentinel su disco rigido (solo per immagini Live DVD)** sia selezionata. Questa casella di controllo è selezionata di default.

Se si deseleziona la casella di controllo, l'applicazione non viene installata nel server fisico e verrà eseguita solo in modalità LIVE DVD. Continuare con il [Passo 21](#).
- 15 Nella console di installazione live di YaST2, selezionare **Avanti**.

La console di installazione live di YaST2 esegue l'installazione dell'applicazione sul disco rigido. Alcuni dei passaggi precedenti vengono ripetuti nella console di installazione live di YaST2.
- 16 Nella schermata **Partizionamento suggerito** viene visualizzata la configurazione suggerita per le partizioni. Esaminare la configurazione delle partizioni, configurarla se necessario e selezionare **Avanti**. Modificare le impostazioni soltanto se si conoscono i requisiti di configurazione delle partizioni in SLES.

Nella schermata sono disponibili varie opzioni che consentono di configurare le partizioni. Per ulteriori informazioni sulla configurazione delle partizioni, vedere [Using the YaST Partitioner](#) (Utilizzo della modalità di partizionamento di YaST) nella *documentazione di SLES* e la [Sezione 6.6, "Pianificazione delle partizioni per la memorizzazione dei dati"](#), a pagina 45.
- 17 Immettere la password root e selezionare **Avanti**.
- 18 Nella schermata **Impostazioni di installazione live** vengono visualizzate le impostazioni di installazione selezionate. Esaminare le impostazioni, configurarle se necessario e selezionare **Installa**.
- 19 Per confermare l'installazione, selezionare **Installa**.

Attendere che l'installazione venga completata. Una volta eseguita l'installazione, l'avvio di tutti i servizi potrebbe richiedere alcuni minuti in quanto il sistema esegue un'inizializzazione unica.
- 20 Selezionare **OK** per riavviare il sistema.
- 21 Annotare l'indirizzo IP dell'applicazione mostrato nella console.
- 22 Per eseguire il login all'applicazione, immettere il nome utente root e la password nella console.

Il valore di default del nome utente è `root` e la password è quella impostata nel [Passo 17](#).
- 23 Procedere con la [Sezione 13.3, "Configurazione dell'applicazione successiva all'installazione"](#), a pagina 84.

### 13.1.3 Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione

Le procedure di installazione per un'istanza di Gestione servizi di raccolta e per un'istanza del motore di correlazione sono uguali, fatta eccezione per il fatto che è necessario effettuare il download del file dell'applicazione ISO corrispondente dal [sito Web dei download di NetIQ](#).

- 1 Eseguire i passaggi da 1 a [Passo 13](#) della [Sezione 13.1.2, "Installazione di Sentinel"](#), a pagina 80.
- 2 Per installare Gestione servizi di raccolta o il motore di correlazione, 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 Gestione servizi di raccolta o del motore di correlazione 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.

- ♦ **Nome utente del canale di comunicazione:** specificare il nome utente del canale di comunicazione, vale a dire il nome utente di Gestione servizi di raccolta o del motore di correlazione.
- ♦ **Password utente del canale di comunicazione:** specificare la password utente del canale di comunicazione.

Le credenziali utente del canale di comunicazione sono memorizzate nel file /  
`<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties` che risiede nel server Sentinel.

Per verificare le credenziali, vedere la riga seguente nel file `activemqusers.properties`:

**Per Gestione servizi di raccolta:**

```
collectormanager=<password>
```

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

**Per il motore di correlazione:**

```
correlationengine=<password>
```

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

- ♦ **Installare l'applicazione Sentinel su disco rigido (solo per immagini Live DVD):**

verificare di aver selezionato la casella di controllo affinché l'applicazione venga installata nel server fisico.

Se si deseleziona la casella di controllo, l'applicazione non viene installata nel server fisico e verrà eseguita solo in modalità Live DVD.

3 Fare clic su **Avanti**.

4 Quando richiesto, accettare il certificato.

5 Completare [Passo 15](#) mediante [Passo 20](#) in [Sezione 13.1.2, "Installazione di Sentinel"](#), a [pagina 80](#).

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

Sulla console viene visualizzato un messaggio che include il tipo di applicazione (Gestione servizi di raccolta o motore di correlazione 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 22](#) mediante [Passo 23](#) in [Sezione 13.1.2, "Installazione di Sentinel"](#), a [pagina 80](#).

## 13.2 Installazione dell'applicazione Sentinel OVF

In questa sezione sono riportate le informazioni necessarie per installare Sentinel, Gestione servizi di raccolta e il motore di correlazione 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.

- ♦ [Sezione 13.2.1, "Installazione di Sentinel"](#), a [pagina 83](#)
- ♦ [Sezione 13.2.2, "Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione"](#), a [pagina 84](#)

## 13.2.1 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 NetIQ](#).
- 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 che si desidera, quindi fare clic su **Avanti**.
- 6 Selezionare il layout della tastiera, quindi fare clic su **Avanti**.
- 7 Leggere e accettare il contratto di licenza del software SUSE Linux Enterprise Server (SLES) 11 SP3.
- 8 Leggere e accettare il contratto di licenza con l'utente finale di NetIQ Sentinel.
- 9 Nella pagina Nome host e nome dominio, specificare il nome host e il nome del dominio. Deselezionare **Assegnare il nome host all'IP di loopback**.
- 10 Fare clic su **Avanti**. La configurazione del nome host è salvata.
- 11 Scegliere una delle seguenti opzioni per la connessione di rete:
  - ♦ Per utilizzare le impostazioni di rete attuali, selezionare **Utilizzare la configurazione seguente** nella pagina Configurazione di rete II, quindi fare clic su **Avanti**.
  - ♦ Per modificare le impostazioni di connessione alla rete, selezionare **Cambia**, effettuare le modifiche desiderate, quindi fare clic su **Avanti**.Le impostazioni della connessione di rete sono salvate.
- 12 Impostare l'ora e la data, quindi fare clic su **Avanti**.

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

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

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

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

Se la quantità di memoria disponibile è superiore a 2.5 GB ma inferiore a 6.7 GB, l'installazione visualizza un messaggio per notificare che la quantità di memoria a disposizione è inferiore a quella consigliata. Quando viene visualizzato il messaggio, fare clic su **Avanti** per continuare con l'installazione.
- 14 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.
- 15 Annotare l'indirizzo IP dell'applicazione mostrato nella console. Per accedere alla console Web di Sentinel, utilizzare lo stesso indirizzo IP.

## 13.2.2 Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione

Per installare un'istanza di Gestione servizi di raccolta o del motore di correlazione in un server VMware ESX come immagine dell'applicazione OVF:

- 1 Eseguire i passaggi da 1 a 10 della [Sezione 13.2.1, "Installazione di Sentinel"](#), a pagina 83.
- 2 Specificare il nome host/indirizzo IP del server Sentinel al quale la Gestione servizi di raccolta deve connettersi.
- 3 Specificare il numero della porta di Communication Server. La porta di default è 61616.
- 4 Specificare il nome utente ActiveMQ, vale a dire il nome utente di Gestione servizi di raccolta o del motore di correlazione. Il nome utente di default è `collectormanager` per Gestione servizi di raccolta e `correlationengine` per il motore di correlazione.
- 5 Specificare la password per l'utente ActiveMQ.

Le credenziali utente di ActiveMQ sono memorizzate nel file `<dir_installazione>/etc/opt/novell/sentinel/config/activemqusers.properties`, che risiede nel server Sentinel.

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

### Per Gestione servizi di raccolta:

```
collectormanager=<password>
```

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

### Per il motore di correlazione:

```
correlationengine=<password>
```

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

- 7 Fare clic su **Avanti**.
- 8 Accettare il certificato.
- 9 Per completare l'installazione, fare clic su **Avanti**.

Al termine dell'installazione viene visualizzato un messaggio che include il tipo di applicazione (Gestione servizi di raccolta o motore di correlazione 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.

## 13.3 Configurazione dell'applicazione successiva all'installazione

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

- ♦ [Sezione 13.3.1, "Configurazione di WebYaST"](#), a pagina 85
- ♦ [Sezione 13.3.2, "Creazione di partizioni"](#), a pagina 85
- ♦ [Sezione 13.3.3, "Registrazione degli aggiornamenti"](#), a pagina 86
- ♦ [Sezione 13.3.4, "Configurazione dell'applicazione con SMT"](#), a pagina 86

## 13.3.1 Configurazione di WebYaST

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

- 1 Effettuare il login all'applicazione Sentinel.
- 2 Fare clic su **Applicazione**.
- 3 Configurare il server di Sentinel per ricevere gli aggiornamenti come descritto in [Sezione 13.3.3, "Registrazione degli aggiornamenti"](#), a pagina 86.
- 4 Fare clic su **Avanti** per completare la configurazione iniziale.

## 13.3.2 Creazione di partizioni

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 [Sezione 6.6, "Pianificazione delle partizioni per la memorizzazione dei dati"](#), a pagina 45. 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
```

### 13.3.3 Registrazione degli aggiornamenti

Per ricevere le patch di aggiornamento, è necessario registrare l'applicazione Sentinel nel relativo canale di aggiornamento. Per registrare l'applicazione, ottenere prima di tutto il codice di registrazione o la chiave di attivazione dal [servizio di assistenza clienti NetIQ](#).

Per registrare l'applicazione e ricevere gli aggiornamenti, utilizzare la procedura seguente:

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

### 13.3.4 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 NetIQ Customer Center completo di importanti funzionalità.

- ♦ [“Prerequisiti” a pagina 86](#)
- ♦ [“Configurazione dell'applicazione” a pagina 87](#)
- ♦ [“Esecuzione dell'upgrade dell'applicazione” a pagina 87](#)

#### Prerequisiti

- ♦ Ottenere le credenziali di NetIQ Customer Center per Sentinel in modo da poter usufruire degli aggiornamenti forniti da NetIQ. Per ulteriori informazioni su come ottenere le credenziali, rivolgersi al [supporto NetIQ](#).
- ♦ Assicurarsi che SLES 11 SP3 sia installato con i pacchetti seguenti sul computer in cui si desidera installare SMT:
  - ♦ 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 presenti 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 informazioni sulla configurazione dell'applicazione con SMT, vedere [Subscription Management Tool \(SMT\) for SUSE Linux Enterprise 11](#) (Subscription Management Tool (SMT) per SUSE Linux Enterprise 11).

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

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

## Esecuzione dell'upgrade dell'applicazione

Per informazioni sull'upgrade dell'applicazione, vedere la [Sezione 25.3, "Esecuzione dell'upgrade dell'applicazione mediante SMT"](#), a pagina 134.

# 13.4 Interruzione e avvio del server mediante WebYaST

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

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



---

# 14 Installazione di Gestione servizi di raccolta NetFlow

Gestione servizi di raccolta NetFlow deve essere installato in un computer separato e non in quello in cui risiede il server Sentinel, Gestione servizi di raccolta o un motore di correlazione.

## 14.1 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).

## 14.2 Procedura di installazione di Gestione servizi di raccolta NetFlow

Per l'installazione delle istanze di Gestione servizi di raccolta NetFlow è possibile utilizzare uno dei metodi seguenti:

- ♦ **Standard:** utilizza i valori di default per la configurazione di NetFlow.
- ♦ **Personalizzato:** consente di personalizzare il numero di porta del server Sentinel.

---

### Nota

- ♦ Per inviare i dati del flusso di rete al server Sentinel è necessario essere un amministratore, appartenere al ruolo Provider di NetFlow o disporre dell'autorizzazione Invia dati NetFlow.
- ♦ Se si intende installare più di un'istanza di Gestione servizi di raccolta NetFlow, per inviare i dati del flusso di rete a Sentinel è necessario creare un nuovo account utente per ciascuna istanza. L'utilizzo di diversi account utente per ciascuna istanza di Gestione servizi di raccolta NetFlow offre un livello di controllo aggiuntivo sulle istanze che sono autorizzate a inviare i dati a Sentinel.

---

Per installare Gestione servizi di raccolta NetFlow:

- 1 Avviare l'interfaccia Web di Sentinel specificando l'URL seguente nell'interfaccia Web in uso:

`https://<IP_Address_Sentinel_server>:8443`

<Indirizzo\_IP\_server\_Sentinel> è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

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

- 2 Nella barra degli strumenti, fare clic su **Download**.
- 3 Sotto l'intestazione Gestione servizi di raccolta NetFlow, fare clic su **Download del programma di installazione**.

- 4 Fare clic su **Salva file** per salvare il programma di installazione nell'ubicazione desiderata.
- 5 Al prompt dei comandi, specificare il comando seguente per decomprimere il file di installazione.

