Guida all'installazione

Novell®
Sentinel 6.1 Rapid Deployment

SP2

Aprile 2011

www.novell.com

Note legali

Novell, Inc. non rilascia alcuna dichiarazione e non fornisce alcuna garanzia in merito al contenuto o all'uso di questa documentazione e in particolare non riconosce alcuna garanzia, espressa o implicita, di commerciabilità o idoneità per uno scopo specifico. Novell, Inc. si riserva inoltre il diritto di aggiornare la presente pubblicazione e di modificarne il contenuto in qualsiasi momento, senza alcun obbligo di notificare tali modifiche a qualsiasi persona fisica o giuridica.

Inoltre, Novell, Inc. non rilascia alcuna dichiarazione e non fornisce alcuna garanzia in merito a qualsiasi software e in particolare non riconosce alcuna garanzia, espressa o implicita, di commerciabilità o idoneità per uno scopo specifico. Novell, Inc. si riserva inoltre il diritto di modificare qualsiasi parte del software Novell in qualsiasi momento, senza alcun obbligo di notificare tali modifiche a qualsiasi persona fisica o giuridica.

Qualsiasi informazione tecnica o prodotto fornito in base a questo Contratto può essere soggetto ai controlli statunitensi relativi alle esportazioni e alla normativa sui marchi di fabbrica in vigore in altri paesi. L'utente si impegna a rispettare la normativa relativa al controllo delle esportazioni e a ottenere qualsiasi licenza o autorizzazione necessaria per esportare, riesportare o importare prodotti finali. L'utente si impegna inoltre a non esportare o riesportare verso entità incluse negli elenchi di esclusione delle esportazioni statunitensi o a qualsiasi paese sottoposto a embargo o che sostiene movimenti terroristici, come specificato nella legislazione statunitense in materia di esportazioni. L'utente accetta infine di non utilizzare i prodotti finali per utilizzi correlati ad armi nucleari, missilistiche o biochimiche. Per ulteriori informazioni sull'esportazione di software Novell, vedere la pagina Web sui servizi commerciali internazionali di Novell (http://www.novell.com/info/exports/). Novell non si assume alcuna responsabilità relativa al mancato ottenimento, da parte dell'utente, delle autorizzazioni di esportazione necessarie.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Documentazione online: per accedere alla documentazione online più recente relativa a questo o ad altri prodotti Novell, vedere la pagina Web della documentazione Novell (http://www.novell.com/documentation).

Marchi di fabbrica di Novell

Per informazioni sui marchi di fabbrica di Novell, vedere l'elenco di marchi di fabbrica e di servizio di Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiali di terze parti

Tutti i marchi di fabbrica di terze parti appartengono ai rispettivi proprietari.

Sommario

Informazioni sulla Guida

Questa Guida contiene l'introduzione a Novell Sentinel 6.1 Rapid Deployment Service Pack 2 e le relative procedure di installazione.

Destinatari

La presente documentazione è rivolta ai professionisti della protezione delle informazioni.

Feedback

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

Documentazione aggiuntiva

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

- *Guida all'installazione di Novell Sentinel Rapid Deployment* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html)
- *Novell Sentinel Rapid Deployment User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) (in lingua inglese)
- *Novell Sentinel Rapid Deployment Reference Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/bookinfo.html) (in lingua inglese)
- *Guida all'installazione di Novell Sentinel* (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/)
- *Novell Sentinel User Guide* (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/) (in lingua inglese)
- *Novell Sentinel Reference Guide* (http://www.novell.com/documentation/sentinel61/s61_reference/?page=/documentation/sentinel61/s61_reference/data/) (in lingua inglese)

- *Sentinel SDK* (http://www.novell.com/developer/develop_to_sentinel.html) (in lingua inglese)

  Il sito di Sentinel SDK fornisce informazioni dettagliate sullo sviluppo dei servizi di raccolta (proprietari o JavaScript) e sulle azioni correlate di JavaScript.

Come contattare Novell

- *Sito Web di Novell* (http://www.novell.com)
- *Supporto tecnico Novell* (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- *Supporto autonomo Novell* (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- *Sito per il download delle patch* (http://download.novell.com/index.jsp)
- *Supporto Novell 24 ore su 24, 7 giorni su 7* (http://www.novell.com/company/contact.html)
- *TID di Sentinel* (http://support.novell.com/products/sentinel)
- Forum di supporto della comunità di Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sito Web dei plug-in di Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html)
- Elenco notifiche e-mail: iscrizione tramite il sito Web dei plug-in di Sentinel

Panoramica sul prodotto

1

Sentinel 6.1 Rapid Deployment è una versione semplificata di Novell Sentinel che sfrutta i componenti open source PostgreSQL, activeMQ e JasperReports.

Le seguenti sezioni consentono di comprendere i componenti principali del sistema Sentinel 6.1 Rapid Deployment. Questa *Guida all'installazione di Sentinel Rapid Deployment* contiene informazioni dettagliate sulle procedure di installazione e di configurazione. La *Sentinel Rapid Deployment User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) (in lingua inglese) contiene informazioni dettagliate su architettura, operazioni e procedure amministrative.

1.1 Panoramica di Sentinel 6.1 Rapid Deployment

Sentinel è una soluzione di gestione degli eventi e delle informazioni di sicurezza che riceve le informazioni da numerose origini all'interno di un'azienda: consente di standardizzarle, assegnare loro priorità e presentarle all'utente affinché possa intraprendere le opportune azioni in base alle minacce, ai rischi e alle policy.

Sentinel automatizza processi di raccolta log, analisi e generazione di rapporti per assicurare che i controlli IT siano in grado di supportare in modo efficace i requisiti di rilevamento e controllo delle minacce. Sentinel sostituisce i processi manuali onerosi a livello di risorse umane con il monitoraggio costante e automatico degli eventi di sicurezza e conformità e dei controlli IT.

Sentinel raccoglie e correla inoltre le informazioni sulla sicurezza e di altra natura dall'infrastruttura in rete di un'organizzazione, nonché da sistemi, dispositivi e applicazioni di terze parti. Sentinel presenta i dati raccolti in un'interfaccia grafica, identifica i problemi di sicurezza o di conformità e controlla le attività di correzione allo scopo di ottimizzare i processi esposti agli errori e creare un programma di gestione più rigoroso e sicuro.

La gestione automatizzata delle risposte ai casi consente di documentare e formalizzare il processo di controllo, inoltro 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.

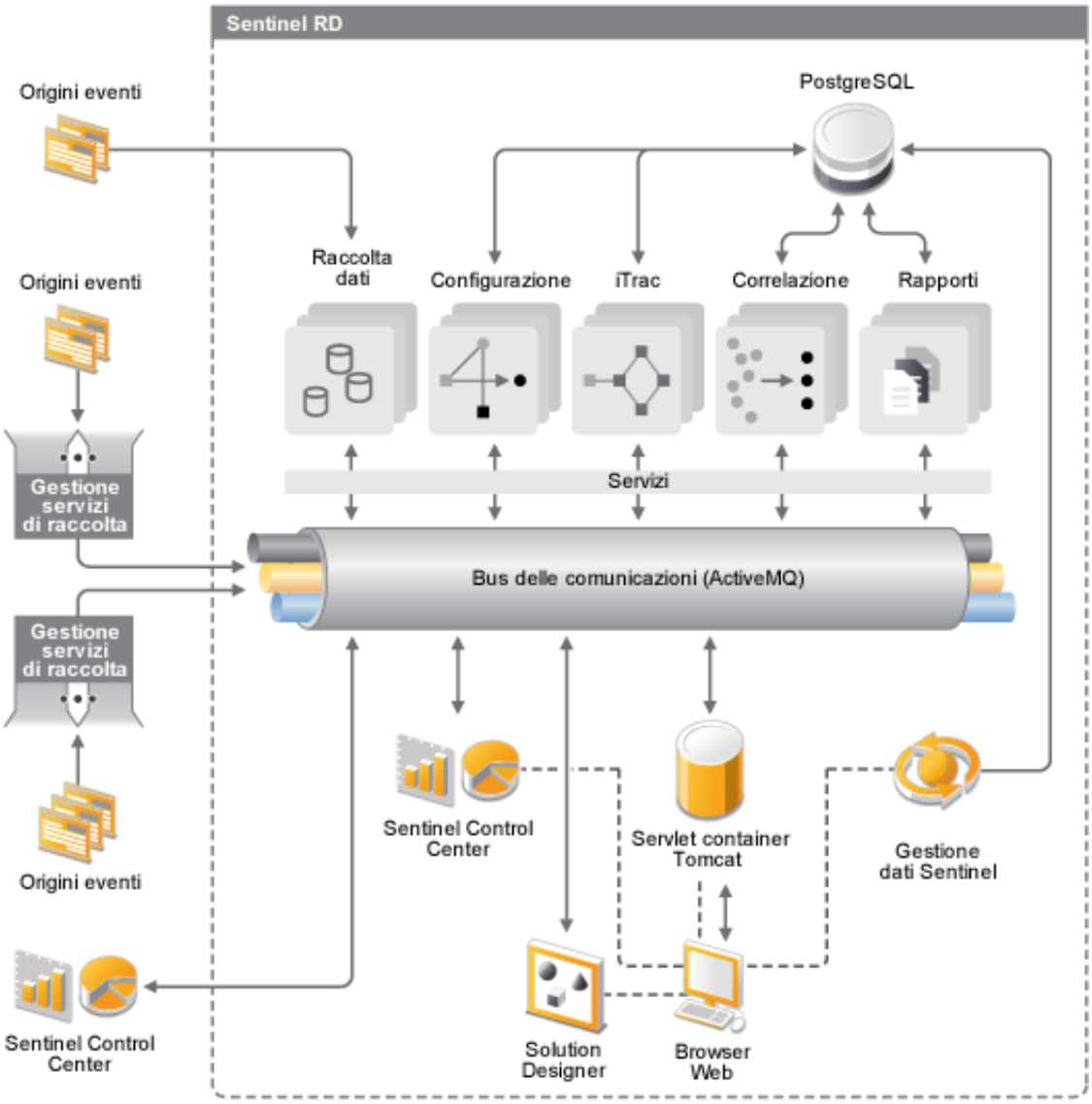
I pacchetti soluzione sono un modo semplice per distribuire e impostare le regole di correlazione di Sentinel, gli elenchi dinamici, le mappe, i rapporti e i flussi di lavoro iTRAC nei controlli. Tali controlli possono essere strutturati per soddisfare specifici requisiti normativi, ad esempio lo standard di sicurezza dei dati nel settore delle carte di pagamento, oppure possono essere correlati a una specifica origine di dati, ad esempio gli eventi di autenticazione utente per un database.

Funzioni di Sentinel Rapid Deployment:

- Monitoraggio della conformità e gestione della sicurezza in tempo reale automatizzati e integrati in tutti i sistemi e le reti.
- Framework che consente alle policy aziendali di influenzare policy e azioni del dipartimento IT.
- Documentazione e generazione automatica di rapporti sulla sicurezza, sui sistemi e sugli eventi di accesso all'interno dell'azienda.
- Gestione e dei casi e aggiornamento computer incorporati.
- Possibilità di dimostrare e monitorare la conformità con le policy interne e le normative vigenti quali Sarbanes-Oxley, HIPAA, GLBA e FISMA. Il contenuto richiesto per l'implementazione di tali controlli è distribuito e implementato mediante i pacchetti soluzione.

Nella seguente illustrazione è riportata l'architettura concettuale di Sentinel Rapid Deployment, che mostra i componenti necessari per la gestione della conformità e della sicurezza.

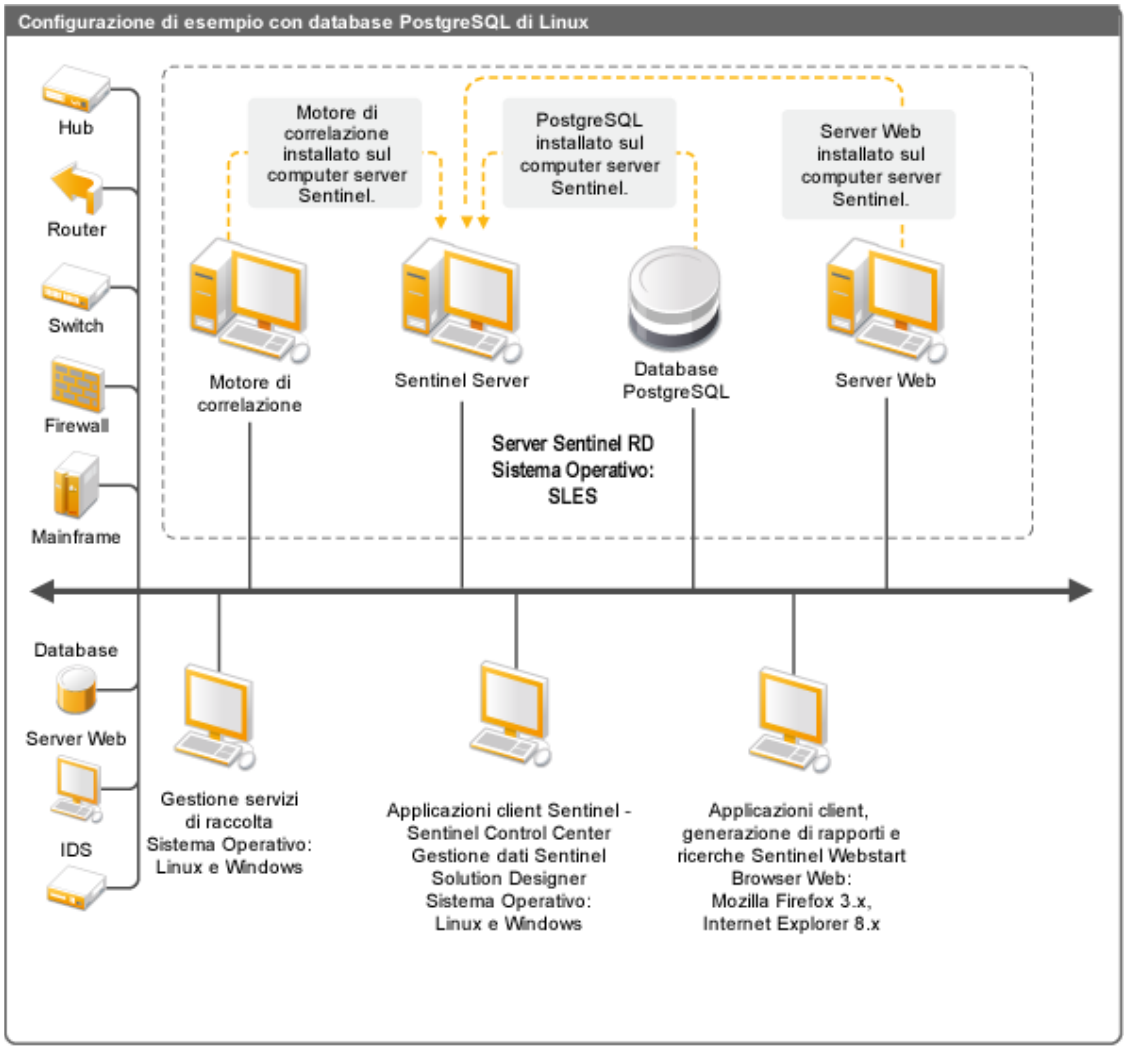
Figura 1-1 *Architettura concettuale di Sentinel*



1.2 Configurazione di Sentinel 6.1 Rapid Deployment

Nella seguente illustrazione è raffigurata la configurazione di Sentinel 6.1 Rapid Deployment.

Figura 1-2 *Configurazione di Sentinel 6.1 Rapid Deployment*



1.3 Interfacce utente di Sentinel Rapid Deployment

Sentinel include le seguenti intuitive interfacce utente:

- Interfaccia Web di Sentinel 6.1 Rapid Deployment
- Sentinel Control Center
- Gestione dati Sentinel
- Sentinel Solution Designer
- Sentinel Plug-In SDK

1.3.1 Interfaccia Web di Sentinel 6.1 Rapid Deployment

Con l'interfaccia Web di Novell Sentinel 6.1 Rapid Deployment è possibile gestire i rapporti e avviare Sentinel Control Center (SCC), Gestione dati Sentinel e Solution Designer. Dalla pagina *Applicazioni* dell'interfaccia Web di Sentinel 6.1 Rapid Deployment è anche possibile effettuare il download del programma di installazione di Gestione servizi di raccolta e del client.

Per ulteriori informazioni, vedere "Managing Sentinel Rapid Deployment Through the Web Interface" in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.3.2 Sentinel Control Center

Il modulo (SCC) offre un dashboard integrato per la gestione della sicurezza che consente agli analisti di identificare rapidamente le nuove tendenze o i nuovi attacchi, elaborare e interagire con le informazioni grafiche in tempo reale e rispondere ai casi.

È possibile avviare SCC come applicazione client o mediante Java Web Start.

Le funzioni chiave di SCC includono:

- **Visualizzazioni Active Views:** fornisce funzionalità di analisi e visualizzazione in tempo reale.
- **Analisi:** esegue e salva le interrogazioni offline.
- **Casi:** consente di creare e gestire i casi.
- **Correlazione:** consente di definire e gestire le regole di correlazione.
- **iTRAC:** consente di gestire i processi per la documentazione, l'applicazione e il controllo dei processi di risoluzione dei casi.
- **Generazione di rapporti:** fornisce la cronologia dei rapporti e delle metriche.
- **Gestione origini eventi:** consente di distribuire e monitorare il servizio di raccolta.
- **Solution Manager:** installa, implementa e verifica i contenuti del pacchetto soluzione.

Per ulteriori informazioni, vedere "Sentinel Control Center" in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.3.3 Gestione dati Sentinel

Gestione dati Sentinel consente di gestire il database di Sentinel. In Gestione dati Sentinel è possibile eseguire le seguenti operazioni:

- Controllare l'utilizzo dello spazio del database.
- Visualizzare e gestire le partizioni del database.
- Gestire gli archivi del database.
- Reimportare nel database i dati archiviati.

Per ulteriori informazioni, vedere "Sentinel Data Manager" in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.3.4 Sentinel Solution Designer

Sentinel Solution Designer viene utilizzato per creare e modificare i pacchetti soluzione, ovvero serie di pacchetti di contenuto Sentinel, ad esempio regole di correlazione, azioni, workflow iTRAC e rapporti.

Il contenuto di Sentinel è la funzionalità estesa del sistema Sentinel. Tale contenuto include le azioni, gli integratori e i plug-in di Sentinel come i servizi di raccolta, i connettori e i pacchetti soluzione che potrebbero contenere altri svariati tipi di plug-in. Questi componenti modulari vengono utilizzati per essere integrati con sistemi di terze parti, installare una soluzione di sicurezza completa basata sul controllo e fornire rimedi automatizzati per i casi rilevati.