```
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:

```
cd <directory_name>
```

- 7 Per installare Gestione servizi di raccolta NetFlow, immettere il comando seguente:

```
./install-netflow
```

- 8 Specificare il numero corrispondente alla lingua che si desidera utilizzare per l'installazione, quindi premere Invio.
- 9 Premere la BARRA SPAZIATRICE per leggere il contratto di licenza.
- 10 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.
- 11 Specificare se si desidera eseguire un'installazione standard o personalizzata.
- 12 Specificare il nome host o l'indirizzo IP del server Sentinel che deve ricevere i dati del flusso di rete.
- 13 (Condizionale) Se si sceglie l'installazione personalizzata, specificare il numero di porta del server Sentinel.  
Il numero di porta di default è 8443.
- 14 Specificare il nome utente e la password per l'autenticazione al server Sentinel.

---

**Nota:** accertarsi che le credenziali utente specificate dispongano dell'autorizzazione Invia dati NetFlow o dei privilegi di amministratore. In caso contrario, l'installazione viene completata ma quando Gestione servizi di raccolta NetFlow invia i dati al server Sentinel l'autenticazione ha esito negativo.

---

L'installazione viene completata. Affinché Gestione servizi di raccolta NetFlow stabilisca la connessione con il server Sentinel sono necessari alcuni minuti.

- 15 (Facoltativo) È possibile verificare se Gestione servizi di raccolta NetFlow è stato installato correttamente eseguendo una delle operazioni seguenti:
  - ♦ Verificare che i servizi di Gestione servizi di raccolta NetFlow siano in esecuzione:

```
/etc/init.d/sentinel status
```
  - ♦ Verificare che Gestione servizi di raccolta NetFlow abbia stabilito una connessione con il server Sentinel:

```
netstat -an |grep 'ESTABLISHED' |grep <HTTPS_port_number>
```
  - ♦ Verificare che Gestione servizi di raccolta NetFlow sia visualizzato nella console Web di Sentinel facendo clic su **Raccolta > NetFlow**.
- 16 Abilitare l'inoltro del traffico del flusso di rete nel dispositivo da cui si desidera raccogliere i dati del flusso di rete.  
Durante la procedura di abilitazione di NetFlow sul dispositivo è necessario specificare l'indirizzo IP del server Sentinel e la porta su cui Gestione servizi di raccolta NetFlow riceve i dati dal dispositivo abilitato NetFlow. Il numero di porta di default è 3578. Per ulteriori informazioni, consultare la documentazione specifica del dispositivo abilitato NetFlow.

---

# 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.

- ♦ [Sezione 15.1, "Installazione di un servizio di raccolta"](#), a pagina 91
- ♦ [Sezione 15.2, "Installazione di un connettore"](#), a pagina 91

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

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

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

Per configurare 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
```

- ♦ Verifica dell'attivazione ed esecuzione dei servizi di Sentinel:

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

- ♦ Verifica dell'attivazione ed esecuzione dei servizi Web:

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

Il numero di porta di default è 8443.

- ♦ Accesso all'interfaccia Web di Sentinel:

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

```
https://<IP_Address/DNS_Sentinel_server:8443>
```

IP\_Address/DNS\_Sentinel\_server è l'indirizzo IP o il nome DNS del server Sentinel e 8443 è la sua porta di default.

3. Eseguire il login con il nome utente e la password dell'amministratore specificati durante l'installazione. Il nome utente di default è admin.



---

# IV Configurazione di Sentinel

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

- ♦ [Capitolo 17, "Orario di configurazione", a pagina 97](#)
- ♦ [Capitolo 18, "Modificare la configurazione dopo l'installazione", a pagina 103](#)
- ♦ [Capitolo 19, "Configurazione dei plug-in pronti all'uso", a pagina 105](#)
- ♦ [Capitolo 20, "Abilitazione della modalità FIPS 140-2 in un'installazione esistente di Sentinel", a pagina 107](#)
- ♦ [Capitolo 21, "Esecuzione di Sentinel in modalità FIPS 140-2", a pagina 109](#)



---

# 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.

- ♦ [Sezione 17.1, "L'orario in Sentinel", a pagina 97](#)
- ♦ [Sezione 17.2, "Configurazione dell'orario in Sentinel", a pagina 99](#)
- ♦ [Sezione 17.3, "Configurazione della soglia di ritardo degli eventi", a pagina 99](#)
- ♦ [Sezione 17.4, "Gestione dei fusi orari", a pagina 99](#)

## 17.1 L'orario in Sentinel

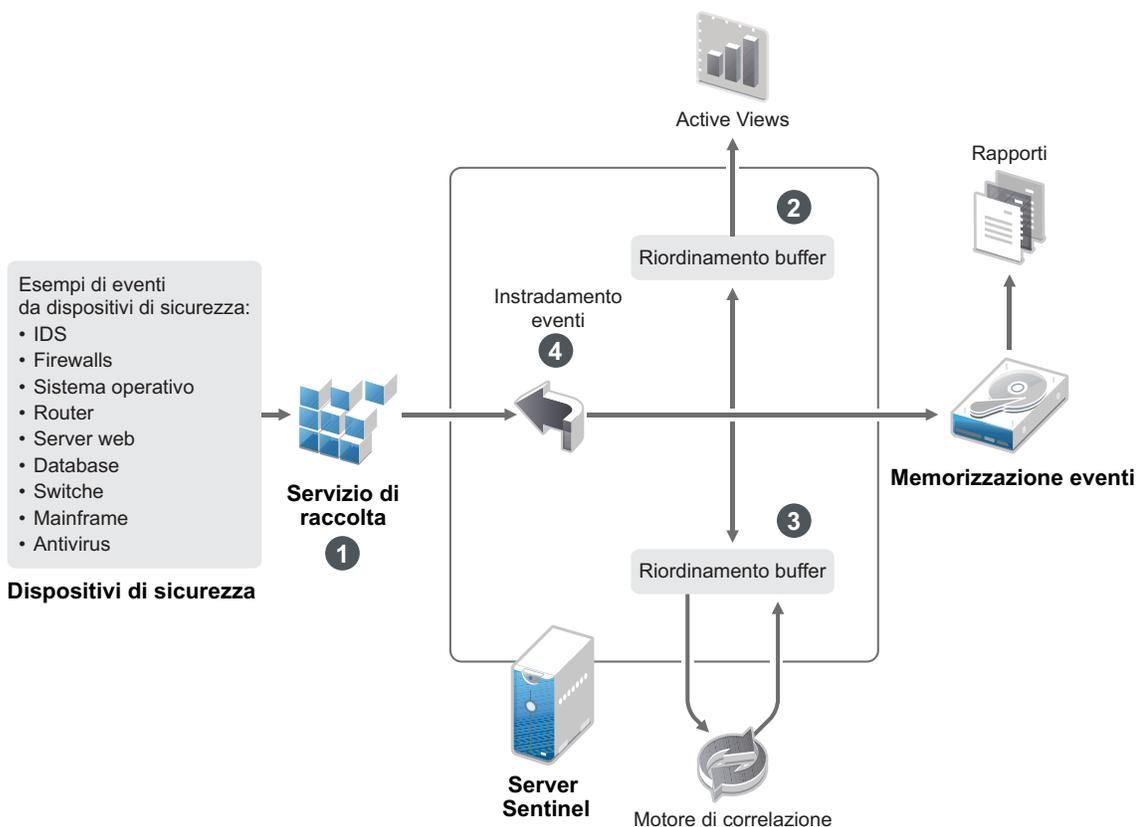
Sentinel è un sistema distribuito e consiste in diversi processi che possono essere realizzati in varie parti della rete. L'origine eventi potrebbe inoltre indurre alcuni ritardi. Per gestire al meglio tale situazione, prima dell'elaborazione i processi di Sentinel riordinano gli eventi in un flusso 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 Gestione servizi di raccolta.
- ♦ **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, viene fornita la spiegazione del modo in cui Sentinel realizza questa operazione:

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 da Active Views. Gli eventi con EventTime oltre i 5 minuti successivi non vengono visualizzati in Active Views, 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 dal motore di correlazione in ordine cronologico. Se EventTime è anteriore a 30 secondi rispetto all'orario del server, il motore di correlazione non elabora gli eventi.
4. Se EventTime è anteriore a 5 minuti rispetto all'orario di sistema di Gestione servizi di raccolta, gli eventi vengono direttamente instradati alla relativa memorizzazione, ignorando i sistemi in tempo reale quali Correlazione, Active Views e Security Intelligence.

## 17.2 Configurazione dell'orario in Sentinel

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

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

Per modificare questa impostazione sull'origine evento:

- 1 Effettuare il login a Gestione origini eventi.

Per ulteriori informazioni, consultare [“Accessing Event Source Management \(Accesso alla Gestione origini eventi\)”](#) nella *NetIQ Sentinel Administration Guide (Guida all'amministrazione di NetIQ Sentinel 7.0.1)*.

- 2 Selezionare con il pulsante destro del mouse l'origine evento della quale si desidera modificare le impostazioni relative all'orario, quindi scegliere **Modifica**.
- 3 Selezionare o meno l'opzione **Origine evento elemento attendibile** presente nella parte inferiore della scheda **Generale**.
- 4 Fare clic su **OK** per salvare la modifica.

## 17.3 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>
```

## 17.4 Gestione dei fusi orari

In un ambiente distribuito, la gestione dei fusi orari può essere molto complessa. Ad esempio, potrebbe presentarsi la situazione in cui un'origine evento si trova in un fuso orario, Gestione servizi di raccolta in un altro, il server Sentinel di back end in un altro e il client che sta visualizzando i dati in

un altro fuso orario ancora. Quando vengono aggiunti elementi quali l'ora legale e le molte origini evento che non segnalano il fuso orario che è stato loro impostato (come tutte le origini syslog), i problemi da gestire potrebbero essere diversi. La flessibilità caratteristica di Sentinel consente di rappresentare nel modo più adeguato l'orario in cui effettivamente si verificano gli eventi e comparare tali eventi con altri provenienti da altre origini evento presenti nello stesso o in un diverso fuso orario.

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

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

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

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 nella Gestione servizi di raccolta. OraEventoDispositivo e OraEvento sono memorizzati come UTC e i campi FOSensore sono memorizzati come stringhe impostate per l'ora locale dell'origine evento. Queste informazioni vengono inviate dalla Gestione servizi di raccolta al server Sentinel e memorizzate nella memorizzazione eventi. Il fuso orario in cui si trova Gestione servizi di raccolta o il server Sentinel non ha alcuna implicazione sul processo o sui dati memorizzati. Tuttavia, quando un client visualizza l'evento in un browser Web, l'OraEvento UTC viene convertita nell'ora

locale relativa a tale browser, affinché tutti gli eventi siano presentati ai client nel fuso orario locale. Se gli utenti desiderano visualizzare l'ora locale dell'origine, possono disporre di ulteriori dettagli consultando i campi FOSensore.