Per ulteriori informazioni, vedere "Solution Packs " in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.3.5 Sentinel Plug-In SDK

Sentinel Plug-in SDK include librerie e codice sviluppato da Novell Engineering, nonché il modello e il codice di esempio che è possibile utilizzare per sviluppare progetti personali. Per ulteriori informazioni, vedere Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html).

1.4 Componenti del server Sentinel

Sentinel è costituito dai componenti seguenti:

1.4.1 Servizio DAS (Data Access Service)

Sentinel Data Access Service è il componente principale utilizzato per comunicare con il database di Sentinel. Il processo DAS e altri componenti del server funzionano congiuntamente per memorizzare gli eventi ricevuti da istanze di Gestione servizi di raccolta nel database, filtrare i dati, elaborare le visualizzazioni Active Views, eseguire interrogazioni del database ed elaborare i risultati e gestire task amministrativi, ad esempio l'autenticazione e l'autorizzazione utente. Per ulteriori informazioni, vedere "Data Access Service" in *Sentinel Rapid Deployment Reference Guide* (in lingua inglese).

1.4.2 Bus messaggi

Sentinel 6.1 Rapid Deployment utilizza un broker dei messaggi open source denominato Apache Active MQ. Il bus dei messaggi è in grado di spostare migliaia di pacchetti di messaggi in un secondo tra i componenti di Sentinel. L'architettura di Apache Active MQ è basata sul middleware

di messaggistica Java, che supporta le chiamate asincrone tra le applicazioni client e server. Le code di messaggi forniscono una memorizzazione temporanea quando il programma di destinazione è occupato o non connesso. Per ulteriori informazioni, vedere “Communication Server” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.4.3 Database di Sentinel

Il prodotto Sentinel è stato creato sulla base di un database backend in cui sono memorizzati gli eventi di sicurezza e tutti i metadati di Sentinel. Sentinel 6.1 Rapid Deployment supporta PostgreSQL. Gli eventi vengono memorizzati nel formato normale, insieme ai dati sulla risorsa e sulla vulnerabilità, alle informazioni sull'identità, allo stato dei casi e del workflow e a molti altri tipi di dati. Per ulteriori informazioni, vedere “Sentinel Data Manager” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.4.4 Gestione servizi di raccolta Sentinel

Gestione servizi di raccolta Sentinel 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 comprendono la trasformazione degli eventi, l'aggiunta di rilevanza aziendale agli eventi mediante tassonomia, l'applicazione di filtri globali sugli eventi, l'instradamento degli eventi e l'invio di messaggi di stato al server Sentinel. Gestione servizi di raccolta Sentinel si connette direttamente al bus dei messaggi. Per ulteriori informazioni, vedere “Collector Manager” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.4.5 Motore di correlazione

Grazie al motore di correlazione sono disponibili nuove funzioni di gestione degli eventi di sicurezza che 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 “Correlation Tab” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.4.6 iTRAC

Sentinel fornisce un sistema di gestione del workflow iTRAC per la definizione e l'automazione dei processi relativi alla risposta dei casi. I casi identificati in Sentinel, tramite una regola di correlazione o manualmente, possono essere associati a un workflow iTRAC. Per ulteriori informazioni, vedere “iTRAC Workflows” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.4.7 Advisor e Rilevamento exploit di Sentinel

Advisor di Sentinel è un servizio facoltativo di sottoscrizione ai dati che include attacchi noti, vulnerabilità e informazioni sulla correzione. Questi dati, associati alle vulnerabilità note e al rilevamento delle istruzioni in tempo reale o a informazioni sulla prevenzione dal rispettivo ambiente, consentono un rilevamento exploit proattivo e la possibilità di agire tempestivamente in caso di attacco a un sistema vulnerabile.

Per default, con Sentinel 6.1 Rapid Deployment viene installato uno snapshot dei dati di Advisor. Per ricevere gli aggiornamenti periodici dei dati di Advisor è necessaria una licenza Advisor. Per ulteriori informazioni, vedere "Advisor Usage and Maintenance" in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.4.8 Server Web

Sentinel Rapid Deployment utilizza Apache Tomcat come server Web per consentire la connessione sicura all'interfaccia Web di Sentinel Rapid Deployment.

1.5 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. Nel sito Web dei plug-in di Sentinel 6.1 (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) sono disponibili ulteriori plug-in (e aggiornamenti) di cui è possibile effettuare il download.

Per effettuare il download di alcuni plug-in, come Remedy Integrator, IBM Mainframe Connector e Connector for SAP XAL, è necessaria una licenza aggiuntiva.

1.5.1 Servizi di raccolta

Sentinel raccoglie dati dai dispositivi di origine e restituisce un flusso di eventi più ricco inserendo tassonomia, rilevamento degli exploit e rilevanza aziendale nel flusso di dati prima che gli eventi siano correlati, analizzati e inviati al database. Un flusso di eventi più corposo indica che i dati vengono collegati al contesto aziendale necessario per identificare e riparare alle minacce interne o esterne e alle violazioni alle norme.

I Servizi di raccolta Sentinel sono in grado di analizzare sintatticamente i dati dai seguenti tipi di dispositivi e altro:

- Sistemi di rilevamento delle intrusioni (host)
- Sistemi di rilevamento delle intrusioni (rete)
- Firewall
- Sistemi operativi
- Monitoraggio delle norme
- Autenticazione
- Router e switch
- VPN
- Sistemi di rilevamento anti-virus
- Server Web
- Database
- Mainframe
- Sistemi di valutazione delle vulnerabilità
- Directory Services
- Sistemi di gestione della rete
- Sistemi proprietari

I servizi di raccolta JavaScript possono essere scritti mediante gli strumenti di sviluppo JavaScript standard e il kit SDK dei servizi di raccolta.

1.5.2 Connettori e integratori

I connettori garantiscono la connettività da Gestione servizi di raccolta alle origini eventi mediante protocolli standard quali JDBC e Syslog. Gli eventi vengono trasferiti dal connettore al servizio di raccolta per l'analisi sintattica.

Gli integratori consentono di eseguire operazioni di correzione sui sistemi all'esterno di Sentinel. Un'azione di correlazione può ad esempio utilizzare l'integratore SOAP per inizializzare un workflow Novell Nsure Identity Manager.

L'integratore Remedy AR facoltativo consente di creare un ticket Remedy dagli eventi o casi Sentinel. Per ulteriori informazioni, vedere “Action Manager and Integrator” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.5.3 Regole di correlazione e azioni

Le regole di correlazione identificano schemi importanti nel flusso degli eventi. Quando si attiva una regola di correlazione, vengono avviate le azioni di correlazione, ad esempio l'invio di notifiche e-mail, l'inizializzazione di un workflow iTRAC o l'esecuzione di un'azione mediante un integratore. Per ulteriori informazioni, vedere “Correlation Tab” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.5.4 Rapporti

Dall'interfaccia Web di Sentinel Rapid Deployment è possibile eseguire un'ampia varietà di rapporti dashboard e operativi utilizzando JasperReports. I rapporti vengono in genere distribuiti tramite pacchetti soluzione.

1.5.5 Workflow iTRAC

I workflow iTRAC forniscono processi coerenti e ripetibili per la gestione dei casi. I modelli di workflow vengono in genere distribuiti tramite pacchetti soluzione. Con iTRAC è fornito in dotazione un set di modelli di default che è possibile adattare alle proprie esigenze. Per ulteriori informazioni, vedere “iTRAC Workflows” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.5.6 Pacchetti soluzione

I pacchetti soluzione sono set di pacchetti di contenuti Sentinel correlati, ad esempio regole di correlazione, azioni, workflow iTRAC e rapporti. Novell fornisce pacchetti soluzione mirati per esigenze aziendali specifiche, ad esempio il pacchetto soluzione PCI-DSS, relativo alla conformità allo standard per la sicurezza dei dati nel settore delle carte di pagamento. Novell crea inoltre pacchetti di servizi di raccolta che includono contenuti focalizzati su un'origine evento specifica, ad esempio Windows Active Directory. Per ulteriori informazioni, vedere “Solution Packs ” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

1.6 Supporto linguistico

I componenti di Sentinel sono disponibili nelle lingue seguenti:

- Ceco
- Inglese
- Francese
- Tedesco
- Italiano
- Giapponese
- Olandese
- Polacco
- Portoghese
- Cinese semplificato
- Spagnolo
- Cinese tradizionale

Requisiti di sistema

2

Per ottenere prestazioni e affidabilità migliori, è necessario installare i componenti di Sentinel Rapid Deployment su software e hardware approvati, come elencato nella presente sezione. I requisiti indicati nella sezione sono stati completamente sottoposti a controllo qualità e certificati.

2.1 Piattaforme supportate

Tabella 2-1 elenca le combinazioni di software e sistemi operativi certificati o supportati da Novell. Le combinazioni certificate sono state testate mediante la suite di test completa di Novell Engineering. Si prevede che le combinazioni supportate siano completamente funzionali.

2.1.1 Sistemi operativi supportati

Novell supporta l'esecuzione di Sentinel Rapid Deployment sulle versioni di sistemi operativi riportate nella presente sezione. Novell supporta inoltre l'esecuzione su sistemi con aggiornamenti minori a tali sistemi operativi, come patch di sicurezza o hotfix. Tuttavia, l'esecuzione di Sentinel Rapid Deployment su sistemi con aggiornamenti maggiori o minori a tali piattaforme non è supportata fino a quando Novell non abbia eseguito le verifiche e le certificazioni necessarie per tali aggiornamenti.

I componenti server di Sentinel Rapid Deployment includono Communication Server, il motore di correlazione, DAS (Data Access Service), il server Web e il servizio di sottoscrizione ai dati di Advisor.

Le applicazioni client di Sentinel includono SCC (Sentinel Control Center), Gestione dati Sentinel e SSD (Sentinel Solution Designer).

Per la Gestione servizi di raccolta sono necessari requisiti di piattaforma specifici.

Tabella 2-1 *Sistemi operativi supportati e certificati*

Piattaforme	Componenti server	Applicazioni client di Sentinel	Gestione servizi di raccolta
SUSE Linux Enterprise Server (SLES) 11 SP1 (a 64 bit)	Certificata	Certificata	Certificata
SUSE Linux Enterprise Server (SLES) 11 SP1 (a 32 bit)	Non supportata	Supportata	Supportata

Piattaforme	Componenti server	Applicazioni client di Sentinel	Gestione servizi di raccolta
SUSE Linux Enterprise Server (SLES) 10 SP3 (a 64 bit)	Certificata	Supportata	Supportata
SUSE Linux Enterprise Server (SLES) 10 SP3 (a 32 bit)	Supportata	Supportata	Supportata
Windows Server 2008 R2 (a 64 bit)	Non supportata	Certificata	Certificata
Windows Server 2003 R2 (a 64 bit)	Non supportata	Supportata	Supportata
Windows Server 2003 R2 (a 32 bit)	Non supportata	Supportata	Supportata
Windows XP SP3 (a 32 bit)	Non supportata	Supportata	Non supportata
Windows Vista SP2 (a 32 bit)	Non supportata	Supportata	Non supportata
Windows 7	Non supportata	Certificata	Non supportata

Per ottenere prestazioni, stabilità e affidabilità ottimali, attenersi alle seguenti linee guida:

- Per SLES, il sistema operativo del computer server di Sentinel Rapid Deployment deve includere almeno i componenti server di base e X Window di SLES.
- Per il server Sentinel Rapid Deployment, utilizzare il file system ext3. Per ulteriori informazioni sui file system, vedere Overview of File Systems in Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) in *Storage Administration Guide* (in lingua inglese).

Nota:

- Sentinel Rapid Deployment non è supportato sulle installazioni Open Enterprise Server di SLES.
- La versione demo a 32 bit del server Sentinel 6.1 Rapid Deployment è progettata per ambienti di dimostrazione e test a scala limitata dove vengono utilizzati sistemi operativi e hardware a 32 bit. I clienti o i partner che hanno stipulato un apposito contratto per Sentinel 6.1 Rapid Deployment possono ricevere dal Supporto tecnico Novell un supporto limitato per i problemi riproducibili sulla piattaforma di produzione a 64 bit. Date le limitazioni intrinseche dell'hardware a 32 bit, il Supporto tecnico Novell non risolve i problemi inerenti alle prestazioni o alla scalabilità con la versione demo a 32 bit. Le versioni demo a 32 bit non sono supportate in un ambiente di produzione.

2.2 Requisiti hardware

I componenti server di Sentinel Rapid Deployment vengono eseguiti su hardware x86-64 (a 64 bit), con alcune eccezioni che, come indicato nella Sezione 2.1.1, “Sistemi operativi supportati”, a pagina 19 dipendono dal sistema operativo. Sentinel è certificato su hardware AMD Opteron e Intel Xeon. I server Itanium non sono supportati.

In questa sezione vengono fornite raccomandazioni generali sull'hardware per la progettazione del sistema Sentinel. I consigli sulla progettazione si basano sugli intervalli di frequenza degli eventi. Tali raccomandazioni si basano tuttavia sui presupposti seguenti:

- La frequenza degli eventi è al limite superiore dell'intervallo EPS (Evento al secondo).

- La dimensione media dell'evento è 1 KB.
- Tutti gli eventi sono memorizzati nel database, ovvero non sono impostati filtri per la rimozione degli eventi.
- I dati significativi relativi a novanta giorni vengono memorizzati in linea nel database.
- Lo spazio di archiviazione per i dati di Advisor non è incluso nelle specifiche Tabella 2-2 a pagina 21 e in Tabella 2-3 a pagina 22.
- Per default, il server Sentinel dispone di 5 GB di spazio su disco per la memorizzazione temporanea nella cache dei dati degli eventi che non è possibile inserire immediatamente nel database.
- Sul server Sentinel è inoltre disponibile uno spazio su disco di default di 5 GB per gli eventi che non è possibile inserire immediatamente nei file degli eventi di aggregazione.
- la sottoscrizione facoltativa ad Advisor richiede 1 GB aggiuntivi di spazio su disco nel server.

Poiché i suggerimenti relativi all'hardware per un'implementazione di Sentinel possono variare di volta in volta, è consigliabile consultare i Servizi Novell Consulting o qualsiasi partner di Novell Sentinel prima di finalizzare l'architettura di Sentinel. È possibile adottare i suggerimenti seguenti come linea guida.

Nella versione SLES, il database è incorporato nel server Sentinel Rapid Deployment ed è installato sullo stesso computer del server.

Nota: a causa degli elevati carichi di eventi e della memorizzazione nella cache locale, è necessario che nel server Sentinel sia disponibile un array di dischi con striping locale o condiviso (RAID) con almeno 4 perni.

Tabella 2-2 *Configurazione di un singolo computer (fino a 2000 eps)*

Componenti	RAM	Spazio	CPU
Computer 1: Server Sentinel Rapid Deployment ◆ Database PostgreSQL incorporato (3 GB) ◆ Gestione servizi di raccolta (1228 MB) ◆ DAS_Core (1579 MB) ◆ DAS_Binary (1404 MB) ◆ Motore di correlazione (1073 MB) ◆ 4 servizi di raccolta (generico, Cisco, Snort e IBM in grado di generare 500 eps ciascuno) ◆ 10 Regole di correlazione distribuite ◆ 10 Active Views univoci ◆ 3 utenti simultanei ◆ 2 mappature distribuite	16 GB	Dischi rigidi SAS (15000 rpm), 1 TB RAID 10 hardware	Dell PowerEdge 2900,2 x Quad-Core Intel Xeon E5310 (1,6 GHz) con NIC Gigabit Ethernet

Tabella 2-3 *Configurazione di tre computer (fino a 5000 eps)*

Componenti	RAM	Spazio	CPU
Computer 1: Server Sentinel Rapid Deployment ◆ Database PostgreSQL incorporato (3 GB) ◆ Gestione servizi di raccolta (1228 MB) ◆ DAS_Core (1579 MB) ◆ DAS_Binary (1404 MB) ◆ Motore di correlazione (1073 MB) ◆ 4 servizi di raccolta (in grado di generare 500 eps ciascuno), 1500 EPS da Gestione servizi di raccolta remoto 1 e 1500 EPS da Gestione servizio di raccolta remoto 2.	16 GB	Dischi rigidi SAS (15000 rpm), 1 TB RAID 10 hardware	Dell PowerEdge 2900,2 x Quad-Core Intel Xeon E5310 (1,6 GHz) con NIC Gigabit Ethernet
Computer 2: Gestione servizi di raccolta ◆ Gestione servizi di raccolta/Servizi di raccolta ◆ 3 servizi di raccolta (in grado di generare 500 eps ciascuno)	4 GB	Disco rigido SATA (3 Gbit/s), 300 GB	Intel Core 2 Duo E6750 (2.66 GHz) con NIC Gigabit Ethernet
Computer 3: Gestione servizi di raccolta ◆ Gestione servizi di raccolta/Servizi di raccolta ◆ 3 servizi di raccolta (in grado di generare 500 eps ciascuno)	4 GB	Disco rigido SATA (3 Gbit/s), 300 GB	Intel Core 2 Duo E6750 (2.66 GHz) con NIC Gigabit Ethernet

2.3 Browser Web supportati

- Mozilla Firefox 3.*x*
- Internet Explorer 8.*x*

2.4 Ambiente virtuale

Sentinel Rapid Deployment è stato ampiamente testato su VMWare ESX Server e Novell supporta completamente Sentinel Rapid Deployment in questo ambiente. Per ottenere prestazioni paragonabili ai risultati dei test del computer fisico svolti 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 informazioni sui consigli per il computer fisico di un sistema SLES vedere Sezione 2.2, “Requisiti hardware”, a pagina 20

2.5 Limiti consigliati

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

- Sezione 2.5.1, “Limiti di Gestione servizi di raccolta”, a pagina 23
- Sezione 2.5.2, “Limiti dei rapporti”, a pagina 24

2.5.1 Limiti di Gestione servizi di raccolta

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

Tabella 2-4 *Numeri delle prestazioni di Gestione servizi di raccolta*

Attributo	Limite	Commenti
Numero massimo di istanze di Gestione servizi di raccolta	20	Il limite specificato presuppone che ciascuna Gestione servizi di raccolta sia in esecuzione con una bassa frequenza EPS (ad esempio, meno di 100 EPS). Il limite diminuisce proporzionalmente all'aumento degli eventi al secondo.
Numero massimo di connettori (utilizzati appieno) in un'unica Gestione servizi di raccolta	1 per core CPU, con almeno un 1 core CPU riservato per il sistema operativo e altre elaborazioni	Un connettore utilizzato appieno, è un connettore che viene eseguito con una frequenza EPS massima per il suo genere.
Numero massimo di connettori (utilizzati appieno) in un'unica Gestione servizi di raccolta	1 per core CPU, con almeno un 1 core CPU riservato per il sistema operativo e altre elaborazioni	Un servizio di raccolta utilizzato appieno, è un servizio che viene eseguito con una frequenza EPS massima per il suo genere.
Numero massimo di dispositivi in un'unica Gestione servizi di raccolta	2000	Anche per il server Sentinel Rapid Deployment il limite è 2000, quindi se in un'unica Gestione servizi di raccolta sono presenti 2000 dispositivi, per il sistema complessivo Sentinel è stato raggiunto il limite massimo di dispositivi all'interno della Gestione servizi di raccolta specificata.
Numero massimo di dispositivi nel server Sentinel Rapid Deployment	2000	Il numero di dispositivi nel server Sentinel Rapid Deployment è limitato a 2000.