---

# 18 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 la console Web 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.

---

# 19 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.

- ♦ [Sezione 19.1, “Visualizzazione dei plug-in preinstallati”, a pagina 105](#)
- ♦ [Sezione 19.2, “Configurazione della raccolta di dati”, a pagina 105](#)
- ♦ [Sezione 19.3, “Configurazione dei pacchetti soluzione”, a pagina 105](#)
- ♦ [Sezione 19.4, “Configurazione di azioni e integratori”, a pagina 106](#)

## 19.1 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 Web di Sentinel come amministratore all'indirizzo `https://<indirizzo IP>:8443`, dove 8443 è la porta di default del server Sentinel.
- 2 Fare clic su **Plug-in > Catalogo**.

## 19.2 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 [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel).

## 19.3 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 [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel 7.1)..

I pacchetti soluzione consentono di organizzare in categorie e raggruppare i contenuti in vari set di controlli o policy che vengono gestiti come una sola unità. I controlli inclusi nei pacchetti soluzione vengono preinstallati affinché i contenuti pronti all'uso siano immediatamente disponibili. Tuttavia, tali controlli devono essere formalmente implementati o provati mediante la console Web di Sentinel.

Se è richiesta una verifica rigorosa per dimostrare che l'implementazione di Sentinel funziona come previsto, è possibile utilizzare il processo di attestazione formale incorporato nei pacchetti soluzione. Tale processo implementa e prova i controlli dei pacchetti soluzione allo stesso modo in cui un utente esegue l'implementazione e la prova dei controlli di qualsiasi altro pacchetto soluzione. Come parte

integrante del processo, i programmi incaricati di eseguire l'implementazione e la prova attestano che il lavoro da loro svolto è stato completato. Successivamente, tali attestazioni diventano parte di un audit trail che può essere analizzato per dimostrare che ogni controllo è stato installato in modo adeguato.

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

## 19.4 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](#).

---

# 20 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`.

---

- ♦ [Sezione 20.1, “Abilitazione dell'esecuzione in modalità FIPS 140-2 nel server Sentinel”, a pagina 107](#)
- ♦ [Sezione 20.2, “Abilitazione della modalità FIPS 140-2 in istanze remote di Gestione servizi di raccolta e del motore di correlazione”, a pagina 107](#)

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

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

- 1 Eseguire il login al server Sentinel.
- 2 Passare all'utente `novell` (`su novell`).
- 3 Passare alla directory `bin` di Sentinel.
- 4 Eseguire lo script `convert_to_fips.sh` e seguire le istruzioni visualizzate.
- 5 Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel [Capitolo 21, “Esecuzione di Sentinel in modalità FIPS 140-2”, a pagina 109](#).

## 20.2 Abilitazione della modalità FIPS 140-2 in istanze remote di Gestione servizi di raccolta e del motore di correlazione

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 Gestione servizi di raccolta e del motore di correlazione.

**Per abilitare l'esecuzione in modalità FIPS 140-2 di un'istanza remota di Gestione servizi di raccolta o del motore di correlazione:**

- 1 Eseguire il login al sistema remoto di Gestione servizi di raccolta o del motore di correlazione.
- 2 Passare all'utente `novell` (`su novell`).
- 3 Passare alla directory `bin`. L'ubicazione di default è `/opt/novell/sentinel/bin`.

- 4 Eseguire lo script `convert_to_fips.sh` e seguire le istruzioni visualizzate.
- 5 Completare la configurazione della modalità FIPS 140-2 eseguendo i task descritti nel [Capitolo 21, "Esecuzione di Sentinel in modalità FIPS 140-2"](#), a pagina 109.

---

# 21 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.

- ♦ [Sezione 21.1, "Configurazione del servizio Advisor in modalità FIPS 140-2"](#), a pagina 109
- ♦ [Sezione 21.2, "Configurazione della ricerca distribuita in modalità FIPS 140-2"](#), a pagina 109
- ♦ [Sezione 21.3, "Configurazione dell'autenticazione LDAP in modalità FIPS 140-2"](#), a pagina 111
- ♦ [Sezione 21.4, "Aggiornamento dei certificati del server nelle istanze remote di Gestione servizi di raccolta e del motore di correlazione"](#), a pagina 111
- ♦ [Sezione 21.5, "Configurazione dei plug-in di Sentinel per l'esecuzione in modalità FIPS 140-2"](#), a pagina 112
- ♦ [Sezione 21.6, "Importazione di certificati nel database di archivio chiavi FIPS"](#), a pagina 118
- ♦ [Sezione 21.7, "Ripristino di Sentinel nella modalità non FIPS"](#), a pagina 118

## 21.1 Configurazione del servizio Advisor in modalità FIPS 140-2

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

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

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

Per ulteriori informazioni sull'importazione del certificato, vedere ["Importazione di certificati nel database di archivio chiavi FIPS"](#) a pagina 118.

## 21.2 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 118.](#)
- 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>/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 118.](#)
- 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>/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 118.](#)
- 5 Riavviare i servizi Sentinel nel computer di origine.

## 21.3 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 118.](#)

- 3 Eseguire il login alla console Web di Sentinel come utente con ruolo amministrativo e continuare la configurazione dell'autenticazione LDAP.

Per ulteriori informazioni, vedere ["Configuring LDAP Authentication"](#) (Configurazione dell'autenticazione LDAP) nella [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ 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`.

---

## 21.4 Aggiornamento dei certificati del server nelle istanze remote di Gestione servizi di raccolta e del motore di correlazione

Per configurare le istanze remote esistenti di Gestione servizi di raccolta e del motore di correlazione 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 Gestione servizi di raccolta o del motore di correlazione in modalità non FIPS. Le istanze remote di Gestione servizi di raccolta 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 Gestione servizi di raccolta o del motore di correlazione, è necessario copiare nel sistema remoto il certificato del server Sentinel più recente, affinché Gestione servizi di raccolta o il motore di correlazione possano comunicare con il server Sentinel.

Per aggiornare il certificato del server Sentinel nell'istanza remota di Gestione servizi di raccolta o del motore di correlazione:

- 1 Eseguire il login al computer remoto in cui è installato Gestione servizi di raccolta o il motore di correlazione.
- 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.

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

---

- ♦ [Sezione 21.5.1, “Connettore di Gestione agenti”, a pagina 112](#)
- ♦ [Sezione 21.5.2, “Connettore del database \(JDBC\)”, a pagina 113](#)
- ♦ [Sezione 21.5.3, “Connettore di collegamento Sentinel”, a pagina 113](#)
- ♦ [Sezione 21.5.4, “Connettore Syslog”, a pagina 114](#)
- ♦ [Sezione 21.5.5, “Connettore degli eventi di Windows \(WMI\)”, a pagina 115](#)
- ♦ [Sezione 21.5.6, “Integratore di Collegamento Sentinel”, a pagina 116](#)
- ♦ [Sezione 21.5.7, “Integratore LDAP”, a pagina 117](#)
- ♦ [Sezione 21.5.8, “Integratore SMTP”, a pagina 117](#)
- ♦ [Sezione 21.5.9, “Utilizzo di connettori non FIPS con Sentinel in modalità FIPS 140-2”, a pagina 117](#)

### 21.5.1 Connettore di Gestione agenti

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

**Per configurare il connettore di Gestione agenti affinché venga eseguito in modalità FIPS 140-2:**

- 1 Aggiungere o modificare il server di origine eventi di Gestione agenti. 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 Gestione agenti).
- 2 Selezionare una delle opzioni nel campo *Tipo di autenticazione client*. Il tipo di autenticazione del client determina il livello di rigosità adottato dal server di origine eventi SSL di Gestione agenti per la verifica dell'identità delle origini eventi di Gestione agenti che tentano di inviare dati.
  - ♦ **Aperta:** consente le connessioni SSL provenienti da agenti di Gestione agenti. 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 Gestione agenti. 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 118](#).

---

**Nota:** in modalità FIPS 140-2, il server di origine eventi di Gestione agenti 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 Gestione servizi di raccolta, 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 Gestione servizi di raccolta:** `/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 Gestione agenti consideri attendibile il file del relativo certificato.

---

## 21.5.2 Connettore del database (JDBC)

Eeguire 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 118](#).

- 3 Continuare la configurazione del connettore.

## 21.5.3 Connettore di collegamento Sentinel

Eeguire 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. Eeguire 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 rigidità 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 118](#).

---

**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.

---

## 21.5.4 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 rigidità 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 118](#).

---

**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 Gestione servizi di raccolta, 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 Gestione servizi di raccolta** 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.

---

## 21.5.5 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 118](#).

---

**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 Gestione servizi di raccolta, 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 Gestione servizi di raccolta** 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 118](#).

## 21.5.6 Integratore di Collegamento Sentinel

Eeguire 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 Gestione servizi di raccolta, è necessario copiare il file `/etc/opt/novell/sentinel/config/rcm.cer` dal computer destinatario dell'istanza remota di Gestione servizi di raccolta 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 118](#).

- 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.

---

## 21.5.7 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 118](#).

- 3 Continuare la configurazione dell'istanza dell'integratore.

## 21.5.8 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.

## 21.5.9 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 Gestione servizi di raccolta in modalità non FIPS per la connessione al server Sentinel in modalità FIPS 140-2.

Per ulteriori informazioni, vedere il [Sezione 12.4, "Installazione di istanze di Gestione servizi di raccolta e del motore di correlazione"](#), a pagina 73.

- 2 Installare i connettori non FIPS nell'istanza remota di Gestione servizi di raccolta 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 Gestione servizi di raccolta connessa a un server Sentinel in modalità FIPS 140-2. Per ulteriori informazioni sui problemi noti, vedere le [note di rilascio di Sentinel 7.1](#).

---

## 21.6 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. Poiché non è possibile effettuare l'upload dei certificati mediante l'interfaccia utente di Sentinel in modalità normale 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 Gestione servizi di raccolta, è necessario importare i certificati nel database dell'archivio chiavi FIPS dell'istanza remota di Gestione servizi di raccolta 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 Gestione servizi di raccolta.
- 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 Gestione servizi di raccolta, immettere `sì` o `s`.

## 21.7 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.

- ♦ [Sezione 21.7.1, "Ripristino del server Sentinel nella modalità non FIPS", a pagina 118](#)
- ♦ [Sezione 21.7.2, "Ripristino della modalità non FIPS in istanze remote di Gestione servizi di raccolta e del motore di correlazione", a pagina 119](#)

### 21.7.1 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-fips2013012419111359034887.tar.gz` è il file di backup, eseguire il comando seguente:

```
./backup_util.sh -f non-fips2013012419111359034887.tar.gz -m 'restore'
```

- 5 Riavviare il server Sentinel.

## 21.7.2 Ripristino della modalità non FIPS in istanze remote di Gestione servizi di raccolta e del motore di correlazione

È possibile ripristinare la modalità non FIPS in istanze remote di Gestione servizi di raccolta e del motore di correlazione.

**Per ripristinare la modalità non FIPS in istanze remote di Gestione servizi di raccolta e del motore di correlazione:**

- 1 Eseguire il login al sistema remoto di Gestione servizi di raccolta o del motore di correlazione.
- 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 Gestione servizi di raccolta o del motore di correlazione.