2.5.2 Limiti dei rapporti

Tabella 2-5 *Numeri di prestazioni dei rapporti*

Attributo	Limite	Commenti
Numero massimo di rapporti salvati	200	Tale limite può essere maggiore o minore a seconda delle dimensioni dei rapporti e dello spazio su disco disponibile sul server che non viene utilizzato dal resto del sistema.
Numero massimo di rapporti in esecuzione contemporaneamente	3	Il limite presuppone che il server non sia già molto occupato con la raccolta dati o altri task.

2.6 Risultati dei test

Sentinel Rapid Deployment consente di disporre di diverse configurazioni a seconda delle necessità dell'ambiente. Le seguenti informazioni sui test sulle prestazioni sono il risultato dei test svolti da Novell sulle configurazioni specifiche elencate nelle tabelle riportate sotto.

Poiché i suggerimenti relativi all'hardware per un'implementazione di Sentinel possono variare di volta in volta, è consigliabile consultare i Servizi Novell Consulting o un partner di Novell Sentinel prima di finalizzare l'architettura di Sentinel. È possibile adottare le seguenti informazioni sui test come linea guida.

Il test su Linux è stato eseguito per scalare l'EPS massimo con vari dispositivi e per scalare il numero massimo di dispositivi per un EPS specifico. È stata utilizzata la seguente configurazione hardware:

- **Numero di core CPU:** 4
- **Modello CPU:** CPU Intel Xeon X5770 a 2,93 GHz
- **RAM:** 16 GB
- **Dimensione disco rigido (tipo +RAID e numero di dischi nel RAID):** 1,7 TB (RAID 5, 6 dischi)

Nota: tutti i test sono stati effettuati con origini eventi basate su syslog. Altri servizi di raccolta potrebbero offrire prestazioni diverse.

Nella seguente tabella è illustrato l'EPS massimo che è possibile scalare con un numero diverso di dispositivi su un sistema SLES:

Tabella 2-6 *EPS massimo su un sistema SLES*

Configurazione del sistema	Dispositivi	EPS max
4 istanze di Gestione servizi di raccolta (una locale e tre remote) con 10 servizi di raccolta, in grado di generare 500 EPS ciascuno	25	5000
4 istanze di Gestione servizi di raccolta (una locale e tre remote) con 10 servizi di raccolta, in grado di generare 500 EPS ciascuno	100	5000

Configurazione del sistema	Dispositivi	EPS max
4 istanze di Gestione servizi di raccolta (una locale e tre remote) con 10 servizi di raccolta, in grado di generare 500 EPS ciascuno	1000	5000

Nella seguente tabella è illustrato il numero massimo di dispositivi che è possibile scalare a frequenze EPS diverse su un sistema SLES:

Tabella 2-7 *Numero massimo di dispositivi su un sistema SLES*

Configurazione del sistema	EPS	Numero massimo di dispositivi
1 Gestione servizi di raccolta con 1 servizio di raccolta in grado di generare 500 EPS	500	2000
1 Gestione servizi di raccolta con 2 servizi di raccolta in grado di generare 500 EPS ciascuno	1000	2000
1 Gestione servizi di raccolta con 3 servizi di raccolta in grado di generare 500 EPS ciascuno	1500	2000

Nota:

- Se si desidera scalare altri EPS o dispositivi, installare ulteriori istanze di Gestione servizi di raccolta.
- I limiti massimi di dispositivi non sono imposti, bensì consigliati in base ai test sulle prestazioni effettuati da Novell. Si presuppone una media bassa di eventi al secondo per dispositivo (meno di 3 EPS). Frequenze EPS più elevate provocano un numero massimo di dispositivi sostenibili inferiore. Per arrivare ai limiti approssimativi per una frequenza EPS media specifica o numero di dispositivi, sempre che il numero massimo di dispositivi non superi i limiti indicati sopra, è possibile utilizzare l'equazione (numero massimo di dispositivi) x (media EPS per dispositivo) = frequenza eventi massima.

Installazione

3

Questa sezione fornisce le informazioni necessarie per l'installazione di Sentinel Rapid Deployment e componenti client.

3.1 Panoramica

Il pacchetto di installazione Sentinel fornisce un programma di installazione semplificato del server con computer unico per installare tutto l'occorrente necessario per eseguire Sentinel Rapid Deployment. Il programma di installazione del server Sentinel Rapid Deployment installa i seguenti componenti:

3.1.1 Componenti server

Tabella 3-1 *Componenti e applicazioni del server Sentinel*

Componente	Descrizione
	Nel database di Sentinel sono memorizzati i dati sulla configurazione e gli eventi.
Bus messaggi	Un bus messaggi basato su JMS gestisce la comunicazione tra i componenti del sistema Sentinel.
Motore di correlazione	Il motore di correlazione esegue l'analisi degli eventi in tempo reale.
Advisor	Advisor fornisce una correlazione in tempo reale tra gli attacchi IDS rilevati e i risultati della scansione della vulnerabilità, allo scopo di segnalare immediatamente all'organizzazione l'aumentato rischio.
Servizio DAS (Data Access Service)	Include componenti per la memorizzazione, l'interrogazione, la visualizzazione e l'elaborazione dei dati.

Componente	Descrizione
Server Web	Supporta l'interfaccia Web per Sentinel Rapid Deployment.
Gestione servizi di raccolta	Servizio che gestisce le connessioni alle origini eventi, l'analisi sintattica dei dati, la mappatura e così via. È possibile distribuire la Gestione servizi di raccolta in altre ubicazioni, altri computer e altri sistemi operativi tramite il programma di installazione apposito disponibile nell'interfaccia Web di Sentinel Rapid Deployment. Ad esempio, è possibile installare una Gestione servizi di raccolta aggiuntiva in un computer Windows per raccogliere eventi di Windows.
iTRAC	Sentinel fornisce un sistema di gestione del workflow iTRAC per la definizione e l'automazione dei processi relativi alla risposta dei casi. I casi identificati in Sentinel, tramite una regola di correlazione o manualmente, possono essere associati a un workflow iTRAC.

3.1.2 Applicazioni client

Le applicazioni client Sentinel Control Center, Gestione dati Sentinel e Solution Designer sono installate per default sul server Sentinel Rapid Deployment. È possibile avviare le applicazioni client in uno dei seguenti metodi:

- Mediante l'interfaccia Web di Sentinel Rapid Deployment. Per avviare le applicazioni Sentinel da Webstart, è necessario che nei sistemi client sia installato Java 1.6.0_20 o versione successiva e che sia impostato il percorso JRE.

  Impostare la variabile di ambiente `JAVA_HOME` in modo che faccia riferimento all'ubicazione della cartella `JRE 6`. Impostare il percorso di esportazione in modo che faccia riferimento alla cartella `bin` sotto l'ubicazione JRE 6.
- Utilizzando `<directory_di_installazione>/bin` come utente proprietario dei file di installazione di Sentinel Rapid Deployment. Ad esempio:

  `./bin/<client_application>.sh`

Tabella 3-2 *Applicazioni client di Sentinel*

Componente	Descrizione
Sentinel Control Center	La console principale per gli analisti della sicurezza o della conformità.
Gestione dati Sentinel	Utility per la gestione di database.
Solution Designer	Applicazione per la creazione di pacchetti soluzione.
Gestione servizi di raccolta Sentinel	Servizio che gestisce le connessioni alle origini eventi, l'analisi sintattica dei dati, la mappatura e così via. Un componente Gestione servizi di raccolta è installato nel server Sentinel, ma è possibile installare istanze aggiuntive di Gestione servizi di raccolta su computer Windows o Linux remoti mediante un programma di installazione disponibile per il download.

3.2 Installazione su SUSE Linux Enterprise Server

3.2.1 Prerequisiti

Prima di installare Sentinel Rapid Deployment, assicurarsi che i seguenti prerequisiti siano soddisfatti. Per ulteriori informazioni sui prerequisiti (compreso l'elenco delle piattaforme certificate), vedere Capitolo 2, “Requisiti di sistema”, a pagina 19.

Importante: le installazioni di Sentinel Rapid Deployment mediante il programma di installazione completo devono sempre essere eseguite in un sistema pulito. Se su uno dei computer sono state precedentemente installate altre versioni di Sentinel, come Sentinel Classic o Sentinel Log Manager, prima di procedere è necessario disinstallarle. Per informazioni su come disinstallare le versioni precedenti di Sentinel, vedere le Guide all'installazione corrispondenti:

- Per disinstallare Sentinel Classic, vedere il capitolo “Disinstallazione di Sentinel” in Guida all'installazione di Sentinel (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html).
- Per disinstallare Sentinel Log Manager, vedere il capitolo “Disinstallazione di Sentinel Log Manager” in Guida all'installazione di Sentinel Log Manager 1.1 (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html).

Server

- Verificare che tutti i computer server soddisfino i requisiti minimi di sistema. Per ulteriori informazioni sui requisiti di sistema, vedere Capitolo 2, “Requisiti di sistema”, a pagina 19.
- Configurare il sistema operativo in modo tale che il comando `hostname -f` restituisca un nome host valido.
- Installare e configurare un server SMTP per poter inviare notifiche e-mail dal sistema Sentinel.

Client

- Verificare che tutti i computer client soddisfino i requisiti minimi di sistema. Per ulteriori informazioni sui prerequisiti, vedere Capitolo 2, “Requisiti di sistema”, a pagina 19.
- Assicurarsi di creare una directory il cui nome contenga solo caratteri ASCII (e nessun carattere speciale) dalla quale eseguire il programma di installazione.
- Quando si installano Gestione servizi di raccolta o applicazioni client remote su computer Linux, assicurarsi che nella cartella `/tmp` non siano impostate restrizioni per l'utente admin.

- Assicurarsi che all'utente di dominio di Gestione servizi di raccolta su Windows vengano assegnati i privilegi power user perché i diritti utente normali non sono sufficienti per l'installazione di Gestione servizi di raccolta.
- Se si installa Gestione servizi di raccolta su un computer a 64 bit, assicurarsi che siano disponibili le librerie a 32 bit. Quando si esegue un Servizio di raccolta scritto nel lingua esclusiva del servizio di raccolta (che include quasi tutti i servizi di raccolta scritti prima di giugno 2008) e quando si eseguono alcuni connettori (ad esempio il connettore LEA), sono richieste le librerie a 32 bit. I servizi di raccolta basati su Javascript e gli altri servizi di Sentinel sono abilitati su hardware a 64 bit. È importante verificare la disponibilità di tali librerie soprattutto sulle piattaforme Linux, nelle quali potrebbero non essere incluse per default.

Advisor

Se si desidera installare Advisor, è necessario acquistare la sottoscrizione per Sentinel Exploit Detection e Advisor Data. Una volta acquistata la sottoscrizione, utilizzare Novell eLogin per effettuare il download e aggiornare i dati di Advisor. Per ulteriori informazioni, vedere il capitolo "Advisor Usage and Maintenance" in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

3.2.2 Installazione di Sentinel Rapid Deployment

È possibile installare il server Sentinel Rapid Deployment nei seguenti modi:

- "Installazione mediante singolo script con privilegi root" a pagina 30
- "Installazione per utente non radice" a pagina 32

Durante l'installazione, lo script del programma di installazione di Sentinel Rapid Deployment fornisce le seguenti opzioni:

- **-all:** per utilizzare l'opzione è necessario essere l'utente `radice`. Questa opzione consente di creare un utente (default: `novell`), gruppo di utenti, (default: `novell`) e di installare quindi il server Sentinel Rapid Deployment. Inoltre, all'avvio del sistema i servizi Sentinel Rapid Deployment vengono eseguiti automaticamente.
- **-installazione:** questa opzione consente solo di installare il server Sentinel Rapid Deployment.
- **-createuser:** per utilizzare l'opzione è necessario essere l'utente `radice`. Questa opzione consente solo di creare l'utente (default: `novell`) e il gruppo di utenti (default: `novell`).
- **-createservice:** per utilizzare l'opzione è necessario essere l'utente `radice`. Questa opzione abilita solo l'esecuzione automatica dei servizi Sentinel Rapid Deployment all'avvio del sistema.
- **-help:** questa opzione consente di visualizzare le informazioni su come utilizzare le opzioni dello script di installazione.

Installazione mediante singolo script con privilegi root

1. Eseguire il login come utente `radice`.

   L'utente che esegue l'installazione deve disporre dei diritti di accesso alla scrittura nella directory temporanea in cui viene effettuato il download dei file del programma di installazione.
2. Effettuare il download del programma di installazione `sentinel6_rd_linux_x86-64.tar.gz`dal sito di download di Novell (http://download.novell.com/) in una directory temporanea.

3 Estrarre il programma di installazione:

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

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

```
cd sentinel6_rd_linux_x86-64
```

5 Eseguire lo script `install.sh` con l'opzione `-all`:

```
./install.sh -all
```

Lo script di installazione verifica prima la memoria disponibile, quindi lo spazio su disco. Se la memoria disponibile è inferiore a 1 GB, l'installazione viene automaticamente interrotta dallo script. Se la memoria disponibile è superiore a 1 GB, ma inferiore a 4 GB, lo script visualizza un messaggio in cui si viene informati che la memoria disponibile è inferiore a quella consigliata. Viene chiesto inoltre se si desidera continuare con l'installazione. Immettere `s` in caso affermativo oppure `n` se non si desidera continuare.

6 Specificare il nome utente o premere Invio per selezionare quello di default. Il nome utente di default è `novell`.

Se il nome utente specificato esiste già, si viene notificati con un messaggio da parte del programma di installazione e viene visualizzato il gruppo dell'utente. Procedere con Passo 8.

Se il nome utente specificato non esiste, il programma di installazione lo crea. Procedere con Passo 7.

7 Specificare il nome gruppo o premere Invio per selezionare il nome gruppo di default. Il nome gruppo di default è `novell`.

Se il nome gruppo specificato esiste già, si continua con l'installazione. Se il nome gruppo non esiste, il programma di installazione crea il gruppo e viene visualizzato un messaggio a indicare che il nome utente specificato è stato creato nel gruppo definito.

L'utente e il gruppo specificati sono i proprietari dell'installazione e dei processi in esecuzione di Sentinel.

8 Specificare il percorso di installazione o premere Invio per selezionare il percorso di default. Il percorso di default è `/opt/novell`.

Il percorso di installazione specificato non deve contenere spazi. Se dovesse contenere uno spazio, lo script di installazione richiede di specificare un percorso di installazione privo di spazi.

9 Scegliere una delle lingue seguenti immettendo il numero corrispondente:

Numero di serie	Lingua
1	Ceco
2	Inglese
3	Francese
4	Tedesco
5	Italiano
6	Giapponese
7	Olandese
8	Polacco

Numero di serie	Lingua
9	Portoghese
10	Cinese semplificato
11	Spagnolo
12	Cinese tradizionale

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

10 Leggere il contratto di licenza con l'utente finale e immettere `1` se si accettano i termini indicati e si desidera continuare l'installazione. Per uscire dall'installazione, immettere `2`.

Il programma di installazione avvia quindi l'estrazione dei file e richiede la licenza.

11 Immettere `1` per utilizzare chiave di licenza per un periodo di valutazione di 90 giorni o immettere `2` per utilizzare la chiave di licenza valida.

Se si immette `2`, dal programma di installazione viene richiesto di immettere la chiave di licenza di Sentinel RD valida. Se la chiave di licenza specificata non è valida, dal programma di installazione viene richiesto di specificare di nuovo la chiave di licenza valida. Se la chiave di licenza specificata non è valida al secondo tentativo, viene installata automaticamente la chiave di licenza per un periodo di prova di 90 giorni. È possibile immettere la chiave di licenza valida in un secondo momento.

Lo script carica quindi la licenza di prova o quella valida.

12 Specificare una password per l'utente `dbauser` e confermarla digitandola di nuovo.

Le credenziali `dbauser` vengono utilizzate per creare tabelle e partizioni nel database PostgreSQL.

13 Specificare una password per l'utente `admin` e confermarla digitandola di nuovo.

Quando viene richiesto di specificare le password per gli utenti `admin` e `dbauser`, evitare di utilizzare la barra rovesciata (\) e l'apostrofo (‘) nella password, in quanto tali caratteri non sono consentiti dal database PostgreSQL.

Lo script di installazione installa il database PostgreSQL, crea tabelle e partizioni, quindi installa il server Sentinel Rapid Deployment.

Dopo l'installazione è possibile:

- Avviare l'interfaccia Web di Sentinel Rapid Deployment accedendo a `https://<IP_SERVER>:8443/sentinel.` <*IP_SERVER*> è l'indirizzo IP del computer in cui è installato Sentinel Rapid Deployment.
- Avviare Sentinel Control Center eseguendo `<directory_di_installazione>/bin/control_center.sh` come l'utente creato al Passo 6.

Installazione per utente non radice

Se la policy dell'organizzazione non consente di eseguire l'intero processo di installazione come utente `radice`, è possibile completare l'installazione in due fasi. La prima parte della procedura di installazione deve essere eseguita con privilegi `radice`, mentre la seconda parte viene eseguita come utente amministrativo di Sentinel, creato durante la prima parte.

1 Eseguire il login al server in cui si desidera installare Sentinel Rapid Deployment.

L'utente che esegue l'installazione deve disporre dei diritti di accesso alla scrittura nella directory temporanea in cui viene effettuato il download dei file del programma di installazione.