---

# V Esecuzione dell'upgrade di Sentinel

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

- ♦ [Capitolo 22, “Elenco di controllo per l'implementazione”, a pagina 123](#)
- ♦ [Capitolo 23, “Prerequisiti”, a pagina 125](#)
- ♦ [Capitolo 24, “Upgrade dell'installazione tradizionale di Sentinel”, a pagina 127](#)
- ♦ [Capitolo 25, “Esecuzione dell'upgrade dell'applicazione Sentinel”, a pagina 131](#)
- ♦ [Capitolo 26, “Esecuzione dell'upgrade dei plug-in di Sentinel”, a pagina 137](#)



---

# 22 Elenco di controllo per l'implementazione

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

*Tabella 22-1 Elenco di controllo per l'implementazione*

<input type="checkbox"/>	Task	Vedere
<input type="checkbox"/>	Accertarsi che i computer in cui si installano Sentinel e i relativi componenti siano conformi ai requisiti specificati.	<a href="#">Sito Web delle informazioni tecniche di NetIQ Sentinel</a>
<input type="checkbox"/>	Per informazioni sui problemi noti, esaminare le note di rilascio relative al sistema operativo supportato.	<a href="#">Note di rilascio di SUSE</a>
<input type="checkbox"/>	Esaminare le note di rilascio di Sentinel per informazioni sulle nuove funzionalità e i problemi noti.	<a href="#">Note di rilascio di Sentinel</a>



---

# 23 Prerequisiti

- ♦ Sezione 23.1, “Prerequisito per l'esecuzione di Sentinel in modalità FIPS”, a pagina 125
- ♦ Sezione 23.2, “Prerequisito per versioni precedenti a Sentinel 7.1.1”, a pagina 125

## 23.1 Prerequisito per l'esecuzione di Sentinel in modalità FIPS

Il prerequisito seguente si applica nel caso in cui sia stato eseguito il downgrade della versione di Java utilizzando JRE 7 Update 45 per risolvere i problemi di connessione fra client e Sentinel in esecuzione in modalità FIPS come menzionato in [Problemi noti di Sentinel 7.2.2](#).

Se nelle directory di installazione di Sentinel sono presenti collegamenti simbolici, il programma di installazione di Sentinel interrompe l'upgrade. Quando si effettua il download e si installa JRE 7 Update 45 per eseguire il downgrade della versione Java, la cartella JRE contiene una sottocartella denominata `man` in cui risiedono collegamenti simbolici. Per completare l'upgrade a Sentinel 7.3 e versioni successive è quindi necessario eliminare la cartella `man`. Tuttavia, in caso di download e installazione di JDK 7 Update 45 invece di JRE 7 Update 45, la cartella `man` non conterrà collegamenti simbolici e non dovrà essere eliminata.

### Per eliminare la cartella `man`:

- 1 Eseguire il login al server Sentinel come utente novell.
- 2 Specificare il comando seguente per cambiare la directory:

```
cd /opt/novell/sentinel/jre/
```

- 3 Eliminare la cartella `man`:

```
rm -rf man
```

## 23.2 Prerequisito per versioni precedenti a Sentinel 7.1.1

In Sentinel 7.1.1 e versioni successive è inclusa la versione 2.4.1 di MongoDB. In MongoDB 2.4 è necessario rimuovere dal database i nomi utente duplicati. Se si esegue l'upgrade da versioni di Sentinel precedenti alla 7.1.1, verificare se sono presenti utenti duplicati e rimuoverli.

### Per individuare gli utenti duplicati, utilizzare la procedura seguente:

- 1 Eseguire il login al server Sentinel 7.1 o versioni precedenti come utente novell.
- 2 Passare alla directory seguente:

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

- 3 Per verificare la presenza di utenti duplicati, eseguire i comandi seguenti:

```
./mongo --port 27017 --host "localhost"  
use analytics
```

```
db.system.users.find().count()
```

Se il valore di `count` è superiore a 1, significa che sono presenti utenti duplicati.

**Per rimuovere gli utenti duplicati, utilizzare la procedura seguente:**

- 1 Per ottenere un elenco degli utenti, eseguire il comando seguente:

```
db.system.users.find().pretty()
```

Il comando fornisce un elenco di utenti con le voci duplicate. Il primo utente dell'elenco è quello originale. Si dovrà quindi mantenere il primo utente ed eliminare gli altri presenti nell'elenco.

- 2 Per rimuovere gli utenti duplicati, eseguire il comando seguente:

```
db.system.users.remove({ _id : ObjectId("object_ID") })
```

- 3 Per verificare che gli utenti duplicati siano stati rimossi, eseguire il comando seguente:

```
db.system.users.find().pretty()
```

- 4 Passare all'utente amministratore del database:

```
use admin
```

- 5 Ripetere le operazioni dal [Passo 1](#) al [Passo 3](#) per verificare e rimuovere eventuali duplicati di `dbausers` nel database di amministrazione.

---

# 24 Upgrade dell'installazione tradizionale di Sentinel

- ♦ Sezione 24.1, “Esecuzione dell'upgrade di Sentinel”, a pagina 127
- ♦ Sezione 24.2, “Upgrade di Sentinel come utente non root”, a pagina 128
- ♦ Sezione 24.3, “Upgrade di Gestione servizi di raccolta e del motore di correlazione”, a pagina 130

## 24.1 Esecuzione dell'upgrade di Sentinel

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

- 1 eseguire il backup della configurazione, quindi creare un'esportazione ESM.  
Per ulteriori informazioni sul backup dei dati, vedere “[Backing Up and Restoring Data](#)” (Backup e ripristino dei dati) nella *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).
- 2 (Condizionale) Se nei file `server.xml`, `collector_mgr.xml` o `correlation_engine.xml` le impostazioni di configurazione sono state personalizzate, accertarsi di aver creato i rispettivi file delle proprietà denominati con l'ID del componente dell'oggetto affinché le personalizzazioni non vadano perse con l'upgrade. Per ulteriori informazioni, vedere “[Maintaining Custom Settings in XML Files](#)” (Conservazione delle impostazioni personalizzate nei file XML) nella *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di Sentinel NetIQ).
- 3 Effettuare il download della versione più recente del programma di installazione dal [sito Web dei download di NetIQ](#).
- 4 Effettuare il login come utente `root` al server in cui si desidera eseguire l'upgrade di Sentinel.
- 5 Specificare il seguente comando per estrarre i file di installazione dal file `.tar`:  

```
tar xfz <install_filename>
```

  
Sostituire `<nomefile_installazione>` con il nome attuale del file di installazione.
- 6 Passare alla directory in cui è stato estratto il file d'installazione.
- 7 Per eseguire l'upgrade di Sentinel, specificare il comando seguente:  

```
./install-sentinel
```
- 8 Per continuare impostando una lingua desiderata, selezionare il numero visualizzato accanto alla lingua.  
Il contratto di licenza con l'utente finale viene visualizzato nella lingua selezionata.
- 9 Leggere il contratto di licenza con l'utente finale, immettere `sì` o `s` per accettarlo, quindi continuare con il processo di installazione.
- 10 Lo script di installazione individua una versione precedente al prodotto già esistente nel sistema e richiede all'utente di specificare se si desidera eseguire l'upgrade del prodotto. Per continuare con l'upgrade, premere `s`.  
L'installazione inizia a installare tutti i pacchetti RPM. Il completamento dell'installazione potrebbe richiedere alcuni secondi.

- 11 Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.
- 12 Svuotare la cache di Java Web Start nei computer client, affinché venga utilizzata la versione più recente delle applicazioni Sentinel.  
Per svuotare la cache di Java Web Start è possibile utilizzare il comando `avaws -clearcache` o Java Control Center. Per ulteriori informazioni, vedere [http://www.java.com/en/download/help/plugin\\_cache.xml](http://www.java.com/en/download/help/plugin_cache.xml).
- 13 (Condizionale) Nel caso in cui sia stato eseguito un upgrade sostanziale del database PostgreSQL (ad esempio da 8.0 a 9.0 o da 9.0 a 9.1) eliminare i file della versione precedente dal database PostgreSQL. Per informazioni sull'esecuzione dell'upgrade del database PostgreSQL, vedere le note di rilascio di Sentinel.
  - 13a Passare all'utente novell.  

```
su novell
```
  - 13b Passare alla cartella bin:  

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```
  - 13c Cancellare i vecchi file PostgreSQL utilizzando il comando seguente:  

```
./delete_old_cluster.sh
```
- 14 (Condizionale) In caso di upgrade da Sentinel 7.1.1 o versioni precedenti, il programma di installazione non esegue la migrazione dei dati di security intelligence (SI) di default. Per eseguire la migrazione dei dati SI da Sentinel 7.1.1 o versioni precedenti, abilitarla manualmente come segue:
  - 14a Passare all'utente Novell.  

```
su novell
```
  - 14b Aprire il file `/etc/opt/novell/sentinel/config/server.xml`.
  - 14c Nella sezione `BaseliningRuntime` del componente aggiungere la proprietà seguente:  

```
<property name="baselining.migration.check">true</property>
```
  - 14d Riavviare il server Sentinel.
- 15 Per eseguire l'upgrade dei sistemi di Gestione servizi di raccolta e del motore di correlazione, vedere la [Sezione 24.3, "Upgrade di Gestione servizi di raccolta e del motore di correlazione"](#), a [pagina 130](#).

## 24.2 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 [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel).
- 2 (Condizionale) Se nei file `server.xml`, `collector_mgr.xml` o `correlation_engine.xml` le impostazioni di configurazione sono state personalizzate, accertarsi di aver creato i rispettivi file delle proprietà denominati con l'ID del componente dell'oggetto affinché le personalizzazioni non

vadano perse con l'upgrade. Per ulteriori informazioni, vedere “[Maintaining Custom Settings in XML Files](#)” (Conservazione delle impostazioni personalizzate nei file XML) nella *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di Sentinel NetIQ).

- 3 Effettuare il download dei file di installazione dal [sito Web dei download di NetIQ](#).
- 4 Nella riga di comando, specificare il comando seguente per estrarre i file di installazione dal file tar:

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

Sostituire *<nomefile\_installazione>* con il nome attuale del file di installazione.

- 5 Effettuare il login come utente `root` al server in cui si desidera eseguire l'upgrade di Sentinel.
- 6 Estrarre l'RPM `squashfs` dai file di installazione di Sentinel.
- 7 Installare `squashfs` nel server Sentinel.

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

- 8 Specificare il comando seguente per modificare l'utente `novell` non root appena creato: `novell:`  
`su novell`

- 9 (Condizionale) Per eseguire un upgrade interattivo:

- 9a** Immettere il comando seguente:

```
./install-sentinel
```

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

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

- 9b** Continuare con la [Passo 11](#).

- 10 (Condizionale) Per eseguire un upgrade automatico, specificare il comando seguente:

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

L'installazione continua con i valori memorizzati nel file di risposta. L'upgrade di Sentinel è terminato.

- 11 Immettere il numero corrispondente alla lingua che si desidera utilizzare per l'upgrade.

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

- 12 Leggere la licenza con l'utente finale e immettere `sì` o `s` per accettarla e continuare l'upgrade.

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

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

- 14 Svuotare la cache di Java Web Start nei computer client, affinché venga utilizzata la versione più recente delle applicazioni Sentinel.

Per svuotare la cache di Java Web Start è possibile utilizzare il comando `avaws -clearcache` o Java Control Center. Per ulteriori informazioni, vedere [http://www.java.com/en/download/help/plugin\\_cache.xml](http://www.java.com/en/download/help/plugin_cache.xml).

- 15 (Condizionale) Nel caso in cui sia stato eseguito un upgrade sostanziale del database PostgreSQL (ad esempio da 8.0 a 9.0 o da 9.0 a 9.1) eliminare i file della versione precedente dal database PostgreSQL. Per informazioni sull'esecuzione dell'upgrade del database PostgreSQL, vedere le note di rilascio di Sentinel.

- 15a** Passare all'utente Novell.

```
su novell
```

**15b** Passare alla cartella bin:

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

**15c** Cancellare i vecchi file PostgreSQL utilizzando il comando seguente:

```
./delete_old_cluster.sh
```

**16** (Condizionale) In caso di upgrade da Sentinel 7.1.1 o versioni precedenti, il programma di installazione non esegue la migrazione dei dati di security intelligence (SI) di default. Per eseguire la migrazione dei dati SI da Sentinel 7.1.1 o versioni precedenti, abilitarla manualmente come segue:

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

```
su novell
```

**16b** Aprire il file `/etc/opt/novell/sentinel/config/server.xml`.

**16c** Nella sezione `BaseliningRuntime` del componente aggiungere la proprietà seguente:

```
<property name="baselining.migration.check">true</property>
```

**16d** Riavviare il server Sentinel.

## 24.3 Upgrade di Gestione servizi di raccolta e del motore di correlazione

Per eseguire l'upgrade di Gestione servizi di raccolta o del motore di correlazione, 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 *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).

2 Eseguire il login all'interfaccia Web di Sentinel come utente con un ruolo amministrativo.

3 Selezionare **Download**.

4 Fare clic su **Download del programma di installazione** nella sezione Programma di installazione della Gestione servizi di raccolta.

Viene visualizzata una finestra contenente le opzioni per aprire o salvare il file del programma di installazione nel computer locale.

5 Salvare il file.

6 Copiare il file in un'ubicazione temporanea.

7 Estrarre i contenuti del file.

8 Eseguire lo script seguente:

**Per Gestione servizi di raccolta:**

```
./install-cm
```

**Per il motore di correlazione:**

```
./install-ce
```

9 Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo.

---

# 25 Esecuzione dell'upgrade dell'applicazione Sentinel

Le procedure riportate in questo capitolo descrivono come eseguire l'upgrade dell'applicazione Sentinel e delle applicazioni Gestione servizi di raccolta e Motore di correlazione.

- ♦ Sezione 25.1, “Esecuzione dell'upgrade dell'applicazione mediante Zypper”, a pagina 131
- ♦ Sezione 25.2, “Esecuzione dell'upgrade dell'applicazione mediante WebYaST”, a pagina 132
- ♦ Sezione 25.3, “Esecuzione dell'upgrade dell'applicazione mediante SMT”, a pagina 134

## 25.1 Esecuzione dell'upgrade dell'applicazione mediante Zypper

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

- 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 *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.0.1).
- 2 (Condizionale) Se nei file `server.xml`, `collector_mgr.xml` o `correlation_engine.xml` le impostazioni di configurazione sono state personalizzate, accertarsi di aver creato i rispettivi file delle proprietà denominati con l'ID del componente dell'oggetto affinché le personalizzazioni non vadano perse con l'upgrade. Per ulteriori informazioni, vedere “[Maintaining Custom Settings in XML Files](#)” (Conservazione delle impostazioni personalizzate nei file XML) nella *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di Sentinel NetIQ).
- 3 Eseguire il login alla console dell'applicazione come utente `root`.
- 4 Eseguire il comando seguente:  

```
/usr/bin/zypper patch
```
- 5 (Condizionale) In caso di upgrade da Sentinel 7.0.1 o versioni precedenti, immettere `1` per accettare il cambiamento di fornitore da Novell a NetIQ.
- 6 (Condizionale) In caso di upgrade da versioni di Sentinel precedenti alla 7.2, nel programma di installazione viene visualizzato un messaggio che indica di risolvere la dipendenza per alcuni pacchetti dell'applicazione. Immettere `1` per disinstallare i pacchetti dipendenti.
- 7 Immettere `y` per continuare.
- 8 Per accettare il contratto di licenza, immettere `yes`.
- 9 Riavviare l'applicazione Sentinel.
- 10 Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.
- 11 Svuotare la cache di Java Web Start nei computer client, affinché venga utilizzata la versione più recente delle applicazioni Sentinel.

Per svuotare la cache di Java Web Start è possibile utilizzare il comando `avaws -clearcache` o Java Control Center. Per ulteriori informazioni, vedere [http://www.java.com/en/download/help/plugin\\_cache.xml](http://www.java.com/en/download/help/plugin_cache.xml).

**12** (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.

**12a** Passare all'utente Novell.

```
su novell
```

**12b** Passare alla cartella bin:

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

**12c** Cancellare i vecchi file PostgreSQL utilizzando il comando seguente:

```
./delete_old_cluster.sh
```

**13** (Condizionale) In caso di upgrade da Sentinel 7.1.1 o versioni precedenti, il programma di installazione non esegue la migrazione dei dati di security intelligence (SI) di default. Per eseguire la migrazione dei dati SI da Sentinel 7.1.1 o versioni precedenti, abilitarla manualmente come segue:

**13a** Passare all'utente Novell.

```
su novell
```

**13b** Aprire il file `/etc/opt/novell/sentinel/config/server.xml`.

**13c** Nella sezione `BaseliningRuntime` del componente aggiungere la proprietà seguente:

```
<property name="baselining.migration.check">true</property>
```

**13d** Riavviare il server Sentinel.

---

**Nota:** per eseguire l'upgrade di Gestione servizi di raccolta e del motore di correlazione, eseguire dal [Passo 3](#) al [Passo 9](#).

---

## 25.2 Esecuzione dell'upgrade dell'applicazione mediante WebYaST

---

**Nota:** gli upgrade dell'applicazione da versioni precedenti a Sentinel 7.2 devono essere eseguiti mediante l'utility da riga di comando Zypper, poiché l'esecuzione dell'upgrade rende necessaria l'interazione con l'utente. WebYaST non consente tale interazione con l'utente. Per informazioni sull'uso di Zypper per eseguire l'upgrade dell'applicazione, consultare [Sezione 25.1, "Esecuzione dell'upgrade dell'applicazione mediante Zypper"](#), a pagina 131..

---

- 1 Eseguire il login all'applicazione Sentinel come utente in un ruolo amministrativo.
- 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 [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel 7.0.1).
- 3 (Condizionale) Se nei file `server.xml`, `collector_mgr.xml` o `correlation_engine.xml` le impostazioni di configurazione sono state personalizzate, accertarsi di aver creato i rispettivi file delle proprietà denominati con l'ID del componente dell'oggetto affinché le personalizzazioni non vadano perse con l'upgrade. Per ulteriori informazioni, vedere ["Maintaining Custom Settings in XML Files"](#) (Conservazione delle impostazioni personalizzate nei file XML) nella [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di Sentinel NetIQ).

- 4 **Se si desidera eseguire l'upgrade dell'applicazione Sentinel**, fare clic su **Applicazione** per avviare WebYaST.
- 5 **Se si desidera eseguire l'upgrade di un'istanza di Gestione servizi di raccolta o del motore di correlazione**, specificare l'URL del relativo computer utilizzando la porta 4984 per avviare WebYaST immettendo `https://<indirizzo_IP>:4984`, dove <indirizzo\_IP> è l'indirizzo IP dell'istanza di Gestione servizi di raccolta o del motore di correlazione. Completare [Passo 7](#) mediante [Passo 10](#).
- 6 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 [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel).
- 7 (Condizionale) Se non è già stato fatto, registrare l'applicazione per l'esecuzione automatica degli aggiornamenti.  
Per ulteriori informazioni, vedere il [Sezione 13.3.3, “Registrazione degli aggiornamenti”](#), a [pagina 86](#).  
Se l'applicazione non è registrata, in Sentinel viene visualizzato un avviso di colore giallo che indica tale stato.
- 8 Per verificare se vi sono aggiornamenti disponibili, fare clic su **Aggiorna**.  
Gli aggiornamenti disponibili vengono visualizzati.
- 9 Selezionare e applicare gli aggiornamenti.  
Il completamento degli aggiornamenti potrebbe richiedere alcuni minuti. Una volta completato l'aggiornamento, viene visualizzata la pagina di login di WebYaST.  
Prima di eseguire l'upgrade dell'applicazione, WebYaST interrompe automaticamente il servizio Sentinel. Una volta completato l'upgrade, questo servizio deve essere riavviato manualmente.
- 10 Riavviare il servizio Sentinel mediante l'interfaccia Web.  
Per ulteriori informazioni, vedere il [Sezione 13.4, “Interruzione e avvio del server mediante WebYaST”](#), a [pagina 87](#).
- 11 Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.
- 12 Svuotare la cache di Java Web Start nei computer client, affinché venga utilizzata la versione più recente delle applicazioni Sentinel.  
Per svuotare la cache di Java Web Start è possibile utilizzare il comando `avaws -clearcache` o Java Control Center. Per ulteriori informazioni, vedere [http://www.java.com/en/download/help/plugin\\_cache.xml](http://www.java.com/en/download/help/plugin_cache.xml).
- 13 (Condizionale) Nel caso in cui sia stato eseguito un upgrade sostanziale del database PostgreSQL (ad esempio da 8.0 a 9.0 o da 9.0 a 9.1) eliminare i file della versione precedente dal database PostgreSQL. Per informazioni sull'esecuzione dell'upgrade del database PostgreSQL, vedere le note di rilascio di Sentinel.
  - 13a Passare all'utente Novell.  

```
su novell
```
  - 13b Passare alla cartella bin:  

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```
  - 13c Cancellare i vecchi file PostgreSQL utilizzando il comando seguente:  

```
./delete_old_cluster.sh
```

- 14** (Condizionale) In caso di upgrade da Sentinel 7.1.1 o versioni precedenti, il programma di installazione non esegue la migrazione dei dati di security intelligence (SI) di default. Per eseguire la migrazione dei dati SI da Sentinel 7.1.1 o versioni precedenti, abilitarla manualmente come segue:

**14a** Passare all'utente Novell:

```
su novell
```

**14b** Aprire il file `/etc/opt/novell/sentinel/config/server.xml`.

**14c** Nella sezione `BaseliningRuntime` del componente aggiungere la proprietà seguente:

```
<property name="baselining.migration.check">true</property>
```

**14d** Riavviare il server Sentinel.

## 25.3 Esecuzione dell'upgrade dell'applicazione mediante SMT

Negli ambienti protetti in cui l'applicazione deve essere eseguita senza un accesso diretto a Internet, è possibile configurarla con Subscription Management Tool (SMT), che consente di eseguire l'upgrade alle versioni più recenti disponibili.

- 1 Assicurarsi che l'applicazione sia configurata con SMT.

Per ulteriori informazioni, vedere il [Sezione 13.3.4, "Configurazione dell'applicazione con SMT"](#), a pagina 86.

- 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 [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel 7.0.1).
- 3 (Condizionale) Se nei file `server.xml`, `collector_mgr.xml` o `correlation_engine.xml` le impostazioni di configurazione sono state personalizzate, accertarsi di aver creato i rispettivi file delle proprietà denominati con l'ID del componente dell'oggetto affinché le personalizzazioni non vadano perse con l'upgrade. Per ulteriori informazioni, vedere ["Maintaining Custom Settings in XML Files"](#) (Conservazione delle impostazioni personalizzate nei file XML) nella [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di Sentinel NetIQ).
- 4 Eseguire il login alla console dell'applicazione come utente `root`.
- 5 Aggiornare l'archivio per l'upgrade:

```
zypper ref -s
```

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

```
zypper lr
```

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

```
zypper lu
```

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

```
zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
```

- 9 Aggiornare l'applicazione:

```
zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
```

**10** Riavviare l'applicazione.

```
rcsentinel restart
```



---

# 26 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 Installazione di Sentinel per alta disponibilità

In questa appendice si descrive come installare NetIQ 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 dell'utente, rivolgersi al supporto NetIQ.