2. Effettuare il download del programma di installazione `sentinel6_rd_linux_x86-64.tar.gz`dal sito di download di Novell (http://download.novell.com/) in una directory temporanea.
3. Estrarre il programma di installazione:

   ```
   tar zxvf sentinel6_rd_linux_x86-64.tar.gz
   ```
4. Eseguire il login come utente `radice`.
5. Passare alla directory in cui è stato estratto il programma di installazione:

   ```
   cd sentinel6_rd_linux_x86-64
   ```
6. Eseguire lo script `install.sh` con l'opzione `-createuser`:

   ```
   ./install.sh -createuser
   ```
7. Specificare il nome utente o premere Invio per selezionare quello di default. Il nome utente di default è `novell`.

   Se il nome utente specificato esiste già, si viene notificati con un messaggio da parte del programma di installazione e viene visualizzato il gruppo dell'utente. Procedere con Passo 9.

   Se il nome utente specificato non esiste, il programma di installazione lo crea. Procedere con Passo 8.
8. Specificare il nome gruppo o premere Invio per selezionare il nome gruppo di default. Il nome gruppo di default è `novell`.

   Se il nome gruppo specificato esiste già, si continua con l'installazione. Se il nome gruppo non esiste, il programma di installazione crea il gruppo e viene visualizzato un messaggio a indicare che il nome utente specificato è stato creato nel gruppo definito.

   L'utente e il gruppo specificati sono i proprietari dell'installazione e dei processi in esecuzione di Sentinel.
9. Specificare il percorso di installazione o premere Invio per selezionare il percorso di default. Il percorso di default è `/opt/novell`.

   Il percorso di installazione specificato non deve contenere spazi. Se dovesse contenere uno spazio, lo script di installazione richiede di specificare un percorso di installazione privo di spazi.
10. Eseguire il login come utente non radice. Ad esempio.

    ```
    su - novell
    ```
11. Eseguire lo script di installazione con l'opzione `-install`:

    ```
    ./install.sh -install
    ```

    Lo script di installazione verifica prima la memoria disponibile, quindi lo spazio su disco. Se la memoria disponibile è inferiore a 1 GB, l'installazione viene automaticamente interrotta dallo script. Se la memoria disponibile è superiore a 1 GB, ma inferiore a 4 GB, lo script visualizza un messaggio in cui si viene informati che la memoria disponibile è inferiore a quella consigliata. Viene chiesto inoltre se si desidera continuare con l'installazione. Immettere `s` in caso affermativo oppure `n` se non si desidera continuare.
12. Specificare il percorso di installazione o premere Invio per selezionare il percorso di default. Il percorso di default è `/opt/novell`.

Il percorso di installazione specificato non deve contenere spazi. Se dovesse contenere uno spazio, lo script di installazione richiede di specificare un percorso di installazione privo di spazi.

13 Scegliere una delle lingue seguenti immettendo il numero corrispondente:

Numero di serie	Lingua
1	Ceco
2	Inglese
3	Francese
4	Tedesco
5	Italiano
6	Giapponese
7	Olandese
8	Polacco
9	Portoghese
10	Cinese semplificato
11	Spagnolo
12	Cinese tradizionale

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

14 Leggere il contratto di licenza con l'utente finale e immettere `1` se si accettano i termini indicati e si desidera continuare l'installazione. Per uscire dall'installazione, immettere `2`.

Il programma di installazione avvia quindi l'estrazione dei file e richiede la licenza.

15 Immettere `1` per utilizzare chiave di licenza per un periodo di valutazione di 90 giorni o immettere `2` per utilizzare la chiave di licenza valida.

Se si immette `2`, dal programma di installazione viene richiesto di immettere la chiave di licenza di Sentinel RD valida. Se la chiave di licenza specificata non è valida, dal programma di installazione viene richiesto di specificare di nuovo la chiave di licenza valida. Se la chiave di licenza specificata non è valida al secondo tentativo, viene installata automaticamente la chiave di licenza per un periodo di prova di 90 giorni. È possibile immettere la chiave di licenza valida in un secondo momento.

Lo script carica quindi la licenza di prova o quella valida.

16 Specificare una password per l'utente `dbauser` e confermarla digitandola di nuovo.

Le credenziali `dbauser` vengono utilizzate per creare tabelle e partizioni nel database PostgreSQL.

17 Specificare una password per l'utente `admin` e confermarla digitandola di nuovo.

Quando viene richiesto di specificare le password per gli utenti `admin` e `dbauser`, evitare di utilizzare la barra rovesciata (\) e l'apostrofo (‘) nella password, in quanto tali caratteri non sono consentiti dal database PostgreSQL.

18 (Condizionale) Una volta completata l'installazione, se si desidera eseguire automaticamente i servizi Sentinel Rapid Deployment all'avvio del sistema, eseguire lo script `install.sh` con l'opzione `-createservice` come utente `radice`:

```
./install.sh -createservice
```

Dopo l'installazione è possibile:

- Avviare l'interfaccia Web di Sentinel Rapid Deployment accedendo a `https://<IP_SERVER>:8443/sentinel`. *<IP_SERVER>* è l'indirizzo IP del computer in cui è installato Sentinel Rapid Deployment.
- Avviare Sentinel Control Center eseguendo `<directory_di_installazione>/bin/control_center.sh` come l'utente creato al Passo 7 sopra.

3.3 Installazione di Gestione servizi di raccolta e applicazioni client

Utilizzare l'interfaccia Web di Novell Sentinel Rapid Deployment per effettuare il download del programma di installazione della Gestione servizi di raccolta e del client.

3.3.1 Download dei programmi di installazione

1 Avviare un browser Web e digitare l'URL seguente:

`https://<svrname.example.com>:8443/sentinel`

Sostituire `<nomesvr.esempio.com>` con il nome DNS o l'indirizzo IP effettivo del server in cui è in esecuzione Sentinel. Per questo URL viene fatta distinzione tra maiuscole e minuscole.

2 Se viene richiesto di verificare i certificati, controllare le informazioni dei certificati, quindi fare clic su *Sì* se sono valide.

3 Specificare il nome utente e la password per accedere all'account Sentinel.

4 Utilizzare l'elenco a discesa *Lingue* per selezionare la lingua.

Si tratta della stessa lingua del codice linguistico del server Sentinel Rapid Deployment e del computer locale. Verificare che le impostazioni della lingua del browser siano configurate per supportare la lingua desiderata.

5 Fare clic su *Accesso*.

6 Selezionare *Applicazioni*.

È possibile effettuare il download dei seguenti programmi di installazione:

Opzioni	Descrizione	Azione
Programma di installazione della Gestione servizi di raccolta	Il programma di installazione di Gestione servizi di raccolta consente di installare Gestione servizi di raccolta Sentinel sulle piattaforme Windows e Linux supportate.	Fare clic sull'opzione di *download del programma di installazione della Gestione servizi di raccolta* e seguire le istruzioni visualizzate.
Programma di installazione del client	Il programma di installazione del client consente di installare Sentinel Control Center, Sentinel Solution Designer e Gestione dati Sentinel sulle piattaforme supportate.	Fare clic sull'opzione di *download del programma di installazione client* e seguire le istruzioni visualizzate.

Per ulteriori informazioni sull'installazione di Gestione servizi di raccolta, vedere Sezione 3.3.4, “Installazione di Gestione servizi di raccolta Sentinel su SLES o Windows”, a pagina 39 e per l'installazione del programma di installazione del client, vedere Sezione 3.3.3, “Installazione delle applicazioni Client di Sentinel”, a pagina 36.

3.3.2 Numeri di porta per i componenti client di Sentinel Rapid Deployment

Utilizzare le seguenti porte per configurare le impostazioni firewall che consentono di accedere ai componenti server e client di Sentinel Rapid Deployment.

Tabella 3-3 *Numeri delle porte compatibili per i componenti di Sentinel Rapid Deployment*

Numero di porta	Descrizione
61616	Le istanze di Gestione servizi di raccolta remote utilizzano questo numero di porta per connettersi al server Sentinel Rapid Deployment tramite ActiveMQ.
10013	Sentinel Control Center utilizza questo numero di porta per connettersi al server Sentinel Rapid Deployment tramite un proxy.
5432	Gestione dati Sentinel utilizza questo numero di porta per connettersi al database PostgreSQL.
8443	I client Web utilizzano questo numero di porta per connettersi al server Sentinel Rapid Deployment.

3.3.3 Installazione delle applicazioni Client di Sentinel

È possibile installare l'applicazione client di Sentinel sia sul sistema Linux sia su Windows. Per installare le applicazioni client:

1. Selezionare la cartella in cui si è effettuato il download del programma di installazione del client.
2. Estrarre lo script di installazione dal file:

Piattaforma	Azione
Windows	Decomprimere il file `client_installer.zip`. I file vengono decompressi in una directory denominata `disk1`.
Linux	Eseguire il comando riportato di seguito con privilegi di utente root: `unzip client_installer.zip` I file vengono decompressi in una directory denominata `disk1`.

3 Individuare la directory di installazione e avviare l'installazione:

Piattaforma	Azione
Windows	Eseguire `disk1\setup.bat` **Nota:** in un computer con Windows Vista, avviare il prompt dei comandi selezionando l'opzione *Esegui come amministratore* nel menu di scelta rapida.
Linux	◆ **Modalità GUI:** `<directory_di_installazione>/disk1/setup.sh` ◆ **Modalità console:** `<directory_di_installazione>/disk1/setup.sh –console`

La procedura indicata di seguito riguarda solo la modalità GUI.

4 Fare clic sulla freccia giù e selezionare una lingua.

5 Nella schermata iniziale fare clic su *Avanti*.

6 Leggere e accettare le condizioni del Contratto di licenza per l'utente finale. Fare clic su *Avanti*.

7 Accettare la directory di installazione di default o fare clic su *Sfoglia* per specificare l'ubicazione dell'installazione. Fare clic su *Avanti*.

Importante: non è possibile eseguire l'installazione in una directory il cui nome contiene caratteri speciali o caratteri non ASCII. Ad esempio, quando si installa Sentinel Rapid Deployment su Windows x86-64, il percorso di default è `C:\\Programmi (x86)`. Per evitare caratteri speciali, come le parentesi in (x86), per continuare l'installazione è necessario modificare il percorso di default.

8 Selezionare le applicazioni Sentinel che si desidera installare.

Sono disponibili le seguenti opzioni:

Componente	Descrizione
Sentinel Control Center	La console principale per gli analisti della sicurezza o della conformità.
Gestione dati Sentinel (Sentinel Data Manager, SDM)	Utilizzato per le attività di gestione manuale del database.
Solution Designer	Consente di creare pacchetti soluzioni.

9 Se si sceglie di installare Sentinel Control Center, il programma di installazione richiede di allocare la quantità massima di spazio di memoria a Sentinel Control Center. Specificare le dimensioni massime dell'heap JVM (MB) da utilizzare solo per Sentinel Control Center.

   L'intervallo consentito è 64-1024 MB.

   Questa opzione non è disponibile se sono già installate applicazioni Sentinel.

10 Specificare il nome utente o premere Invio per selezionare il nome utente di default. Il nome utente di default è `esecadm`.

   Si tratta del nome utente proprietario del prodotto Sentinel installato. Se l'utente non è già esistente, ne verrà creato uno insieme alla home directory nella directory specificata.

11 Specificare la home directory dell'utente o premere Invio per selezionare la directory di default. La directory di default è `/export/home`.

   Se il nome utente è `esecadm`, la home directory corrispondente è `/export/home/esecadm`.

12 Specificare la password per l'utente ed eseguire il login come utente `esecadm` se al Passo 10 si è selezionato il nome utente di default. Altrimenti, impostare la password per l'utente creato al Passo 10.

13 Specificare le seguenti informazioni.

   - **Porta bus messaggi:** la porta in cui è in ascolto il server di comunicazione. I componenti che si connettono direttamente al server di comunicazione utilizzano questa porta. Il numero di porta di default è 61616.
   - **Porta proxy di Sentinel Control Center:** porta sulla quale il server proxy SSL (proxy Data Access Server) è in ascolto per accettare il nome utente e la password. Il server proxy SSL accetta le credenziali in base alle connessioni autenticate. Sentinel Control Center utilizza questa porta per eseguire la connessione al server Sentinel. Il numero di porta di default è `10013`.
   - **Nome host del server di comunicazione:** indirizzo IP o nome host del computer in cui è installato il server Sentinel Rapid Deployment.

   Assicurarsi che i numeri di porta siano gli stessi del server Sentinel Rapid Deployment in `<directory_di_installazione>/config/configuration.xml` per abilitare le comunicazioni. Annotare il numero di queste porte per installazioni future in altri computer. Per ulteriori informazioni sui numeri di porta, vedere Sezione 3.3.2, “Numeri di porta per i componenti client di Sentinel Rapid Deployment”, a pagina 36.

14 Fare clic su *Avanti*.

   Viene visualizzato un riepilogo dell'installazione.

15 Fare clic su *Installa*.

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

Nota: al login successivo utilizzare il nome utente specificato in Passo 10.

se si dimentica il nome utente impostato, aprire una console terminale e immettere il comando seguente come utente `radice`:

```
env | grep ESEC_USER
```

questo comando restituisce il nome utente se l'utente è già stato creato e le variabili ambiente sono già impostate.

3.3.4 Installazione di Gestione servizi di raccolta Sentinel su SLES o Windows

Il programma di installazione di Gestione servizi di raccolta Sentinel è disponibile per il download nella pagina Applicazioni dell'interfaccia Web di Sentinel Rapid Deployment. Per installare Gestione servizi di raccolta:

1. Selezionare la cartella in cui si è effettuato il download del programma di installazione di Gestione servizi di raccolta.
2. Estrarre lo script di installazione dal file:

Piattaforma	Azione
Windows	Decomprimere il file `scm_installer.zip`. I file vengono decompressi in una directory denominata `disk1`.
Linux	Eseguire il comando riportato di seguito con privilegi di utente root: `unzip scm_installer.zip` I file vengono decompressi in una directory denominata `disk1`.

3. Individuare la directory `disk1` e avviare l'installazione:

Piattaforma	Azione
Windows	Eseguire il comando seguente: `disk1\setup.bat`
Linux	◆ **Modalità GUI:** `<directory_di_installazione>/disk1/setup.sh` ◆ **Modalità console:** `<directory_di_installazione>/disk1/setup.sh –console`

4. Selezionare una lingua per continuare con l'installazione.
5. Leggere la schermata introduttiva e fare clic su *Avanti*.
6. Leggere e accettare le condizioni del Contratto di licenza per l'utente finale. Fare clic su *Avanti*.
7. Accettare la directory di installazione di default o fare clic su *Sfoglia* per specificare l'ubicazione dell'installazione, quindi fare clic su *Avanti*.

   Importante: non è possibile eseguire l'installazione in una directory il cui nome contiene caratteri speciali o caratteri non ASCII. Ad esempio, quando si installa Sentinel su Windows x86-64, il percorso di default è `C:\\Programmi (x86)`. Per evitare caratteri speciali, come le parentesi in (x86), per continuare l'installazione è necessario modificare il percorso di default.

8. Specificare il nome utente dell'amministratore di Sentinel e il percorso della home directory corrispondente.

   Questa opzione non è disponibile se sono già installate applicazioni Sentinel.

   ◆ **Nome utente dell'amministratore di Sentinel del sistema operativo:** il default è `esecadm`.

Si tratta del nome utente proprietario del prodotto Sentinel installato. Se l'utente non è già esistente, ne verrà creato uno insieme alla home directory corrispondente nella directory specificata.

- **Home directory dell'utente amministratore di Sentinel del sistema operativo:** di default è `/export/home`. Se `esecadm` è il nome utente, la home directory corrispondente è `/export/home/esecadm`.

Per eseguire il login come utente `esecadm`, è innanzitutto necessario impostare la relativa password.

9 Specificare le seguenti informazioni.

- **Porta bus messaggi:** la porta in cui è in ascolto il server di comunicazione. I componenti che si connettono direttamente al server di comunicazione utilizzano questa porta. Il numero di porta di default è 61616.
- **Nome host server di comunicazione:** l'IP o il nome host del computer in cui è installato il server di Sentinel Rapid Deployment.

Assicurarsi che i numeri di porta siano gli stessi su tutti i computer del sistema Sentinel per abilitare le comunicazioni. Annotare il numero di queste porte per installazioni future in altri computer.

10 Fare clic su *Avanti*.

11 Specificare le seguenti informazioni.

- **Configurazione memoria automatica:** selezionare la quantità di memoria totale da allocare a Gestione servizi di raccolta. Il programma di installazione determina automaticamente la distribuzione ottimale della memoria tra i componenti, prendendo in considerazione i requisiti previsti per il sistema operativo e l'overhead del database.

  Importante: è possibile modificare il valore -Xmx nel file `configuration.xml` per modificare la RAM allocata al processo Gestione servizi di raccolta. Il file `configuration.xml` è disponibile in `<directory_di_installazione>/config` su Linux o `<directory_di_installazione>\config` su Windows.

- **Configurazione memoria personalizzata:** fare clic su *Configura* per perfezionare le allocazioni della memoria. Questa opzione è disponibile solo se è presente una quantità di memoria sufficiente nel computer.

12 Fare clic su *Avanti*.

Viene visualizzata una schermata di riepilogo con le funzioni selezionate per l'installazione.

13 Fare clic su *Installa*.

14 Al termine dell'installazione viene richiesto di immettere il nome utente e la password utilizzati dalla strategia ActiveMQ JMS per connettersi al broker.

Utilizzare il nome utente `collectormanager` e la relativa password disponibile nel file `<directory_di_installazione>/config/activemqusers.properties` sul server Sentinel.

Di seguito è riportato un esempio di credenziali disponibili nel file `activemqusers.properties`:

```
collectormanager=cefc76062c58e2835aa3d777778f9295
```

`collectormanager` è il nome utente e `cefc76062c58e2835aa3d777778f9295` è la password corrispondente.

È necessario utilizzare l'utente collectormanager e la password corrispondente durante l'installazione del servizio Gestione servizi di raccolta. In questo caso, l'utente `collectormanager` dispone solo dei diritti di accesso ai canali di comunicazione richiesti per le operazioni di Gestione servizi di raccolta.

Al termine dell'installazione viene richiesto di riavviare il computer o di eseguire di nuovo il login e avviare manualmente in servizi Sentinel.

15 Fare clic su *Fine* per riavviare il sistema.

16 Eseguire di nuovo il login con il nome utente specificato al Passo 8.

Se si dimentica il nome utente, aprire una console terminale e immettere il comando seguente con credenziali `radice`.

```
env | grep ESEC_USER
```

Questo comando restituisce il nome utente se l'utente è già stato creato e le variabili ambiente sono già impostate.

Nota: l'installazione di Gestione servizi di raccolta sulla piattaforma Windows 2008 crea alcuni problemi, così come per le istanze di Gestione servizi di raccolta con immagini. Per informazioni sulla risoluzione di questi problemi, vedere Appendice B, “Suggerimenti per la soluzione dei problemi”, a pagina 91.

3.4 Avvio e interruzione manuale dei servizi Sentinel

Per avviare manualmente i servizi Sentinel, utilizzare i comandi seguenti:

Piattaforma	Comando
Linux	`<directory_di_installazione>/bin/sentinel.sh start`
Windows	`<directory_di_installazione>/bin/sentinel.bat start`

Per interrompere manualmente i servizi Sentinel, utilizzare i comandi seguenti:

Piattaforma	Comando
Linux	`<directory_di_installazione>/bin/sentinel.sh stop`
Windows	`<directory_di_installazione>/bin/sentinel.bat stop`

È inoltre possibile utilizzare il comando seguente per avviare o interrompere i servizi Sentinel.

```
/etc/init.d/sentinel.sh stop|start
```

3.5 Upgrade manuale di Java

La versione 1.6.0_24 di Java viene venduta insieme al programma di installazione del server Sentinel Rapid Deployment e viene installata contemporaneamente al server. Tuttavia, se si esegue l'upgrade di Java alla versione più recente sul server, affinché Sentinel Rapid Deployment la utilizzi, è necessario seguire la procedura indicata di seguito:

1. Effettuare il download dei pacchetti jre in base al sistema operativo su cui è installato il server Sentinel Rapid Deployment.

   L'utente che esegue l'upgrade deve disporre dei diritti di accesso alla scrittura nella directory di installazione di Sentinel Rapid Deployment e nella directory in cui viene effettuato il download dei file dell'upgrade.

   - Se è stato installato Sentinel Rapid Deployment su un SUSE Linux Enterprise Server, effettuare il download di entrambi i pacchetti jre a 32 e a 64 bit dal sito di download di Java (http://www.java.com/en/download/manual.jsp).

2. Rinominare le cartelle `jre` e `jre64` nella directory di installazione di Sentinel Rapid Deployment rispettivamente in `jre_old` e `jre64_old`.

   ```
   cd <install_path>/sentinel_rd
   mv jre jre_old
   mv jre64 jre64_old
   ```

   Nota: la ridenominazione delle cartelle è necessaria per ripristinare le versioni precedenti nel caso in cui l'upgrade di Java non funzioni correttamente. È possibile eliminare le cartelle rinominate se dopo l'upgrade Java funziona correttamente.

3. Estrarre i pacchetti jre di cui si è effettuato il download.
4. Rinominare la cartella 32 bit in `jre` e la directory 64 bit in `jre64`.
5. Copiare le cartelle `jre` e `jre64` rinominate nella directory di installazione di Sentinel Rapid Deployment.

   ```
   copy jre <install_path>/sentinel_rd/
   copy jre64 <install_path>/sentinel_rd/
   ```

6. (Condizionale) Assicurarsi che vengano impostate la proprietà e le autorizzazioni necessarie delle cartelle `jre` e `jre64` per l'utente che esegue il server Sentinel Rapid Deployment.
7. Riavviare il server Sentinel Rapid Deployment, riavviare il browser e verificare che Java sia installato correttamente.

3.6 Configurazione successiva all'installazione

Questa sezione consente di comprendere la configurazione successiva all'installazione per i servizi Sentinel Rapid Deployment.

3.6.1 Modifica delle impostazioni di data e ora

In Sentinel Control Center è possibile ignorare il formato di data e ora di default. Per ulteriori informazioni su come personalizzare il formato di data e ora secondo il fuso orario locale, vedere il sito Web di Java (http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html).

1. Modificare il file `SentinelPreferences.properties`.

   `<directory_di_installazione>/config/SentinelPreferences.properties`

2. Rimuovere il commento dalla riga seguente e personalizzare il formato di data e ora nei campi corrispondenti dell'evento di Sentinel Control Center:

   ```
   com.eSecurity.Sentinel.event.datetimeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
   ```

3.6.2 Configurazione di un integratore SMTP per l'invio di notifiche di Sentinel

In Sentinel Rapid Deployment, un'azione JavaScript SendEmail funziona con un integratore SMTP per inviare i messaggi di posta da diversi contesti all'interno dell'interfaccia di Sentinel ai destinatari dei messaggi. Affinché possa funzionare, è necessario configurare l'integratore SMTP con dati validi. Per ulteriori informazioni, vedere "Sending an E-mail" in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

Un'istanza di azione singola del plug-in azione SendEmail viene creata automaticamente in tutte le installazioni di Sentinel. Nell'azione SendEmail non sono necessarie configurazioni, solo i destinatari del messaggio di posta e i contenuti di quest'ultimo sono configurati nei parametri di azione.

L'azione SendEmail viene attivata internamente da Sentinel per l'invio della posta nelle seguenti situazioni:

- Quando si genera una regola di correlazione, viene attivata un'azione SendEmail. SendEmail è l'azione indicata dall'icona di ingranaggio ed è valida soltanto per la correlazione (a differenza dell'azione SendEmail di JavaScript indicata dall'icona JavaScript JS).
- Quando il flusso di lavoro include un passaggio o attività di posta configurata per l'invio di e-mail.
- Quando un utente apre un caso e sceglie di eseguire un'attività configurata per l'invio di e-mail.
- Quando un utente fa clic con il pulsante destro del mouse su un evento e seleziona *E-mail*.
- Quando un utente apre un caso e seleziona *Invia caso tramite e-mail*.

3.6.3 Servizi di Gestione servizi di raccolta

- "Installazione del servizio Gestione servizi di raccolta aggiuntivo" a pagina 44
- "Utilizzo del servizio di raccolta generico" a pagina 44

Installazione del servizio Gestione servizi di raccolta aggiuntivo

I servizi Gestione servizi di raccolta gestiscono tutti i processi di raccolta e di analisi sintattica dei dati. Talvolta potrebbe essere necessario aggiungere un ulteriore nodo di Gestione servizi di raccolta Sentinel all'ambiente di Sentinel per bilanciare il carico tra i computer. I servizi Gestione servizi di raccolta remoti offrono numerosi vantaggi:

- Consentono di analizzare sintatticamente ed elaborare gli eventi distribuiti per migliorare le prestazioni del sistema.
- Consentono il filtraggio, la cifratura e la compressione dei dati nel sistema di origine tramite la collocazione con le origini eventi. In tal modo si riducono i requisiti per la larghezza di banda ed è possibile ottenere maggiore una sicurezza dei dati.
- Consentono l'installazione su sistemi operativi aggiuntivi. Ad esempio, l'installazione di un nodo di Gestione servizi di raccolta su Microsoft Windows per abilitare la raccolta dati utilizzando il protocollo WMI.
- Consentono la memorizzazione dei file nella cache, grazie alla quale Gestione servizi di raccolta remota è in grado di memorizzare nella cache grandi quantità di dati quando il server è temporaneamente occupato con l'archiviazione o l'elaborazione di un sovraccarico negli eventi. Si tratta di un vantaggio per i protocolli, come Syslog, che non supportano la memorizzazione degli eventi nella cache a livello nativo.

I componenti della Gestione servizi di raccolta possono essere sottoposti a bilanciamento del carico installando istanze di questi componenti in computer aggiuntivi. È possibile installare una Gestione servizi di raccolta aggiuntiva eseguendo il programma di installazione su un computer nuovo. Per ulteriori informazioni sull'installazione di Gestione servizi di raccolta, vedere Sezione 3.3.4, “Installazione di Gestione servizi di raccolta Sentinel su SLES o Windows”, a pagina 39.

Utilizzo del servizio di raccolta generico

Durante l'installazione del server Sentinel Rapid Deployment, viene configurato un servizio di raccolta denominato servizio di raccolta generico. Per default, vengono creati 5 eventi al secondo.

Se si desidera aggiungere ulteriori servizi di raccolta nel sistema, è possibile effettuarne il download dal sito Web di Novell (http://support.novell.com/products/sentinel/collectors.html).

3.6.4 Gestione temporale

È necessario connettere il server Sentinel a un server NTP (Network Time Protocol) o a un altro tipo di server dell'orario. Se l'ora di sistema tra i vari computer non è sincronizzata, il motore di correlazione di Sentinel e Active Views non funzioneranno correttamente. Gli eventi provenienti dalle istanze di Gestione servizi di raccolta non saranno considerati in tempo reale e verranno quindi inviati direttamente al database di Sentinel, senza passare dai Control Center e dai motori di correlazione di Sentinel.

Di default, la soglia per i dati in tempo reale è di 120 secondi. Questa soglia può essere modificata impostando opportunamente il valore di `esecurity.router.event.realtime.expiration` nel file `event-router.properties`. L'ora degli eventi di Sentinel viene stabilita sulla base dell'ora del dispositivo attendibile o dell'ora della Gestione servizi di raccolta. L'ora del dispositivo attendibile può essere selezionata durante la configurazione di un servizio di raccolta. L'ora del dispositivo attendibile corrisponde all'ora in cui viene generato il log dal dispositivo e l'ora della Gestione servizi di raccolta corrisponde all'ora del sistema corrente del sistema Gestione servizi di raccolta.

3.7 Autenticazione LDAP

Oltre all'autenticazione del database, Sentinel Sentinel Rapid Deployment supporta l'autenticazione LDAP. È possibile abilitare gli utenti al login in Sentinel Rapid Deployment utilizzando le rispettive credenziali di Novell eDirectory o Microsoft Active Directory configurando il server Sentinel Rapid Deployment per l'autenticazione LDAP.

3.7.1 Panoramica

È possibile configurare il server Sentinel Rapid Deployment per l'autenticazione LDAP su una connessione SSL sicura con o senza l'impiego di ricerche anonime nella directory LDAP.

Nota: se si disabilita la ricerca anonima nella directory LDAP, evitare di configurare il server Sentinel Rapid Deployment per l'uso della ricerca anonima.

- **Ricerca anonima:** quando si creano account utenti LDAP Sentinel Rapid Deployment, è necessario specificare il nome utente della directory, ma non il nome distinto (DN) dell'utente.

  Quando l'utente LDAP esegue il login a Sentinel Rapid Deployment, il server SRD esegue una ricerca anonima nella directory LDAP in base al nome utente specificato, individua il DN corrispondente, quindi autentica il login utente a fronte della directory LDAP utilizzando il DN.

- **Ricerca non anonima:** quando si creano account utenti LDAP Sentinel Rapid Deployment, è necessario specificare sia il nome utente della directory, sia il DN dell'utente.

  Quando l'utente LDAP esegue il login a Sentinel Rapid Deployment, il server SRD autentica il login utente a fronte della directory LDAP utilizzando il DN dell'utente specificato e non esegue alcuna ricerca anonima nella directory LDAP.

  Esiste un ulteriore approccio applicabile solo ad Active Directory. Per ulteriori informazioni, vedere Autenticazione LDAP non anonima utilizzando l'attributo UserPrincipalName in Active Directory.

3.7.2 Prerequisiti

Esportazione del certificato CA del server LDAP

La connessione SSL sicura al server LDAP richiede l'esportazione del certificato CA del server LDAP in un file codificato in base64.

- **eDirectory:** vedere Exporting an Organizational CA's Self-Signed Certificate (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html) (in lingua inglese).

  Per esportare un certificato CA eDirectory in iManager, è necessario installare i plug-in di Novell Certificate Server per iManager.
- **Active Directory:** vedere Abilitazione di LDAP su SSL con un'autorità di certificazione di terze parti (http://support.microsoft.com/kb/321051).

Abilitazione della ricerca anonima nella directory LDAP

Per eseguire l'autenticazione LDAP utilizzando la ricerca anonima, è necessario abilitare questa funzione nella directory LDAP. Per default, la ricerca anonima viene abilitata in eDirectory e disabilitata in Active Directory.

Per abilitare la ricerca anonima nella directory LDAP, fare riferimento a quanto segue:

- **eDirectory:** vedere ldapBindRestrictions nella sezione Attributes on the LDAP Server Object (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html) (in lingua inglese).
- **Active Directory:** è necessario assegnare all'oggetto Utente ACCESSO ANONIMO l'autorizzazione dell'elenco e l'accesso alla lettura appropriati per gli attributi `sAMAccountName` e `objectclass`. Per ulteriori informazioni, vedere Come configurare Active Directory per consentire le query anonime (http://support.microsoft.com/kb/320528).

  Per Windows Server 2003, è necessario eseguire un'ulteriore configurazione. Per ulteriori informazioni, vedere Configuring Active Directory on Windows Server 2003 (http://support.microsoft.com/kb/326690/en-us) (in lingua inglese).

3.7.3 Configurazione del server Sentinel per l'autenticazione LDAP

1. Assicurarsi che i prerequisiti riportati inSezione 3.7.2, “Prerequisiti”, a pagina 45 siano soddisfatti.
2. Eseguire il login al server Sentinel Rapid Deployment come utente `radice`.
3. Copiare il file del certificato CA del server LDAP nella directory `<directory_di_installazione>/config`.
4. Impostare la proprietà e le autorizzazioni del file del certificato come indicato di seguito:

   ```
   chown novell:novell <directory_di_installazione>/config/<file-cert>
   ```

   ```
   chmod 700 <directory_di_installazione>/config/<file-cert>
   ```
5. Passare all'utente `novell`:

   ```
   su - novell
   ```
6. Passare alla directory `<directory_di_installazione>/bin`.
7. Eseguire lo script di configurazione dell'autenticazione LDAP:

```
./ldap_auth_config.sh
```

Lo script esegue un backup dei file di configurazione `auth.login` e `configuration.xml` nella directory `config` come `auth.login.sav` e `configuration.xml.sav` prima di modificarli per l'autenticazione LDAP.

8 Specificare le seguenti informazioni.

Premere Invio per accettare il valore di default oppure specificare un nuovo valore per ignorare quello di default.

- **Ubicazione installazione di Sentinel:** directory di installazione sul server Sentinel.
- **Nome host o indirizzo IP server LDAP:** nome host o indirizzo IP del computer in cui è installato il server LDAP. Il valore di default è localhost. Tuttavia, è consigliato non installare il server LDAP sullo stesso computer in cui è installato il server di Sentinel
- **Porta server LDAP:** numero di porta per una connessione LDAP sicura. Il numero di porta di default è 636.
- **Ricerche anonime nella directory LDAP:** specificare `s` per eseguire le ricerche anonime. Altrimenti specificare `n`. Il valore di default è `s`.

  Se si specifica `n`, completare la configurazione LDAP e seguire la procedura indicata nella sezione "Autenticazione LDAP senza l'esecuzione di ricerche anonime" a pagina 48.
- **Directory LDAP utilizzata:** questo parametro è visualizzato solo se si è specificato "s" per le ricerche anonime. Specificare 1 per Novell eDirectory o 2 per Active Directory. Il valore di default è 1.
- **Sottoalbero LDAP per ricerca utenti:** questo parametro è visualizzato solo se si è specificato "s" per le ricerche anonime. È il sottoalbero della directory che contiene gli oggetti Utente. Di seguito sono riportati alcuni esempi su come specificare il sottoalbero in eDirectory e Active Directory:
  - eDirectory:

    ```
    ou=users,o=novell
    ```

    Nota: per eDirectory, se non si specifica alcun sottoalbero, la ricerca viene eseguita in tutta la directory.
  - Active Directory:

    ```
    CN=users,DC=TESTAD,DC=provo, DC=novell,DC=com
    ```

    Nota: per Active Directory, non è possibile lasciare vuoto il sottoalbero.
- **Nome file del certificato server LDAP:** nome file del certificato CA di eDirectory/ Active Directory copiato al Passo 3.

9 Immettere uno dei seguenti comandi:

- `s` per accettare i valori immessi.
- `n` per immettere nuovi valori.
- `q` per uscire dalla configurazione.

Al completamento della configurazione:

- Il certificato del server LDAP viene aggiunto in un archivio chiavi denominato `<directory_di_installazione>/config/ldap_server.keystore`.
- I file di configurazione `auth.login` e `configuration.xml` nella directory `<directory_di_installazione>/config` vengono aggiornati per abilitare l'autenticazione LDAP.

10 Immettere `s` per riavviare il servizio Sentinel.

Importante: in caso di errori, ripristinare le modifiche apportate ai file di configurazione `auth.login` e `configuration.xml` nella directory `config`:

```
cp -p auth.login.sav auth.login
cp -p configuration.xml.sav configuration.xml
```

---

11 (Condizionale) Se si è specificato `n` per Ricerche anonime nella directory LDAP:, continuare con “Autenticazione LDAP senza l'esecuzione di ricerche anonime” a pagina 48.

Autenticazione LDAP senza l'esecuzione di ricerche anonime

Se durante la configurazione dell'autenticazione LDAP di Sentinel Rapid Deployment si è specificato "n" per le ricerche anonime nella directory LDAP, l'autenticazione LDAP non esegue la ricerca anonima.

Quando si crea un account utente LDAP da Sentinel Control Center, assicurarsi di specificare *DN utente LDAP* per l'autenticazione LDAP non anonima. È possibile utilizzare questo approccio sia per eDirectory sia per Active Directory.

Per ulteriori informazioni, vedere “Creating an LDAP User Account for Sentinel” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

Inoltre, per Active Directory, è possibile utilizzare un approccio alternativo per eseguire l'autenticazione LDAP senza ricerche anonime. Per ulteriori informazioni, vedere Autenticazione LDAP non anonima utilizzando l'attributo UserPrincipalName in Active Directory.

Autenticazione LDAP non anonima utilizzando l'attributo UserPrincipalName in Active Directory

Per Active Directory, è altresì possibile eseguire l'autenticazione LDAP senza ricerche anonime, utilizzando l'attributo userPrincipalName:

1 Assicurarsi che l'attributo userPrincipalName sia impostato a <*sAMAccountName@dominio*> per l'utente Active Directory.

Per ulteriori informazioni, vedere User-Principal-Name Attribute (http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx) (in lingua inglese).

2 Assicurarsi di aver eseguito dal Passo 1 a pagina 46 al Passo 10 a pagina 48 e di aver specificato `n` per “Ricerche anonime nella directory LDAP:” a pagina 47.