---

**Nota:** la configurazione per alta disponibilità è supportata solo nel server Sentinel. Le istanze di Gestione servizi di raccolta e del motore di correlazione possono comunque comunicare con il server Sentinel ad alta disponibilità.

---

- ♦ [Capitolo 27, "Concetti", a pagina 141](#)
- ♦ [Capitolo 28, "Requisiti di sistema", a pagina 145](#)
- ♦ [Capitolo 29, "Installazione e configurazione", a pagina 147](#)
- ♦ [Capitolo 30, "Upgrade di Sentinel in configurazione ad alta disponibilità", a pagina 161](#)
- ♦ [Capitolo 31, "backup e recupero d'emergenza", a pagina 167](#)



---

# 27 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.

- ♦ [Sezione 27.1, "Sistemi esterni", a pagina 141](#)
- ♦ [Sezione 27.2, "Memorizzazione condivisa", a pagina 141](#)
- ♦ [Sezione 27.3, "Monitoraggio dei servizi", a pagina 142](#)
- ♦ [Sezione 27.4, "Fencing", a pagina 142](#)

## 27.1 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 avvisi in qualsiasi nodo del cluster (in questo caso Sentinel deve essere configurato con un IP virtuale).

## 27.2 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.

---

**Nota:** 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.

---

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.

## 27.3 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.

## 27.4 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.



# 28 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:
  - ♦ Il sistema operativo SUSE Linux Enterprise Server (SLES) 11 SP3
  - ♦ Il pacchetto SUSE Linux Enterprise Server 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 siano disponibili il programma di installazione di Sentinel (file TAR) e l'immagine ISO di SUSE Linux High Availability Extension (SLE HAE) con licenze valide.
- (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:

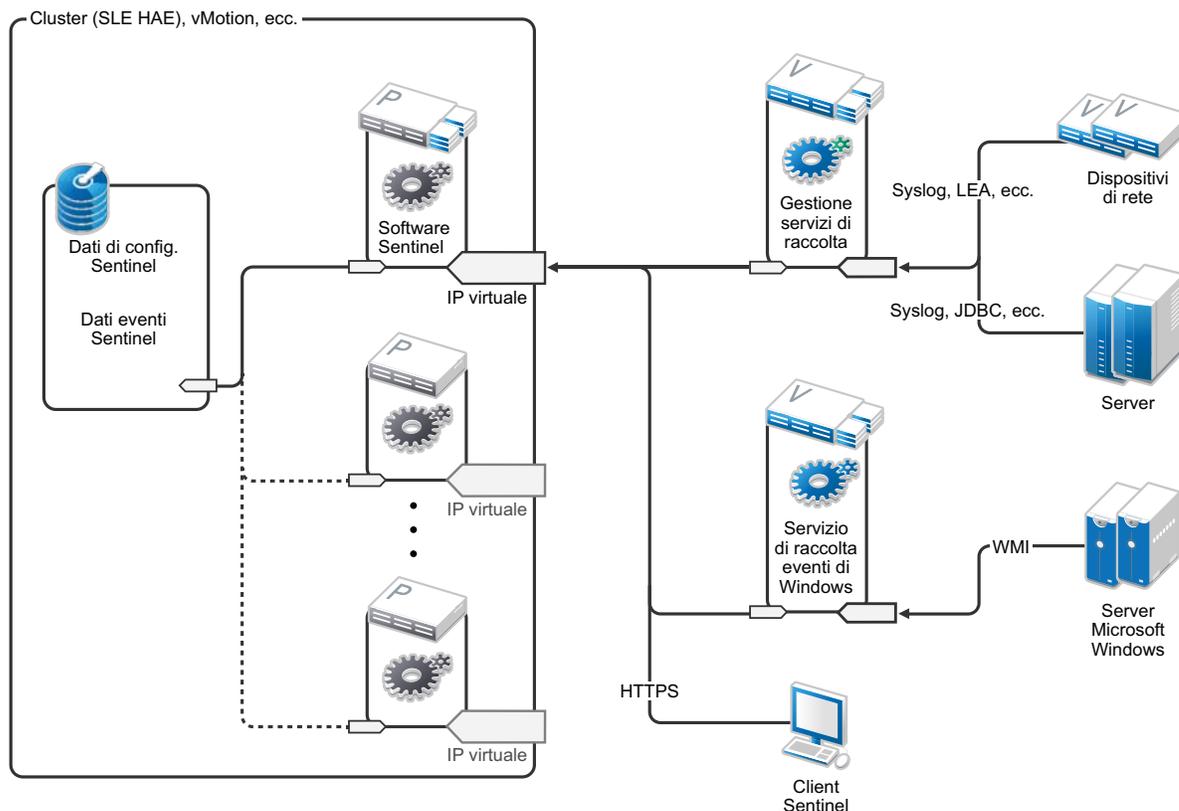
```
/sbin/modprobe -v --ignore-install <watchdog driver name>
```
- Accertarsi che i nodi del cluster in cui risiedono i servizi Sentinel siano conformi ai requisiti specificati nel [Capitolo 5, "Requisiti di sistema", a pagina 37](#).
- Memorizzazione condivisa sufficiente per i dati di Sentinel e per 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](#). NetIQ consiglia di utilizzare una macchina virtuale SUSE Linux standard configurata con le destinazioni iSCSI come memorizzazione condivisa.
- 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. NetIQ consiglia di utilizzare due macchine virtuali SUSE Linux.
- 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. NetIQ consiglia di utilizzare un indirizzo IP dedicato per eseguire la connessione alla destinazione iSCSI.

- ❑ Accertarsi di disporre di un 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. NetIQ consiglia un semplice indirizzo IP unicast, ma per gli ambienti di produzione è preferibile il multicast.

# 29 Installazione e configurazione

In questa sezione 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:



- ♦ [Sezione 29.1, "Configurazione iniziale", a pagina 148](#)
- ♦ [Sezione 29.2, "Configurazione della memorizzazione condivisa", a pagina 149](#)
- ♦ [Sezione 29.3, "Installazione di Sentinel", a pagina 152](#)
- ♦ [Sezione 29.4, "Installazione del cluster", a pagina 155](#)
- ♦ [Sezione 29.5, "Configurazione del cluster", a pagina 155](#)
- ♦ [Sezione 29.6, "Configurazione delle risorse", a pagina 158](#)
- ♦ [Sezione 29.7, "Configurazione della memorizzazione secondaria", a pagina 159](#)

## 29.1 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
<input type="checkbox"/>	Le caratteristiche di CPU, RAM e spazio su disco di ciascun nodo del cluster devono essere conformi ai requisiti di sistema indicati nel <a href="#">Capitolo 5, "Requisiti di sistema"</a> , a pagina 37 e basati sulla frequenza eventi prevista.
<input type="checkbox"/>	Le caratteristiche di spazio su disco e I/O per i nodi di memorizzazione devono essere conformi ai requisiti di sistema indicati nel <a href="#">Capitolo 5, "Requisiti di sistema"</a> , a pagina 37 e basati sulla frequenza eventi prevista e sulle policy di conservazione dei dati per la memorizzazione primaria e/o secondaria.
<input type="checkbox"/>	Se si desidera configurare i firewall del sistema operativo affinché limitino l'accesso a Sentinel e al cluster, vedere il <a href="#">Capitolo 8, "Porte utilizzate"</a> , a pagina 55, 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.
<input type="checkbox"/>	Accertarsi che l'orario di tutti i nodi del cluster sia sincronizzato. A tale scopo è possibile utilizzare NTP o una tecnologia analoga.
<input type="checkbox"/>	<ul style="list-style-type: none"><li>◆ 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 <code>/etc/hosts</code>.</li><li>◆ Accertarsi di non aver assegnato un nome host a un indirizzo IP di loopback.</li><li>◆ Quando si configurano il nome host e il nome di dominio durante l'installazione del sistema operativo, deselezionare <b>Assegnare il nome host all'IP di loopback</b>.</li></ul>

**NetIQ consiglia di utilizzare la configurazione seguente:**

- ◆ **(Condizionale) Per le installazioni tradizionali ad alta disponibilità:**
  - ◆ Due macchine virtuali SUSE Linux 11 SP3 come nodi cluster.
  - ◆ (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 le 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 [Sezione 13.1.2, "Installazione di Sentinel"](#), a pagina 80.
- ◆ 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 SUSE Linux e SLE HAE, nonché i requisiti dell'applicazione Sentinel.

- ♦ Una macchina virtuale SUSE Linux 11 SP3 configurata con destinazioni iSCSI 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 SUSE Linux, 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).

---

## 29.2 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.

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:** NetIQ consiglia di configurare la memorizzazione condivisa e di provarne il montaggio 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 che risiedono in una macchina virtuale SUSE Linux, NetIQ consiglia di utilizzare la procedura seguente:**

- 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 delle dimensioni desiderate per la memorizzazione primaria di Sentinel, utilizzare il comando `dd`:

```
dd if=/dev/zero of=/localdata count=10240000 bs=1024
```
- 3 Creare un file di 10 GB contenente gli zeri copiati dal file `/dev/zero` pseudo-device. Per i dettagli relativi alle opzioni della riga di comando, vedere le informazioni o la pagina principale del comando `dd`.

- 4 Per creare un file per la memorizzazione secondaria, ripetere i passaggi da 1 a 3:

```
dd if=/dev/zero of=/networkdata count=10240000 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.

---

## 29.2.1 Configurazione delle destinazioni iSCSI

Configurare i file `localdata` e `networkdata` come 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 **Indirizzo**, assegnare l'indirizzo IP statico 10.0.0.3, che sarà l'IP per le comunicazioni iSCSI interne.
- 6 Fare clic su **Avanti** e successivamente su **OK**.
- 7 Nella schermata principale, selezionare **Servizi di rete > Destinazione iSCSI**.
- 8 Se richiesto, installare il software necessario `iscsitarget RPM` dal supporto di SUSE Linux 11 SP3.
- 9 Fare clic su **Servizio** e selezionare l'opzione **In avvio** affinché il servizio venga avviato quando si avvia il sistema operativo.
- 10 Fare clic su **Globale** e selezionare **Nessuna autenticazione** perché il Resource Agent OCF attuale per iSCSI non supporta l'autenticazione.
- 11 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.
- 12 Fare clic su **Aggiungi** per aggiungere un nuovo LUN.
- 13 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`.
- 14 Ripetere i passaggi 12 e 13, ma questa volta aggiungere LUN 1 e `/networkdata`.
- 15 Non modificare i valori di default delle altre opzioni. Fare clic su **OK** e successivamente su **Avanti**.
- 16 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.
- 17 Uscire da YaST.

---

**Nota:** mediante la procedura vengono espone 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.

---

## 29.2.2 Configurazione degli iniziatori iSCSI

Per formattare i dispositivi, utilizzare la procedura seguente:

- 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 **Indirizzo** e assegnare l'indirizzo IP statico 10.0.0.1, che sarà l'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 (open-iscsi RPM) dal supporto di SUSE Linux 11 SP3.
- 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), selezionare **Nessuna autenticazione** e fare clic su **Avanti**.
- 12 Selezionare la destinazione iSCSI rilevata con indirizzo IP 10.0.0.3 e successivamente **Login**.
- 13 Passare alla modalità automatica nel menu a discesa **Avvio** e selezionare **Nessuna autenticazione**, quindi 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 Vista sistema dovrebbero apparire nell'elenco i nuovi dischi rigidi (ad esempio `/dev/sdb` e `/dev/sdc`); saranno di tipo IET-VIRTUAL-DISK. 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 ext3 primaria, ma non montarlo. Verificare che l'opzione Non montare la partizione sia selezionata.
- 19 Selezionare **Avanti** e, dopo aver verificato le modifiche che verranno apportate, fare clic su **Fine**. Presumendo che si crei una sola partizione di grandi dimensioni in questo LUN iSCSI, è necessario terminare la configurazione con un disco `/dev/sdb1` o simile formattato (di seguito definito `/dev/<SHARED1>`).
- 20 Tornare a Partizionatore e ripetere la procedura di creazione delle partizioni/formattazione (passaggi da 16 a 19) per `/dev/sdc` o qualsiasi altro dispositivo di blocco utilizzato per la memorizzazione secondaria. Si dovrebbe così ottenere una partizione `/dev/sdc1` o un disco formattato simile (di seguito definito `/dev/<NETWORK1>`).
- 21 Uscire da YaST.
- 22 **(Condizionale) Se si esegue un'installazione tradizionale ad alta disponibilità**, creare un punto di montaggio e testare 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'IP del nodo con un diverso 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 5 sostituire l'IP del nodo con un diverso IP per ciascun nodo del cluster.

## 29.3 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.

NetIQ consiglia di 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.

### 29.3.1 Installazione nel primo nodo

- ♦ [“Installazione tradizionale ad alta disponibilità” a pagina 152](#)
- ♦ [“Installazione dell'applicazione Sentinel ad alta disponibilità” a pagina 153](#)

#### 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 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
```