3 Nel server Sentinel modificare la sezione `LdapLogin` nel file `<Directory di installazione>/config/auth.login`:

```
LdapLogin {
 com.sun.security.auth.module.LdapLoginModule required
 userProvider="ldap://LDAP server IP:636/DN of the Container that contains
the user objects"
 authIdentity="{USERNAME}@Domain Name"
 userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
 useSSL=true;
 };
```

Ad esempio:

```
LdapLogin {
 com.sun.security.auth.module.LdapLoginModule required
 userProvider="ldap://137.65.151.12:636/DC=Test-
AD,DC=provo,DC=novell,DC=com"
 authIdentity="{USERNAME}@Test-AD.provo.novell.com"
 userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
 useSSL=true;
 };
```

4 Riavviare il servizio Sentinel:

```
/etc/init.d/sentinel stop
```

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

3.7.4 Configurazione di più server LDAP per failover

Per configurare uno o più server LDAP come server di failover per l'autenticazione LDAP:

1 Assicurarsi di aver seguito la procedura indicata dal Passo 2 a pagina 46 al Passo 10 a pagina 48 per configurare il server Sentinel per l'autenticazione LDAP a fronte del server LDAP primario.

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

3 Interrompere il servizio Sentinel.

```
/etc/init.d/sentinel stop
```

4 Passare alla directory `<directory_di_installazione>/config`:

```
cd <directory_di_installazione>/config
```

5 Aprire il file `auth.login` per modificarlo.

```
vi auth.login
```

6 Aggiornare `userProvider` nella sezione LdapLogin per specificare più URL LDAP. Separare ciascun URL con spazi.

Ad esempio:

```
userProvider="ldap://ldap-url1 ldap://ldap-url2"
```

Per Active Directory, assicurarsi che il sottoalbero nell'URL LDAP non sia vuoto.

Per ulteriori informazioni su come specificare più URL LDAP, vedere la descrizione dell'opzione `userProvider` in Class LdapLogin Module (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

7 Salvare le modifiche.

8 Esportare il certificato di ciascun server LDAP di failover e copiare il file del certificato nella directory `<directory_di_installazione>/config` sul server Sentinel.

Per ulteriori informazioni, vedere “Esportazione del certificato CA del server LDAP” a pagina 46.

9 Assicurarsi che vengano impostate la proprietà e le autorizzazioni necessarie del file del certificato per ciascun server LDAP di failover.

```
chown novell:novell <directory_di_installazione>/config/<cert-file>
chmod 700 <directory_di_installazione>/config/<cert-file>
```

10 Aggiungere ciascun certificato del server LDAP di failover all'archivio chiavi `ldap_server.keystore` creato al Passo 8 nella sezione “Configurazione del server Sentinel per l'autenticazione LDAP” a pagina 46.

```
<directory_di_installazione>/jre64/bin/keytool -importcert -noprompt -
trustcacerts -file <certificate-file> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

Sostituire *<file-certificato>* con il nome file del certificato LDAP in formato codificato in base64 e sostituire *<nome_alias>* con il nome alias del certificato da importare.

Importante: assicurarsi di specificare l'alias. Se non è specificato alcun alias, per default keytool considera `mykey` come alias. Quando si importano più certificati in un archivio chiavi senza specificare un alias, keytool riporta un errore a indicare che l'alias esiste già.

---

11 Avviare il servizio Sentinel.

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

La connessione del servizio al server LDAP di failover potrebbe risultare impossibile se il timeout del server Sentinel si verifica prima che questo rilevi che il server LDAP primario è inattivo. Affinché il server Sentinel si connetta al server LDAP di failover senza timeout:

1 Eseguire il login al server Sentinel come utente `radice`.

2 Aprire il file `sysctl.conf` per modificarlo:

```
vi /etc/sysctl.conf
```

3 Assicurarsi che il valore `net.ipv4.tcp_syn_retries` sia impostato a 3. Se la voce non esiste, aggiungere la voce. Salvare il file:

```
net.ipv4.tcp_syn_retries = 3
```

4 Eseguire il comando per applicare le modifiche:

```
/sbin/sysctl -p
/sbin/sysctl -w net.ipv4.route.flush=1
```

5 Impostare il valore di timeout del server Sentinel aggiungendo il parametro `-Desecurity.remote.timeout=60` in `control_center.sh` e `solution_designer.sh` nella directory *<directory_di_installazione>*`/bin`:

control_center.sh:

```
"<directory_di_installazione>/jre/bin/java" $MEMORY -
Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
Desecurity.cache.directory="<directory_di_installazione>/data/
control_center.cache" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<directory_di_installazione>/config/
control_center_log.prop" -
Djava.security.auth.login.config="<directory_di_installazione>/config/
auth.login" $SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Dice.pilots.html4.baseFontFamily="Arial Unicode MS" -
Desecurity.remote.timeout=60 -jar ../lib/console.jar
```

solution_designer.sh:

```
"<directory_di_installazione>/jre/bin/java" -classpath $LOCAL_CLASSPATH
$MEMORY -Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
Dsentinel.installer.jar.location="<directory_di_installazione>/lib/
contentinstaller.jar" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<directory_di_installazione>/config/
solution_designer_log.prop" -
Djava.security.auth.login.config="<directory_di_installazione>/config/
auth.login" $SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Desecurity.cache.directory=../data/solution_designer.cache -
Desecurity.remote.timeout=60
com.esecurity.content.exportUI.ContentPackBuilder
```

3.7.5 Configurazione dell'autenticazione LDAP per più domini Active Directory

Se gli utenti LDAP da autenticare risiedono in più domini Active Directory, è possibile configurare il server Sentinel Rapid Deployment per l'autenticazione LDAP come indicato di seguito:

1. Assicurarsi di aver seguito la procedura indicata dal Passo 2 a pagina 46 al Passo 10 a pagina 48 per configurare il server Sentinel per l'autenticazione LDAP a fronte del controller del dominio Active Directory del primo dominio. Assicurarsi inoltre di aver specificato `n` per "Ricerche anonime nella directory LDAP:" a pagina 47.
2. Eseguire il login al server Sentinel come utente `novell`.
3. Interrompere il servizio Sentinel.

   ```
   /etc/init.d/sentinel stop
   ```
4. Passare alla directory `<directory_di_installazione>/config`:

   ```
   cd <directory_di_installazione>/config
   ```
5. Aprire il file `auth.login` per modificarlo.

   ```
   vi auth.login
   ```
6. Modificare la sezione `LdapLogin` per specificare più URL LDAP separati da spazi.

   Ad esempio:

```
LdapLogin {
        com.sun.security.auth.module.LdapLoginModule required
        userProvider="ldap://<IP of the domain 1 domain controller>:636
ldap://<IP of the domain 2 domain controller>:636"
        authIdentity="{USERNAME}"
        useSSL=true;
};
```

Per ulteriori informazioni su come specificare più URL LDAP, vedere la descrizione dell'opzione `userProvider` in Class LdapLogin Module (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

7 Salvare le modifiche.

8 Esportare il certificato del controller di ciascun dominio e copiare i file del certificato nella directory `<directory_di_installazione>/config` sul server Sentinel.

Per ulteriori informazioni, vedere "Esportazione del certificato CA del server LDAP" a pagina 46.

9 Assicurarsi che vengano impostate la proprietà e le autorizzazioni necessarie dei file del certificato.

```
chown novell:novell <directory_di_installazione>/config/<cert-file>
chmod 700 <directory_di_installazione>/config/<cert-file>
```

10 Aggiungere ciascun certificato all'archivio chiavi `ldap_server.keystore` creato al Passo 8 nella sezione "Configurazione del server Sentinel per l'autenticazione LDAP" a pagina 46.

```
<directory_di_installazione>/jre64/bin/keytool -importcert -noprompt -
trustcacerts -file <certificate-file> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

Sostituire `<file-certificato>` con il nome file del certificato LDAP in formato codificato in base64 e sostituire `<nome_alias>` con il nome alias del certificato da importare.

Importante: assicurarsi di specificare l'alias. Se non è specificato alcun alias, per default keytool considera `mykey` come alias. Quando si importano più certificati in un archivio chiavi senza specificare un alias, keytool riporta un errore a indicare che l'alias esiste già.

---

11 Avviare il servizio Sentinel.

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

3.7.6 Login utilizzando le credenziali dell'utente LDAP

Una volta configurato il server Sentinel per l'autenticazione LDAP, in Sentinel Control Center è possibile creare account utenti LDAP di Sentinel. Per ulteriori informazioni sulla creazione di account utenti LDAP, vedere "Creating an LDAP User Account for Sentinel" in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

Dopo aver creato l'account utente LDAP, è possibile eseguire il login a interfaccia Web di Sentinel Rapid Deployment, Sentinel Control Center e Sentinel Solution Designer utilizzando il nome utente e la password LDAP.

Nota: per modificare una configurazione LDAP esistente, eseguire di nuovo lo script `ldap_auth_config` e specificare i nuovi valori per i parametri.

3.8 Aggiornamento del codice di licenza da un codice di valutazione a un codice di produzione

Se si acquista il prodotto dopo un periodo di valutazione, seguire la procedura descritta sotto per aggiornare la chiave di licenza in modo da non dover ripetere l'installazione:

1. Eseguire il login al computer in cui è installato Sentinel Rapid Deployment come utente del sistema operativo amministratore Sentinel (l'utente di default è `novell`).
2. Al prompt dei comandi, passare alla directory `<directory_di_installazione>/bin`.
3. Immettere il seguente comando:

   ```
   ./softwarekey.sh
   ```
4. Specificare 1 per impostare la chiave primaria. Premere Invio.
5. Immettere la nuova chiave di licenza valida e seguire le istruzioni visualizzate per uscire dopo l'aggiornamento della chiave di licenza.

Upgrade di Sentinel Rapid Deployment

4

Questa sezione contiene le informazioni sull'upgrade di una versione esistente di Sentinel Rapid Deployment alla patch più recente.

Nota: questa patch è applicabile solo all'installazione di Sentinel Rapid Deployment a 64 bit. Se si applica la patch su un sistema demo a 32 bit, l'installazione non sarà funzionale.

4.1 Prerequisiti

- Assicurarsi che sul sistema di cui si esegue l'upgrade sia già installato Sentinel 6.1 Rapid Deployment SP1.
- Assicurarsi che i lavori di Gestione dati Sentinel siano abilitati in modo che la partizione attuale online non raggiunga mai P_MAX. Se raggiunge P_MAX e si aggiungono le partizioni manualmente, l'avvio di Sentinel Control Center risulta impossibile.

4.2 Installazione della patch sul server

1. Eseguire il login come utente `novell` al server in cui si desidera installare la patch.

   Prima di installare la patch, assicurarsi di eseguire il backup del database, della cartella di configurazione e della cartella dei dati di Sentinel utilizzando i seguenti comandi:

   Database di Sentinel:

   ```
   tar -cf backup.tar <directory_di_installazione>/3rdparty/postgresql/
   database_files
   tar -cf backupdata.tar <directory_di_installazione>/3rdparty/postgresql/
   data
   ```

   Cartella di configurazione:

   ```
   tar -cf backupconfig.tar <directory_di_installazione>/config
   ```

   Cartella dei data:

   ```
   tar -cf backupdata.tar <directory_di_installazione>/data
   ```

   Per ulteriori informazioni sui comandi, vedereFile system level back up (http://www.postgresql.org/docs/8.1/static/backup-file.html) (in lingua inglese) nel sito Web di PostgreSQL.

2. Eseguire il backup della configurazione di Gestione origine eventi (ESM) e creare la relativa esportazione.

   Per ulteriori informazioni, vedere “Exporting a Configuration” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

3. Effettuare il download del programma di installazione della patch relativo a Sentinel Rapid Deployment dalla pagina Novell Patch Finder (http://download.novell.com/patch/finder/).
4. Copiare il pacchetto del programma di installazione di cui si è effettuato il download in una directory temporanea.
5. Interrompere i servizi Sentinel:

   ```
   sentinel.sh stop
   ```
6. Specificare il seguente comando per estrarre i file nel pacchetto del programma di installazione:

   ```
   unzip <nomefile_installazione>
   ```

   Sostituire <*nomefile_installazione*> con il nome effettivo del file del programma di installazione.
7. Passare alla directory in cui sono stati estratti i file del programma di installazione:

   ```
   cd <directory_name>
   ```

   Sostituire <*nome_directory*> con il nome effettivo della directory in cui sono stati estratti i file.
8. Specificare il seguente comando per applicare la patch al server, quindi seguire le istruzioni visualizzate:

   ```
   ./service_pack.sh
   ```

   Una volta completata l'installazione, i servizi Sentinel vengono avviati automaticamente.
9. Applicare la patch su tutti i computer in cui sono in esecuzione Gestione servizi di raccolta, applicazioni client o entrambi.

4.3 Upgrade di Gestione servizi di raccolta e applicazioni client

4.3.1 Esecuzione dell'upgrade della Gestione dei servizi di raccolta

Linux

1. Eseguire il login al computer di Gestione servizi di raccolta Sentinel Rapid Deployment come utente `root`.
2. Effettuare il download del programma di installazione della patch relativo a Sentinel Rapid Deployment dalla pagina Novell Patch Finder (http://download.novell.com/patch/finder/).
3. Copiare il file del programma di installazione di cui si è effettuato il download in una directory temporanea.
4. Specificare il seguente comando per estrarre i file nel pacchetto compresso del programma di installazione:

   ```
   unzip <nomefile_installazione>
   ```

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

5 Passare alla directory in cui sono stati estratti i file del programma di installazione:

```
cd <directory_name>
```

Sostituire <*nome_directory*> con il nome effettivo della directory in cui sono stati estratti i file del programma di installazione.

6 Interrompere i servizi di Gestione servizi di raccolta.

```
<directory_di_installazione>/bin/sentinel.sh stop
```

7 Eseguire il programma di installazione Service Pack, quindi seguire le istruzioni visualizzate:

```
./service_pack.sh
```

Una volta completata l'installazione, i servizi di Gestione servizi di raccolta vengono avviati automaticamente.

Windows

1 Eseguire il login al computer di Gestione servizi di raccolta Sentinel Rapid Deployment come utente admin.

2 Effettuare il download del programma di installazione della patch relativo a Sentinel Rapid Deployment dalla pagina Novell Patch Finder (http://download.novell.com/patch/finder/).

3 Copiare il file del programma di installazione in una directory temporanea.

4 Estrarre i file nel pacchetto del programma di installazione.

5 Interrompere i servizi di Gestione servizi di raccolta.

```
<directory_di_installazione>\bin\sentinel.bat stop
```

6 Selezionare la directory in cui sono stati estratti i file del programma di installazione.

7 Effettuare una delle seguenti operazioni per eseguire il programma di installazione:

- Fare doppio clic sul file `service_pack.bat`, quindi seguire le istruzioni visualizzate.
- Da un prompt dei comandi, eseguire il file `service_pack.bat`, quindi seguire le istruzioni visualizzate.

Una volta completata l'installazione, i servizi di Gestione servizi di raccolta vengono avviati automaticamente.

4.3.2 Upgrade delle applicazioni client

- “Linux” a pagina 57
- “Windows” a pagina 58

Linux

1 Eseguire il login come utente `root` al computer in cui sono in esecuzione le applicazioni client di Novell Sentinel Rapid Deployment.

2 Effettuare il download del programma di installazione della patch relativo a Sentinel Rapid Deployment dalla pagina Novell Patch Finder (http://download.novell.com/patch/finder/).

3 Copiare il pacchetto del programma di installazione di cui si è effettuato il download in una directory temporanea.

4. Specificare il seguente comando per estrarre i file nel pacchetto del programma di installazione:

   `unzip <nomefile_installazione>`

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

5. Passare alla directory in cui sono stati estratti i file del programma di installazione:

   `cd <directory_name>`

   Sostituire <*nome_directory*> con il nome effettivo della directory in cui sono stati estratti i file.

6. Eseguire il programma di installazione, quindi seguire le istruzioni visualizzate:

   `./service_pack.sh`

Windows

1. Eseguire il login come amministratore nel computer in cui sono in esecuzione le applicazioni client di Novell Sentinel Rapid Deployment.
2. Effettuare il download del programma di installazione della patch relativo a Sentinel Rapid Deployment dalla pagina Novell Patch Finder (http://download.novell.com/patch/finder/).
3. Copiare il file del programma di installazione di cui si è effettuato il download in una directory temporanea.
4. Estrarre i file nel pacchetto del programma di installazione.
5. Selezionare la directory in cui sono stati estratti i file del programma di installazione.
6. Effettuare una delle seguenti operazioni per eseguire il programma di installazione:
   - Fare doppio clic sul file `service_pack.bat`, quindi seguire le istruzioni visualizzate.
   - Dal prompt dei comandi, eseguire il file `service_pack.bat`, quindi seguire le istruzioni visualizzate.

Considerazioni sulla sicurezza per Sentinel Rapid Deployment

5

In questa sezione vengono fornite istruzioni specifiche su come installare, configurare e aggiornare in modo sicuro Novell Sentinel Rapid Deployment.

5.1 Protezione avanzata

5.1.1 Protezione avanzata pronta per l'uso

- Tutte le porte non necessarie sono disattivate.
- Quando è possibile, è in ascolto una porta di servizio solo per le connessioni locali e non consente le connessioni remote.
- I file sono installati con i privilegi minimi in modo che solo un numero ridotto di utenti sia in grado di leggere i file.
- Le password di default non sono consentite.
- I rapporti sul database vengono eseguiti per l'utente dotato solo delle autorizzazioni di selezione sul database.
- Tutte le interfacce Web richiedono HTTPS.
- È stata effettuata una scansione delle vulnerabilità dell'applicazione e tutti i potenziali problemi sulla sicurezza sono stati risolti.
- Per default, tutte le comunicazioni nella rete utilizzano SSL e sono configurate per l'autenticazione.
- Le password degli account utenti sono cifrate per default quando vengono memorizzate nel file system o nel database.

5.1.2 Come rendere sicuri i dati di Sentinel Rapid Deployment

Vista la natura altamente riservata dei dati contenuti in Sentinel Rapid Deployment, il computer deve essere fisicamente protetto e collocato in un'area sicura della rete. Per raccogliere dati da origini eventi esterne alla rete sicura, utilizzare un'istanza remota di Gestione servizi di raccolta. Per ulteriori informazioni sulle istanze di Gestione servizi di raccolta, vedere “Sezione 3.3, “Installazione di Gestione servizi di raccolta e applicazioni client”, a pagina 35”.

5.2 Protezione delle comunicazioni nella rete

La comunicazione tra i vari componenti di Sentinel Rapid Deployment ha luogo attraverso la rete e in tutto il sistema sono utilizzati diversi tipi di protocolli di comunicazione.

5.2.1 Comunicazione tra processi del server Sentinel

I processi del server Sentinel includono DAS Core, DAS Binary, motore di correlazione, Gestione servizi di raccolta e il server Web. Essi comunicano utilizzando ActiveMQ.

La comunicazione tra questi processi server avviene per default su SSL tramite il bus messaggi ActiveMQ. Per configurare SSL, specificare le informazioni seguenti in `<directory_di_installazione>/configuration.xml`:

```
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
```

Per ulteriori informazioni sulla configurazione di certificati server e client personalizzati, vedere “Processes” in the *Sentinel Rapid Deployment User Guide* (in lingua inglese).

5.2.2 Comunicazione tra il server Sentinel e le applicazioni client di Sentinel

Le applicazioni client di Sentinel come Sentinel Control Center (SCC), Gestione dati Sentinel (Sentinel Data Manager, SDM) e Solution Designer utilizzano per default le comunicazioni SSL tramite il server proxy SSL.

Per abilitare la comunicazione tra il server Sentinel e SCC, SDM e Solution Designer quando vengono eseguiti tutti come applicazioni client sul server, specificare le informazioni seguenti in `<directory_di_installazione>/configuration.xml`:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory">
   <transport type="ssl">
    <ssl host="localhost" keystore="<directory_di_installazione>/config/
.proxyClientKeystore" port="10013" usecacerts="false"/>
   </transport>
  </strategy>
```

Per abilitare la comunicazione tra il server Sentinel e SCC, SDM e Solution Designer eseguiti attraverso Web Start, la strategia di comunicazione è definita sul server nel file `<directory_di_installazione>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml`, come indicato di seguito:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory" >
   <transport type="ssl">
    <ssl host="127.0.0.1" port="10013" keystore="./.novell/sentinel/
.proxyClientKeystore" />
   </transport>
  </strategy>
```

Per ulteriori informazioni sulla configurazione di certificati server e client personalizzati, vedere "Processes" in the *Sentinel Rapid Deployment User Guide* (in lingua inglese).

5.2.3 Comunicazione tra server e database

Il protocollo utilizzato per la comunicazione tra il server e il database è definito dal driver JDBC. Alcuni driver sono in grado di cifrare la comunicazione con il database.

Sentinel Rapid Deployment utilizza il driver PostgreSQL (`postgresql-<versione>.jdbc3.jar`) fornito nella pagina di download di PostgreSQL (http://jdbc.postgresql.org/download.html) per la connessione al database PostgreSQL, che è un'implementazione Java (Tipo IV). Questo driver supporta la cifratura per la comunicazione dei dati. Per configurare la cifratura per la comunicazione dei dati, fare riferimento a PostgreSQL Encryption Options (http://www.postgresql.org/docs/8.1/static/encryption-options.html) (in lingua inglese).

Nota: l'attivazione della cifratura influisce sulle prestazioni del sistema. Pertanto, la comunicazione del database non viene cifrata per default. Tuttavia, ciò non costituisce un problema per la sicurezza in quanto la comunicazione tra il database e il server ha luogo nell'interfaccia di rete di loopback e non è esposta alla rete aperta.

5.2.4 Comunicazione tra istanze di Gestione servizi di raccolta e origini eventi

È possibile configurare Sentinel Rapid Deployment per raccogliere i dati in modo sicuro da varie origini eventi. Tuttavia, la raccolta dei dati sicura dipende da protocolli specifici supportati dall'origine eventi. Ad esempio, è possibile configurare Check Point LEA, Syslog e i connettori di controllo per la cifratura delle rispettive comunicazioni con le origini eventi.

Per ulteriori informazioni sulle funzioni di sicurezza che è possibile abilitare, fare riferimento alla documentazione del fornitore dell'origine evento e del connettore disponibile nel sito Web dei plug-in di Novell Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

5.2.5 Comunicazione con i browser Web

Il server Web è configurato per default per comunicare tramite HTTPS. Per ulteriori informazioni, vedere la documentazione di Tomcat (http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html).

5.2.6 Comunicazione tra il database e gli altri client

È possibile configurare il database SIEM PostgreSQL in modo da consentire la connessione da qualsiasi computer client utilizzando Gestione dati Sentinel o qualsiasi applicazione di terze parti, come Pgadmin.

Per consentire la connessione di Gestione dati Sentinel da qualsiasi computer client, aggiungere la riga seguente al file `<directory_di_installazione>/3rdparty/postgresql/data/pg_hba.conf`:

```
host    all         all         0.0.0.0/0             md5
```

Se si desidera limitare le connessioni client che è possibile eseguire e connettersi al database attraverso Gestione dati Sentinel, sostituire la riga indicata sopra con l'indirizzo IP dell'host. La riga seguente in `pg_hba.conf` indica a PostgreSQL di accettare connessioni dal computer locale, in modo che l'esecuzione di Gestione dati Sentinel sia consentita solo sul server.

```
host all all 127.0.0.1/32 md5
```

Per limitare le connessioni da altri computer client è possibile aggiungere ulteriori voci `host`.

5.3 Protezione di utenti e password

5.3.1 Utenti del sistema operativo

Installazione del server

L'installazione del server Sentinel Rapid Deployment crea un utente del sistema e un gruppo che sono proprietari dei file installati nella `<directory_di_installazione>`. Se l'utente non esiste, viene creato e la rispettiva home directory è impostata a `<directory_di_installazione>`. Per aumentare al massimo la sicurezza, quando si crea un nuovo utente la password corrispondente non viene impostata per default. Se si desidera eseguire il login al sistema come utente creato durante l'installazione, al termine di quest'ultima è necessario impostare una password per l'utente.

Installazione di Gestione servizi di raccolta

Il livello di sicurezza degli utenti del sistema può variare a seconda del sistema operativo sul quale è installato Gestione servizi di raccolta.

Linux: il programma di installazione richiede all'utente di specificare il nome dell'utente del sistema proprietario dei file installati e l'ubicazione in cui creare la relativa home directory. Per default, l'utente del sistema è `esecadm`; questo nome utente di sistema può tuttavia essere modificato. Se l'utente non esiste viene creato insieme alla relativa home directory. Per aumentare al massimo la sicurezza, quando si crea un nuovo utente la password corrispondente non viene impostata durante l'installazione. Se si desidera eseguire il login al sistema come utente, al termine dell'installazione è necessario impostare una password per l'utente. Il gruppo di default è `esec`.

Durante l'installazione del client, se l'utente esiste già, il programma di installazione non chiede nuovamente di indicare l'utente. Questo comportamento è simile a quello della disinstallazione o reinstallazione del software. Tuttavia, è possibile che il programma di installazione richieda di specificare di nuovo l'utente.

1. Eliminare l'utente e il gruppo creati al momento della prima installazione
2. Eliminare le variabili di ambiente ESEC_USER da `/etc/profile`

Windows: non viene creato alcun utente.

Le norme relative alle password per gli utenti del sistema sono definite dal sistema operativo in uso.

5.3.2 Utenti dell'applicazione e del database Sentinel

Tutti gli utenti dell'applicazione Sentinel Rapid Deployment sono utenti del database nativo e le relative password sono protette mediante procedure seguite dalla piattaforma del database nativo. Questi utenti hanno accesso in sola lettura ad alcune tabelle del database, pertanto possono eseguire interrogazioni sul database.

Il programma di installazione crea e configura un database PostgreSQL con i seguenti utenti:

- **admin:** l'utente admin è l'amministratore che esegue il login a tutte le applicazioni Sentinel.
- **dbauser:** dbauser viene creato come utente con privilegi avanzati in grado di gestire il database. La password per dbauser viene impostata al momento dell'installazione del server Sentinel Rapid Deployment. Questa password è memorizzata in `<home directory utente>/.pgpass`. Il sistema segue le policy password del database PostgreSQL. Per ulteriori informazioni, vedere Sezione 5.3.3, “Applicazione di una policy password per gli utenti”, a pagina 64.
- **appuser:** appuser è l'utente privo di privilegi avanzati che viene utilizzato dalle applicazioni Sentinel per la connessione al database. Per default, appuser utilizza una password generata casualmente durante l'installazione e che viene memorizzata e cifrata nei file XML (`das_core.xml`, `das_binary.xml` e `advisor_client.xml`) nella directory <*directory_di_installazione*>/config. È possibile modificare la password per appuser mediante l'utility `<directory_di_installazione>/bin/dbconfig`. Per ulteriori informazioni, vedere “DAS Container Files” in *Sentinel Rapid Deployment Reference Guide* (in lingua inglese).

Nota: un utente di database PostgreSQL è inoltre proprietario dell'intero database, comprese le tabelle del database del sistema. Per default, l'utente del database PostgreSQL è impostato al valore NOLOGIN, in modo che nessuno possa eseguire il login come utente PostgreSQL.

5.3.3 Applicazione di una policy password per gli utenti

Sentinel Rapid Deployment utilizza meccanismi basati su standard per semplificare la procedura di applicazione delle policy password.

Il programma di installazione crea e configura un database PostgreSQL con i seguenti utenti:

dbauser: il proprietario del database (utente amministratore del database). La password viene impostata durante il processo di installazione.

appuser: è l'utente dell'applicazione utilizzato da Sentinel Rapid Deployment per il login al database. La password viene generata in modo casuale durante il processo di installazione ed è destinata al solo uso interno.

admin: è possibile utilizzare le credenziali dell'amministratore per eseguire il login all'interfaccia Web di Sentinel Rapid Deployment. La password viene impostata durante il processo di installazione.

Per default, le password utenti sono memorizzate nel database PostgreSQL incorporato in Sentinel Rapid Deployment. In PostgreSQL è disponibile l'opzione che consente di utilizzare alcuni meccanismi di autenticazione basati su standard, come descritto nella sezione Client Authentication (http://www.postgresql.org/docs/8.3/static/client-authentication.html) (in lingua inglese) della documentazione di PostgreSQL.

L'uso di questi meccanismi influisce su tutti gli account utenti di Sentinel Rapid Deployment, inclusi gli utenti dell'applicazione Web e degli account utilizzati solo da servizi back end, come `dbauser` e `appuser`.

Un'opzione più semplice consiste nell'utilizzare una directory LDAP per autenticare gli utenti dell'applicazione Web. Per abilitare questa opzione sul server Sentinel Rapid Deployment, vedere Sezione 3.7, “Autenticazione LDAP”, a pagina 45. Questa opzione non ha effetto sugli account utilizzati come servizi back end, la cui autenticazione avviene sempre con PostgreSQL a meno che non si modifichino le impostazioni di configurazione PostgreSQL.

È possibile applicare la policy password in modo efficace in Sentinel Rapid Deployment utilizzando tali meccanismi basati su standard e quelli esistenti nell'ambiente, come la directory LDAP.

5.4 Protezione dei dati Sentinel

Importante: vista la natura altamente riservata dei dati contenuti nel server Sentinel, il computer deve essere fisicamente protetto e collocato in un'area sicura della rete. Per raccogliere dati da origini eventi esterne alla rete sicura, utilizzare un'istanza remota di Gestione servizi di raccolta.

Per alcuni componenti è necessario memorizzare le password affinché siano disponibili quando il sistema deve connettersi a una risorsa quale il database o un'origine eventi. In questo caso, quando la password è memorizzata, essa viene prima cifrata per evitare accessi non autorizzati al relativo testo non cifrato.

Anche quando la password è cifrata, è necessario assicurarsi che l'accesso ai dati della password memorizzata sia protetto per evitarne l'esposizione. È possibile, ad esempio, fare in modo che le autorizzazioni sui file che contengono dati riservati non siano leggibili da utenti non autorizzati.

FILE

advisor_client.xml

Credenziali per il database

Le credenziali per il database sono memorizzate nel file <*directory_di_installazione*>/config/server.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Credenziali per Advisor

```
<obj-component id="DownloadComponent">
          <class>esecurity.ccs.comp.advisor.feed.NewAdvClientDownload</class>
      <property name="advisor.downloadfrom.url">https://secure-www.novell.com/
sentinel/advisor/advisordata</property>
      <property name="username">admin</property>
      <!-- Set the password (encrypted) using the adv_change_password script -
->
      <property name="password">jqhlWIX8HD6GDHVX9FApWg==</property>
<property name="compression.enabled">true</property>
      <!--
        Set the following properties to connect through an HTTP proxy.
       Set the proxy password (encrypted) using the adv_change_password script
(make a
        copy of the script and add "-x" to the java cmd line to set the proxy
password
        instead of the advisor password.
      -->
      <!--
      <property name="proxy_host"></property>
      <property name="proxy_port"></property>
      <property name="proxy_username"></property>
      <property name="proxy_password"></property>
      -->
        </obj-component>
```

Configuration.xml

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.Ac
tiveMQStrategyFactory" name="ActiveMQ">
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
    </strategy>
```

das_binary.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

das_core.xml

```
 <class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

In alcune tabelle del database sono memorizzati password e certificati. I dati riservati sono cifrati e memorizzati nelle tabelle riportate di seguito e occorre limitare l'accesso a queste tabelle.

- **evt_src:** dati colonna evt_src_config
- **evt_src_collector:** colonne: evt_src_collector_props
- **evt_src_grp (dubbio):** colonne: evt_src_default_config
- **md_config:** colonna : dati
- **integrator_config:** colonna: integrator_properties
- **md_view_config:** colonna : view_data
- **esec_content:** colonna: content_context, content_hash
- **esec_content_grp_content:** colonne: content_hash
- **sentinel_plugin:** colonne: content_pkg, file_hash

Sentinel Rapid Deployment memorizza sia i dati di configurazione che quelli relativi agli eventi. Questi dati vengono memorizzati nelle seguenti ubicazioni:

Componenti	Percorso dei dati di configurazione	Percorso dei dati degli eventi
Server Sentinel Rapid Deployment	Tabelle del database e file system (*<directory_di_installazione>*/config) Queste informazioni di configurazione includono il database cifrato, l'origine eventi, integratori e password.	Database (tabelle EVENTS, CORRELATED_EVENTS e EVT_SMRY_, AUDIT_RECORD) e file system in *<directory_di_installazione>*/data/eventdata e <*directory_di_installazione*>/data/raw data È possibile archiviare i dati relativi agli eventi nel file system nell'ambito del processo di gestione delle partizioni.
Motore di correlazione	File system (*<directory_di_installazione>*/config). L'unica informazione di configurazione riservata è la coppia di chiavi client utilizzata per la connessione al bus messaggi.	correlation_engine.cache
DAS Core	*<Directory_di_installazione>*/config	das_core.cache

Componenti	Percorso dei dati di configurazione	Percorso dei dati degli eventi
DAS Binary	<*Directory_di_installazione*>/config	I dati relativi agli eventi possono essere memorizzati nella cache se il database è inattivo. das_binary.cache
Gestione servizi di raccolta	File system (<*directory_di_installazione*>/config). L'unica informazione di configurazione riservata è la password utente di Gestione servizi di raccolta utilizzata per la connessione al bus messaggi.	È possibile memorizzare nella cache del file system i dati relativi agli eventi durante condizioni di errore, quali l'inattività del bus messaggi o l'overflow degli eventi. I dati relativi agli eventi vengono memorizzati nella directory <*directory_di_installazione*>/data/collector_mgr.cache.
Applicazioni client	File system (*directory_di_installazione*/config). Nei file di configurazione delle applicazioni client non sono memorizzate informazioni riservate. Le applicazioni client possono, ad esempio, esportare dati ESM in un file system locale. Il file esportato contiene password cifrate, se queste sono presenti nella configurazione delle origini eventi esportate. Sebbene le password siano cifrate, l'autorizzazione all'esportazione di ESM deve essere concessa solo a utenti affidabili.	Nessuno

5.5 Backup delle informazioni

- È necessario eseguire regolarmente il backup degli eventi. I supporti di backup devono essere conservati in una struttura protetta fuori sede.
- Eseguire il backup dei dati del sistema. Per ulteriori informazioni, vedere "Backup and Restore Utility" in *Sentinel Rapid Deployment User Guide* (in lingua inglese).
- Nel caso di dati riservati, utilizzare uno dei metodi seguenti per cifrare il backup dei dati:
  - Cifrare i dati stessi se l'applicazione con cui vengono creati supporta la cifratura. La cifratura dei dati è supportata, ad esempio, da prodotti database e strumenti di terze parti. Utilizzare un software di backup che sia in grado di cifrare i dati durante l'esecuzione del backup. Questo metodo pone problemi di prestazioni e gestibilità, soprattutto per la gestione delle chiavi di cifratura.
  - Utilizzare un'applicazione per la cifratura che consenta di cifrare i supporti di backup con dati riservati durante l'esecuzione del backup.
- Se i supporti vengono trasferiti e conservati fuori sede, è opportuno avvalersi di un'azienda specializzata nella spedizione e nella conservazione. Verificare che i nastri siano contrassegnati con codici a barre per garantirne la tracciabilità, che vengano conservati nel rispetto dell'ambiente e che la loro gestione sia affidata a un'azienda con una solida reputazione nel campo specifico.

- Caricamento dei certificati di recupero. Per default, il servizio Novell Sentinel non è configurato per l'agente di recupero. Durante la configurazione del server tramite YaST, verificare che il percorso dell'agente di recupero sia configurato. Il percorso deve contenere l'elenco di certificati che il servizio può caricare, tra cui gli utenti potranno selezionare quelli desiderati.

  Per ulteriori informazioni, vedere "Certificate Management for Sentinel 6.1 Rapid Deployment Server" in *Sentinel Rapid Deployment Reference Guide* (in lingua inglese).

  YaST contiene moduli per la gestione di base dei certificati X.509, che implica soprattutto la creazione di autorità di certificazione, autorità di certificazione secondarie e relativi certificati. Per ulteriori informazioni sulla gestione e l'aggiornamento dei certificati, vedere Managing X.509 Certification (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html) in *SUSE Linux Enterprise Server 10 Installation and Administration Guide* (http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html) (in lingua inglese).

5.6 Protezione del sistema operativo

- Sentinel Rapid Deployment è supportato in SUSE Linux Enterprise Server (SLES) 10 SP3 o versioni successive. Per ulteriori informazioni su come rendere sicuro un computer SLES, vedere la documentazione di SUSE Linux Enterprise Server 10 (http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html).
- Accesso sicuro al server Sentinel Rapid Deployment con un firewall. Se il server Sentinel è accessibile dall'esterno della rete aziendale, è opportuno utilizzare un firewall per impedire l'accesso diretto da parte di intrusi.