- 4 Eseguire l'installazione standard configurando il prodotto secondo necessità. Mediante il programma di installazione vengono installati i file binari, i database e i file di configurazione. Il programma di installazione consente inoltre d'impostare le credenziali di login, le impostazioni di configurazione e le porte di rete.
- 5 Avviare Sentinel e provare le funzioni di base. Per accedere al prodotto è possibile utilizzare l'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 Specificare l'opzione per la selezione del tipo di configurazione di Sentinel.

- 3c Per immettere una nuova password, specificare 2.

Se si specifica 1, la password non viene memorizzata nel file `install.props`.

- 4 Chiudere Sentinel utilizzando il comando seguente:

```
rcsentinel stop
```

Con questa operazione si rimuovono gli script di avvio automatico, affinché il cluster possa gestire il prodotto.

```
insserv -r sentinel
```

- 5 Spostare la cartella dei dati di Sentinel nella memorizzazione condivisa utilizzando i comandi seguenti. Grazie a questo spostamento i nodi potranno utilizzare la cartella dei dati di Sentinel mediante la memorizzazione condivisa.

```
mkdir -p /tmp/new
mount /dev/<SHARED1> /tmp/new
mv /var/opt/novell/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/  
umount /var/opt/novell/
```

## 29.3.2 Installazione in nodi successivi

- ♦ [“Installazione tradizionale ad alta disponibilità” a pagina 154](#)
- ♦ [“Installazione dell'applicazione Sentinel ad alta disponibilità” a pagina 154](#)

Ripetere l'installazione 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'installazione. 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'installazione). 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  
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props  
cd /  
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.

## 29.4 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 SUSE Linux High Availability Extension con un overlay di componenti Resource Agent specifici di Sentinel, NetIQ consiglia di 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
```

## 29.5 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).

**Per la configurazione dei cluster NetIQ consiglia di 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 SUSE Linux 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, utilizzare il comando `dd`:  

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```
- 2 Creare un file di 1 MB contenente gli zeri copiati dal file `/dev/zero` pseudo-device.
- 3 Eseguire YaST dalla riga di comando o l'interfaccia grafica: `/sbin/yast`
- 4 Selezionare **Servizi di rete > Destinazione iSCSI**.
- 5 Fare clic su **Destinazioni** e selezionare la destinazione esistente.
- 6 Selezionare **Modifica**. L'interfaccia utente visualizzerà un elenco di LUN (unità) disponibili.
- 7 Selezionare **Aggiungi** per aggiungere un nuovo LUN.
- 8 Non modificare il numero 2 dei LUN. Spostarsi nella finestra di dialogo **Percorso** e selezionare il file `/sbd` che è stato creato.
- 9 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.
- 10 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 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 **Destinazioni rilevate**, selezionare la **destinazione** e ripetere il login per aggiornare l'elenco dei dispositivi (lasciare l'opzione di avvio impostata su **Automatico** e **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 Eseguire il comando `sleha-init`.
- 11 Quando viene richiesto l'indirizzo di rete per l'associazione, specificare l'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 il percorso utilizzare il tasto TAB).
- 14 Completare la procedura guidata e verificare che non vengano segnalati errori.
- 15 Avviare YaST.
- 16 Selezionare **Elevata disponibilità > Cluster** (o solo Cluster in alcuni sistemi).
- 17 Nella casella sulla sinistra, verificare che l'opzione **Canali di comunicazione** sia selezionata.
- 18 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).
- 19 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).
- 20 Per completare la configurazione, selezionare **Fine**.
- 21 Uscire da YaST.
- 22 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 **Destinazioni rilevate**, selezionare la **destinazione** e ripetere il login per aggiornare l'elenco dei dispositivi (lasciare l'opzione di avvio impostata su **Automatico e Nessuna autenticazione**).
- 6 Selezionare **OK** e uscire dallo strumento per l'iniziatore iSCSI.
- 7 Eseguire il comando seguente: `sleha-join`.
- 8 Immettere l'indirizzo IP del primo nodo del cluster.

(Condizionale) Se il cluster non si avvia correttamente, eseguire le operazioni seguenti:

- 1 Copiare manualmente `/etc/corosync/corosync.conf` da node01 a node02 o eseguire `csync2 -x -v` in node01, oppure configurare manualmente il cluster in node02 mediante YaST.
- 2 Eseguire il comando `/etc/rc.d/openais start` in node02.

(Condizionale) Se il servizio `xinetd` non aggiunge correttamente il nuovo servizio `csync2`, lo script non funzionerà correttamente. Il servizio `xinetd` è necessario affinché l'altro nodo possa eseguire la sincronizzazione dei file di configurazione del cluster fino a questo nodo. Se si rilevano errori del tipo `csync2 run failed`, potrebbe essersi verificato questo problema.

Per risolvere il problema, eseguire il comando `kill -HUP `cat /var/run/xinetd.init.pid`` e avviare nuovamente lo script `sleha-join`.

- 3 Eseguire `crm_mon` in ciascun nodo per verificare che il cluster funzioni correttamente. Per verificare il cluster è inoltre possibile utilizzare la console Web 'hawk'. Il nome di login di default è `hacluster` e la password `linux`.

(Condizionale) A seconda dell'ambiente dell'utente, eseguire le operazioni seguenti per modificare ulteriori parametri:

- 1 Affinché un errore in un solo nodo di un cluster comprendente due nodi non interrompa improvvisamente tutto il cluster, impostare l'opzione globale `no-quorum-policy` su `ignore`:

```
crm configure property no-quorum-policy=ignore
```

---

**Nota:** se nel cluster sono presenti più di due nodi, non impostare questa opzione.

---

- 2 Affinché la gestione delle risorse ne consenta l'esecuzione e lo spostamento, impostare l'opzione globale del cluster `default-resource-stickiness` su 1:

```
crm configure property default-resource-stickiness=1.
```

## 29.6 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'IP virtuale utilizzato per l'accesso ai servizi.
- ♦ Il database PostgreSQL in cui vengono memorizzati i metadati delle configurazioni e degli eventi.

**NetIQ consiglia di utilizzare la procedura seguente per la configurazione delle risorse:**

NetIQ fornisce uno script `crm` che 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 che compaiono nel cluster; in questo caso eseguire `/etc/rc.d/openais restart` in `node02`.

- 4 Lo script `install-resources.sh` richiederà un paio di valori, più precisamente l'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'installazione in modalità automatica (/tmp/install.props) creato durante l'installazione di Sentinel deve essere presente. Non è necessario eseguire questo script in altri nodi oltre a quello installato per primo, in quanto tutti i file relativi alla configurazione verranno sincronizzati automaticamente con gli altri nodi.

- 5 Se l'ambiente del cliente è diverso da quello della soluzione consigliata da NetIQ, è possibile modificare il file `resources.cli` (nella stessa directory) e cambiare le definizioni originarie dalla stessa ubicazione. Ad esempio, la soluzione consigliata utilizza una semplice risorsa del file system, ma è possibile utilizzare anche una risorsa cLVM maggiormente capace di riconoscere il cluster.
- 6 Dopo aver eseguito lo script di shell, è possibile inviare un comando `crm status` e il risultato dovrebbe essere analogo a quello riportato di seguito:

```
crm status
```

---

```
Last updated: Thu Jul 26 16:34:34 2012
Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
Stack: openais
Current DC: node01 - partition with quorum
Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
2 Nodes configured, 2 expected votes
5 Resources configured.
```

---

```
Online: [ node01, node02 ]
stonith-sbd (stonith:external/sbd): Started node01
Resource Group: sentinelgrp
  sentinelip (ocf::heartbeat:IPaddr2): Started node01
  sentinelfs (ocf::heartbeat:Filesystem): Started node01
  sentineldb (ocf::novell:pgsql): Started node01
  sentinelserver (ocf::novell:sentinel): Started node01
```

- 7 A questo punto è necessario configurare nel cluster le risorse per Sentinel. È possibile analizzare come vengono configurate e raggruppate nello strumento di gestione del cluster, ad esempio eseguendo un comando di stato `crm`.

## 29.7 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 Nella console Web 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.

NetIQ consiglia di utilizzare una semplice destinazione iSCSI 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:** poiché NetIQ consiglia di utilizzare una destinazione iSCSI per questa soluzione, la destinazione verrà montata come directory da utilizzare per la 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 la console Web 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 sentinelifs 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 Web 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`.

NetIQ consiglia di utilizzare versioni semplici delle risorse necessarie, quali ad esempio il semplice Resource Agent del file system; i clienti possono scegliere anche risorse di cluster più sofisticate, come ad esempio cLVM (una versione del file system con volume logico).

---

# 30 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.

- ♦ Sezione 30.1, "Prerequisiti", a pagina 161
- ♦ Sezione 30.2, "Esecuzione dell'upgrade di un'installazione tradizionale ad alta disponibilità di Sentinel", a pagina 161
- ♦ Sezione 30.3, "Esecuzione dell'upgrade di un'installazione in modalità applicazione ad alta disponibilità di Sentinel", a pagina 163

## 30.1 Prerequisiti

- ♦ Effettuare il download della versione più recente del programma di installazione dal [sito Web dei download di NetIQ](#).
- ♦ 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. 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>
```

## 30.2 Esecuzione dell'upgrade di un'installazione tradizionale ad alta disponibilità di Sentinel

- 1 Abilitare la modalità di manutenzione nel cluster:

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

La modalità di manutenzione facilita l'eliminazione di eventuali disturbi sulle risorse del cluster in esecuzione mentre si esegue l'aggiornamento di Sentinel. Il comando seguente può essere eseguito da uno qualsiasi dei nodi del cluster.

- 2 Verificare che la modalità di manutenzione sia attiva:

```
crm status
```

Le risorse del cluster devono apparire nello stato non gestito.

- 3 Upgrade del nodo passivo del cluster:

- 3a** Arrestare lo stack del cluster:

```
rcopenais stop
```

Arrestando lo stack del cluster le risorse rimangono accessibili e si evitano isolamenti dei nodi.

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

**3c** Estrarre i file di installazione dal file `.tar`:

```
tar xfz <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:

```
rcopenais start
```

Ripetere il passaggio 3 per tutti i nodi passivi del cluster.

**3f** Rimuovere gli script di avvio automatico affinché il cluster possa gestire il prodotto.

```
cd /
```

```
insserv -r sentinel
```

**4** Upgrade del nodo attivo del cluster:

**4a** eseguire il backup della configurazione, quindi creare un'esportazione ESM.

Per ulteriori informazioni, vedere [“Backing Up and Restoring Data”](#) (Backup e ripristino dati) nella *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.1)

.

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

```
rcopenais stop
```

Arrestando lo stack del cluster le risorse rimangono accessibili e si evitano isolamenti dei nodi.

**4c** Effettuare il login come utente `root` al server in cui si desidera eseguire l'upgrade di Sentinel.

**4d** Per estrarre i file di installazione dal file `.tar`, eseguire il comando seguente:

```
tar xfz <install_filename>
```

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

```
./install-sentinel
```

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

```
rcopenais start
```

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

```
cd /
```

```
insserv -r sentinel
```

**4h** Per sincronizzare eventuali modifiche apportate ai file di configurazione, eseguire il comando seguente:

```
run 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
```

## 30.3 Esecuzione dell'upgrade di un'installazione in modalità applicazione ad alta disponibilità di Sentinel

È possibile eseguire l'upgrade di un'installazione dell'applicazione Sentinel ad alta disponibilità utilizzando la patch Zypper o WebYaST.

- ♦ [Sezione 30.3.1, "Esecuzione dell'upgrade dell'applicazione Sentinel ad alta disponibilità mediante Zypper"](#), a pagina 163
- ♦ [Sezione 30.3.2, "Esecuzione dell'upgrade dell'applicazione Sentinel ad alta disponibilità mediante WebYaST"](#), a pagina 165

### 30.3.1 Esecuzione dell'upgrade dell'applicazione Sentinel ad alta disponibilità mediante Zypper

Prima di eseguire l'upgrade è necessario registrare tutti i nodi dell'applicazione mediante WebYast. Per ulteriori informazioni, vedere la [Sezione 13.3.3, "Registrazione degli aggiornamenti"](#), a pagina 86. 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 Effettuare il download degli aggiornamenti per l'applicazione Sentinel ad alta disponibilità.

```
zypper -v patch -d
```

Questo comando esegue il download degli aggiornamenti per i pacchetti installati nell'applicazione (Sentinel incluso) in `/var/cache/zypp/packages`.

- 3b Arrestare lo stack del cluster.

```
rcopenais stop
```

Arrestando lo stack del cluster le risorse rimangono accessibili e si evitano isolamenti dei nodi.

- 3c** Dopo aver effettuato il download degli aggiornamenti, installarli utilizzando il comando seguente:

```
rpm -Uvh /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/rpm/
noarch/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/
rpm/x86_64/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-
Updates/rpm/i586/*.rpm --excludepath=/var/opt/novell/
```

- 3d** Per completare la procedura di upgrade, eseguire lo script seguente:

```
/var/adm/update-scripts/sentinel_server_ha_x86_64-update-<version>-
overlay_files.sh
```

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

```
rcopenais start
```

Ripetere il passaggio 3 per tutti i nodi passivi del cluster.

- 4** Upgrade del nodo attivo del cluster:

- 4a** 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 *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel).

- 4b** Arrestare lo stack del cluster.

```
rcopenais stop
```

Arrestando lo stack del cluster le risorse rimangono accessibili e si evitano isolamenti dei nodi.

- 4c** Eseguire il login all'applicazione Sentinel come amministratore.

- 4d** Per eseguire l'upgrade dell'applicazione Sentinel, fare clic su **Applicazione** per avviare WebYaST.

- 4e** Per verificare se vi sono aggiornamenti disponibili, fare clic su **Aggiorna**.

- 4f** Selezionare e applicare gli aggiornamenti.

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

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

- 4g** Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.

- 4h** Al termine dell'upgrade, riavviare lo stack del cluster.

```
rcopenais start
```

- 4i** Per sincronizzare eventuali modifiche apportate ai file di configurazione, eseguire il comando seguente:

```
run 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
```

## 30.3.2 Esecuzione dell'upgrade dell'applicazione Sentinel ad alta disponibilità mediante WebYaST

Prima di eseguire l'upgrade è necessario registrare tutti i nodi dell'applicazione mediante WebYast. Per ulteriori informazioni, vedere la [Sezione 13.3.3, "Registrazione degli aggiornamenti"](#), a pagina 86. 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 Eseguire l'upgrade dei nodi passivi del cluster:

- 3a Arrestare lo stack del cluster.

```
rcopenais stop
```

Arrestando lo stack del cluster le risorse rimangono accessibili e si evitano isolamenti dei nodi.

- 3b Specificare l'URL del nodo passivo del cluster utilizzando la porta 4984 per avviare WebYaST immettendo `https://<indirizzo_IP>:4984`, dove `<indirizzo_IP>` è l'indirizzo IP del nodo passivo del cluster. Eseguire il login all'applicazione Sentinel come amministratore.

- 3c Per verificare se vi sono aggiornamenti disponibili, fare clic su **Aggiorna**.

- 3d Selezionare e applicare gli aggiornamenti.

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

- 3e Al termine dell'upgrade, riavviare lo stack del cluster.

```
rcopenais start
```

Ripetere il [Passo 4](#) per tutti i nodi passivi del cluster.

- 4 Upgrade del nodo attivo del cluster:

- 4a 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 [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel).

- 4b Arrestare lo stack del cluster.

```
rcopenais stop
```

Arrestando lo stack del cluster le risorse rimangono accessibili e si evitano isolamenti dei nodi.

- 4c** Eseguire il login all'applicazione Sentinel come amministratore.
- 4d** Per eseguire l'upgrade dell'applicazione Sentinel, fare clic su **Applicazione** per avviare WebYaST.
- 4e** Per verificare se vi sono aggiornamenti disponibili, fare clic su **Aggiorna**.
- 4f** Selezionare e applicare gli aggiornamenti.  
Il completamento degli aggiornamenti potrebbe richiedere alcuni minuti. Una volta completato l'aggiornamento, viene visualizzata la pagina di login di WebYaST.  
Prima di eseguire l'upgrade dell'applicazione, WebYaST interrompe automaticamente il servizio Sentinel. Una volta completato l'upgrade, questo servizio deve essere riavviato manualmente.
- 4g** Svuotare la cache del browser Web per visualizzare l'ultima versione di Sentinel.
- 4h** Al termine dell'upgrade, riavviare lo stack del cluster.

```
rcopenais start
```

- 4i** Per sincronizzare eventuali modifiche apportate ai file di configurazione, eseguire il comando seguente:

```
run 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
```

---

# 31 backup e recupero d'emergenza

Il cluster di failover ad alta disponibilità descritto nel presente documento offre un livello di 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.

- ♦ [Sezione 31.1, “Backup”, a pagina 167](#)
- ♦ [Sezione 31.2, “PlateSpin”, a pagina 167](#)

## 31.1 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 *NetIQ Sentinel Administration Guide* (Guida all'amministrazione di NetIQ Sentinel 7.1) si descrive come utilizzare gli strumenti integrati di Sentinel per eseguire il backup. Tali strumenti devono essere utilizzati nel nodo attivo del cluster, poiché il nodo passivo non disporrà dell'accesso necessario al dispositivo di memorizzazione condivisa. È possibile utilizzare anche altri strumenti di backup reperibili in commercio, ma potrebbero avere requisiti diversi per quanto riguarda il nodo in cui possono essere utilizzati.

## 31.2 PlateSpin

- ♦ [Sezione 31.2.1, “Errore temporaneo”, a pagina 167](#)
- ♦ [Sezione 31.2.2, “Danneggiamento dei nodi”, a pagina 167](#)
- ♦ [Sezione 31.2.3, “Configurazione dei dati del cluster”, a pagina 168](#)

### 31.2.1 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.

### 31.2.2 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.

### 31.2.3 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 [NetIQ Sentinel Administration Guide](#) (Guida all'amministrazione di NetIQ Sentinel 7.1) si descrive come utilizzare gli strumenti integrati di Sentinel per eseguire il ripristino di un backup. Tali strumenti devono essere utilizzati nel nodo attivo del cluster, poiché il nodo passivo non disporrà dell'accesso necessario al dispositivo di memorizzazione condivisa. È possibile utilizzare anche altri strumenti di backup e ripristino reperibili in commercio, ma potrebbero avere requisiti diversi per quanto riguarda il nodo in cui possono essere utilizzati.

---

# VII Appendici

- ◆ [Appendice A, “Soluzione dei problemi”, a pagina 171](#)
- ◆ [Appendice B, “Disinstallazione”, a pagina 173](#)



---

# A Soluzione dei problemi

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

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

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

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.

## A.2 Non viene creato l'UUID per le Gestioni servizi di raccolta o il Motore di raccolta

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

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

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

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

## A.3 Dopo aver eseguito il login l'interfaccia Web 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**.

---

# B Disinstallazione

In questa appendice sono riportate informazioni relative alla disinstallazione di Sentinel e ai task post-disinstallazione.

- ♦ [Sezione B.1, “Elenco di controllo per la disinstallazione”, a pagina 173](#)
- ♦ [Sezione B.2, “Disinstallazione di Sentinel”, a pagina 173](#)
- ♦ [Sezione B.3, “Task successivi alla disinstallazione”, a pagina 175](#)

## B.1 Elenco di controllo per la disinstallazione

Per disinstallare Sentinel, utilizzare l'elenco di controllo seguente:

- Disinstallare il server Sentinel.
- Disinstallare eventuali istanze di Gestione servizi di raccolta e del motore di correlazione.
- Per completare la disinstallazione, eseguire i task post-disinstallazione.

## B.2 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.

---

### B.2.1 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:

```
/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.

## B.2.2 Disinstallazione di Gestione servizi di raccolta e del motore di correlazione

Per disinstallare Gestione servizi di raccolta e il motore di correlazione:

- 1 Eseguire il login come `root` al computer in cui risiede Gestione servizi di raccolta e il motore di correlazione.

---

**Nota:** se l'installazione è stata eseguita come un utente `root`, non è possibile eseguire la disinstallazione delle istanze remote di Gestione servizi di raccolta o del motore di correlazione 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 Gestione servizi di raccolta o il motore di correlazione sarà rimosso insieme a tutti i dati associati.

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

Lo script prima interrompe il servizio, quindi lo rimuove completamente. Tuttavia, l'icona di Gestione servizi di raccolta e del motore di correlazione rimane visualizzata nell'interfaccia Web nello stato inattivo.

- 5 Per eliminare manualmente Gestione servizi di raccolta e il motore di correlazione, effettuare i passaggi seguenti nell'interfaccia Web:

### **Gestione servizi di raccolta:**

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

### **Motore di correlazione:**

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

## B.2.3 Disinstallazione di Gestione servizi di raccolta NetFlow

Per disinstallare Gestione servizi di raccolta NetFlow, utilizzare la procedura seguente:

- 1 Eseguire il login al computer in cui risiede Gestione servizi di raccolta NetFlow.

---

**Nota:** Eseguire il login con la medesima autorizzazione utente utilizzata per l'installazione di Gestione servizi di raccolta NetFlow.

---

- 2 Passare alla directory seguente:

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

- 3 Eseguire il comando seguente:

```
./uninstall-sentinel
```

- 4 Per disinstallare Gestione servizi di raccolta, immettere `y`.

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

## B.3 Task successivi alla disinstallazione

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

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

Per rimuovere manualmente le impostazioni di sistema di Sentinel:

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

```
userdel -r novell
```

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