  Abilitare le seguenti porte nel firewall:

Componenti	Porta
ActiveMQ	61616
PostgreSQL	5432
Tomcat	8443
Porta client proxy di Sentinel Control Center	10013
Client di fiducia con proxy	10014
server_gateway_interno e gateway_interno Utilizzati tra motore e manager	5556
server_router_interno e client_router_interno Utilizzati tra client e server del router degli eventi	5558
Porta di ascolto degli eventi configurata in `config/collector_mgr.properties` come "`esecurity.agentmanager.event.port`"	35000

Nota: le porte contrassegnate con un asterisco potrebbero essere diverse se già in uso al momento dell'installazione. Se erano già uso al momento dell'installazione, sostituirne i numeri con quelli richiesti al momento dell'installazione.

Per ulteriori informazioni sull'abilitazione di un firewall in SLES 10, vedere Configuring Firewalls with YaST (http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html) in *SLES 10 Administration Guide* (in lingua inglese).

5.7 Visualizzazione degli eventi di revisione Sentinel

Sentinel Rapid Deployment genera eventi di revisione per numerose azioni eseguite dagli utenti e internamente per le attività del sistema. È possibile visualizzare tali eventi in Active Views oppure è possibile accedervi mediante ricerche o rapporti. Tuttavia, per visualizzare gli eventi del sistema è necessario disporre delle autorizzazioni appropriate.

Per ulteriori informazioni, vedere "System Events for Sentinel" in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

5.8 Utilizzo di un certificato CA

È possibile sostituire un certificato firmato da se stessi con un certificato firmato da una delle principali autorità di certificazione, ad esempio VeriSign, Thawte o Entrust. È anche possibile sostituire un certificato firmato da se stessi con un certificato firmato da un'autorità di certificazione meno nota, ad esempio interna alla propria organizzazione o azienda.

Per ulteriori informazioni, vedere "Certificate Management for Sentinel 6.1 Rapid Deployment Server" in *Sentinel Rapid Deployment Reference Guide* (in lingua inglese).

Test delle funzionalità di Sentinel Rapid Deployment

6

Sentinel Rapid Deployment è installato con un servizio di raccolta generico che può essere utilizzato per testare numerose funzionalità di base del sistema. È possibile utilizzare questo servizio di raccolta per testare Active Views, la creazione di casi, regole di correlazioni e rapporti.

6.1 Verifica dell'installazione di Rapid Deployment

La procedura riportata di seguito descrive come testare il sistema Sentinel Rapid Deployment e i risultati previsti. Anche se gli eventi visualizzati non sono gli stessi, i risultati dovrebbero essere simili a quelli riportati di seguito.

A livello di base, questi test consentono di verificare se:

- I servizi Sentinel sono attivi e in esecuzione.
- La comunicazione tramite il bus messaggi è funzionante.
- È in corso l'invio di eventi di revisione interni.
- Gli eventi possono essere inviati da Gestione servizi di raccolta.
- Gli eventi vengono inseriti nel database e possono essere recuperati mediante un rapporto.
- I casi possono essere creati e visualizzati.
- Le regole vengono valutate e gli eventi correlati vengono attivati dal Motore di correlazione.
- Gestione dati Sentinel è connesso al database ed è in grado di leggere le informazioni sulle partizioni.

Se uno qualsiasi di questi test ha esito negativo, esaminare il log di installazione e gli altri file di log e, se necessario, rivolgersi al Supporto tecnico Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup).

Per eseguire il test dell'installazione:

1. Eseguire il login a un'interfaccia Web di Sentinel Rapid Deployment.

   Per ulteriori informazioni, vedere “Accessing the Novell Sentinel Web Interface” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).
2. Selezionare la pagina di ricerca e cercare eventi interni. Dovrebbero essere restituiti uno o più eventi.

   Ad esempio, per cercare gli eventi interni nell'intervallo di gravità 3-5, selezionare *Includi eventi sistema*, quindi immettere *grav.:[DA 3 A 5]* nel campo *Cerca*.

Per ulteriori informazioni su come eseguire la ricerca, fare riferimento a “Running an Event Search” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

La funzione di ricerca non è abilitata per default in SP2. Tuttavia, se si desidera abilitarla, fare riferimento a “Enabling the Search Option in Web User Interface” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

3 Selezionare la pagina dei rapporti, specificare i parametri, quindi eseguire un rapporto.

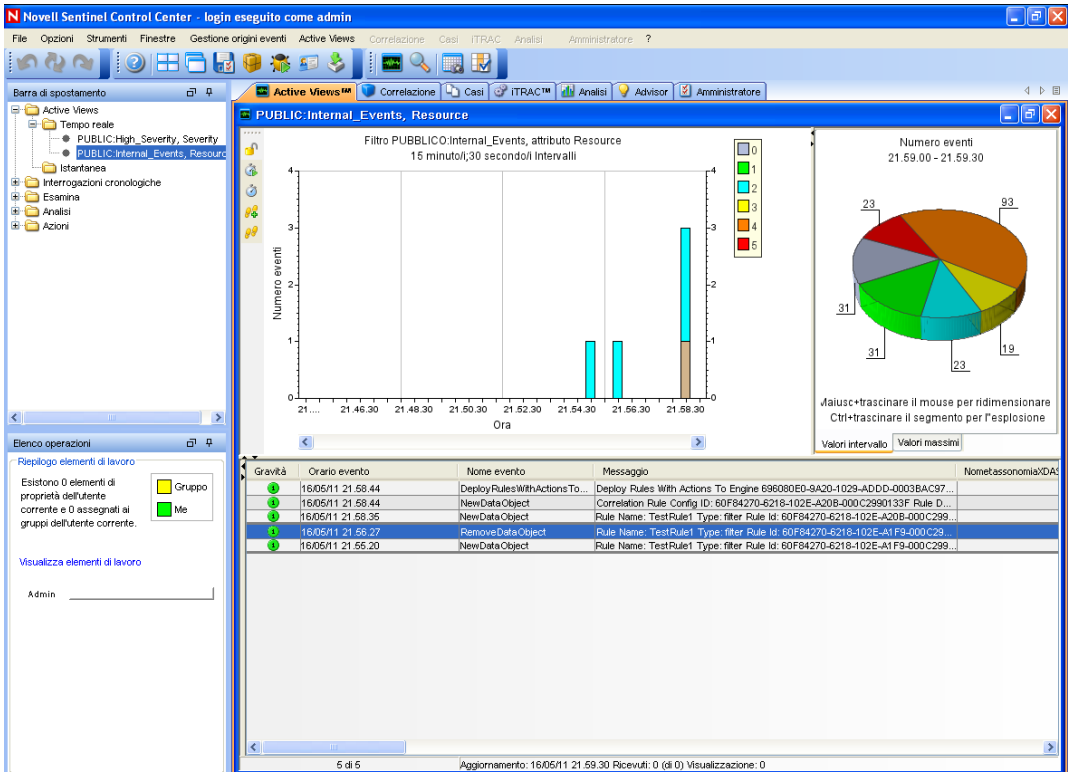
Ad esempio, fare clic sul pulsante *Esegui* accanto a Configurazione eventi di base Sentinel, specificare i parametri desiderati e fare clic su *Esegui*.

Per ulteriori informazioni, fare riferimento a “Running Reports” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

4 Nella pagina Applicazioni fare clic su *Avvia Sentinel Control Center*.

5 Eseguire il login al sistema mediante l'utente amministrativo di Sentinel specificato durante l'installazione (admin per default).

Si apre Sentinel Control Center in cui è possibile visualizzare la scheda *Active Views* con gli eventi filtrati in base ai filtri pubblici *Eventi_Interni* e *Gravità_Alta*.



6 Accedere al menu *Gestione origini eventi*, quindi selezionare *Visualizzazione in diretta*.

7 Nella vista grafica, fare clic con il pulsante destro del mouse su *origine evento 5 eps*, quindi selezionare *Avvia*.

8 Chiudere la finestra Visualizzazione in diretta di Gestione origini eventi.

9 Fare clic sulla scheda *Active Views*.

È possibile visualizzare la finestra attiva intitolata PUBBLICA: Gravità_Alta, Gravità. L'avvio del servizio di raccolta e la visualizzazione dei dati in questa finestra potrebbero richiedere alcuni minuti.

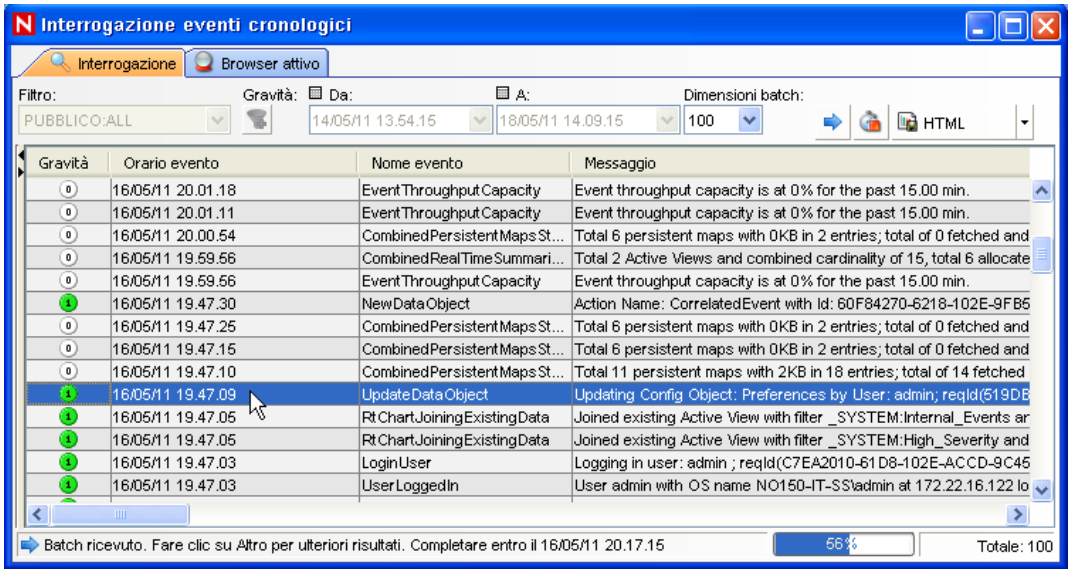
10 Sulla barra degli strumenti fare clic sul pulsante *Interrogazione eventi*. Viene visualizzata la finestra Interrogazione eventi cronologici.

11 Nella finestra Interrogazione eventi cronologici, fare clic sulla freccia verso il basso *Filtro* per selezionare il filtro. Selezionare il filtro *Pubblica: Tutto*.

12 Scegliere un periodo di tempo in cui il servizio di raccolta è stato attivo. Selezionare l'intervallo di date negli elenchi a discesa *Da* e *A*.

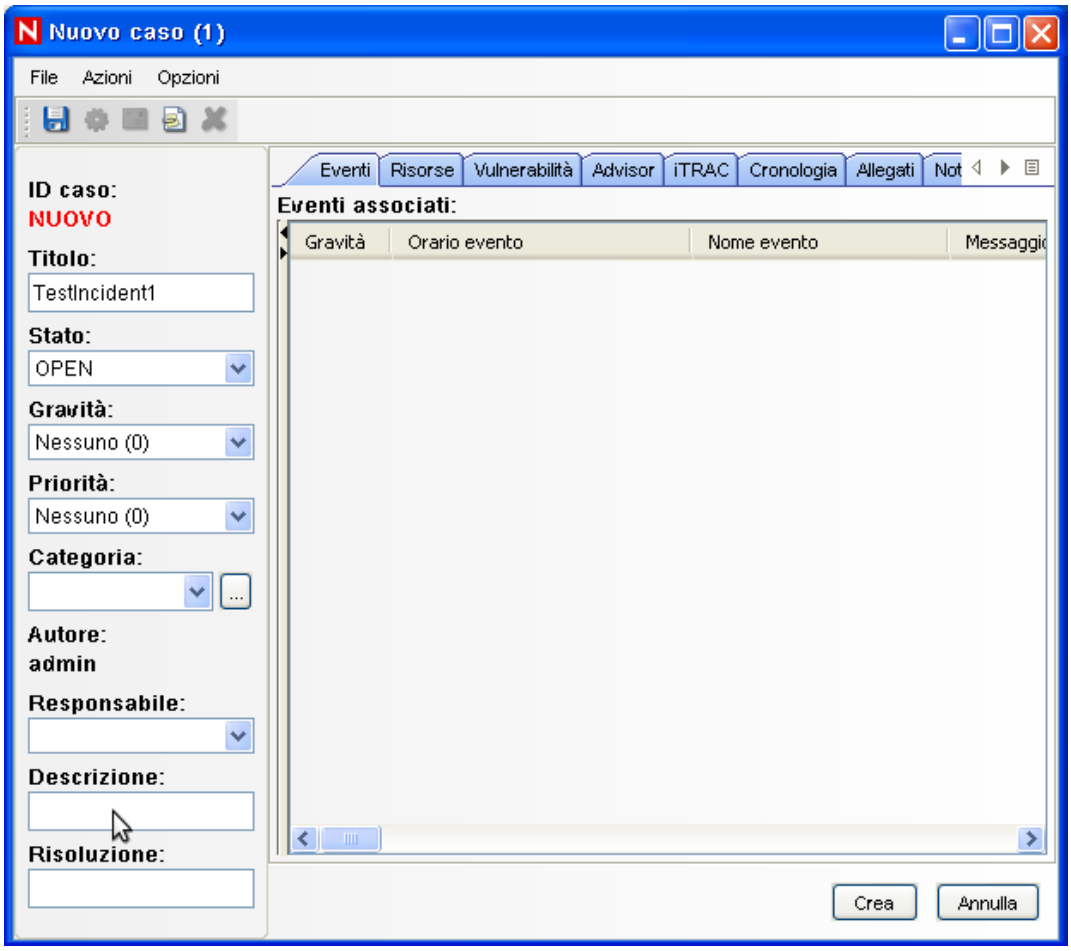
13 Selezionare la dimensione batch.

14 Fare clic sull'icona della lente d'ingrandimento per eseguire l'interrogazione.



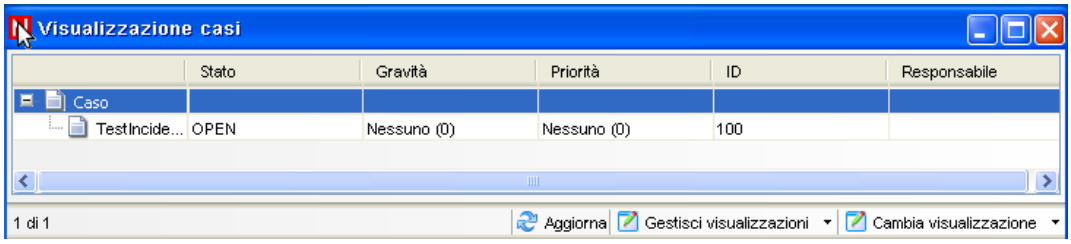
15 Tenere premuto CTRL o MAIUSC, quindi selezionare più eventi dalla finestra Interrogazione eventi cronologici.

16 Fare clic con il pulsante destro del mouse sulla finestra, quindi selezionare *Crea caso* per visualizzare la finestra Nuovo caso.

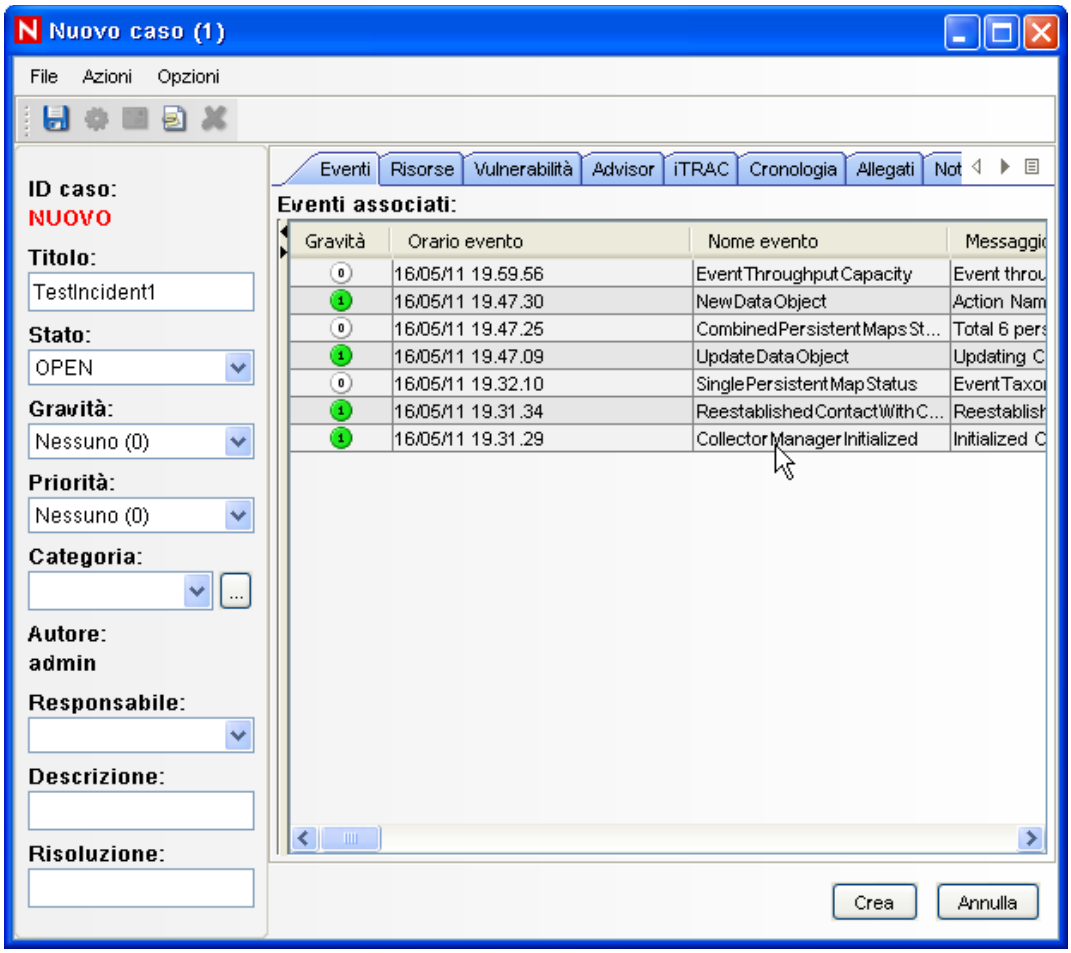


17 Assegnare il nome CasoTest1 e fare clic su *Crea*. Quando viene visualizzata la notifica relativa alla riuscita dell'operazione, fare clic su *Salva*.

18 Fare clic sulla scheda *Caso* per visualizzare il caso appena creato in Gestione visualizzazione caso.



19 Fare doppio clic sul caso per visualizzare gli eventi.



20 Chiudere la finestra Caso.

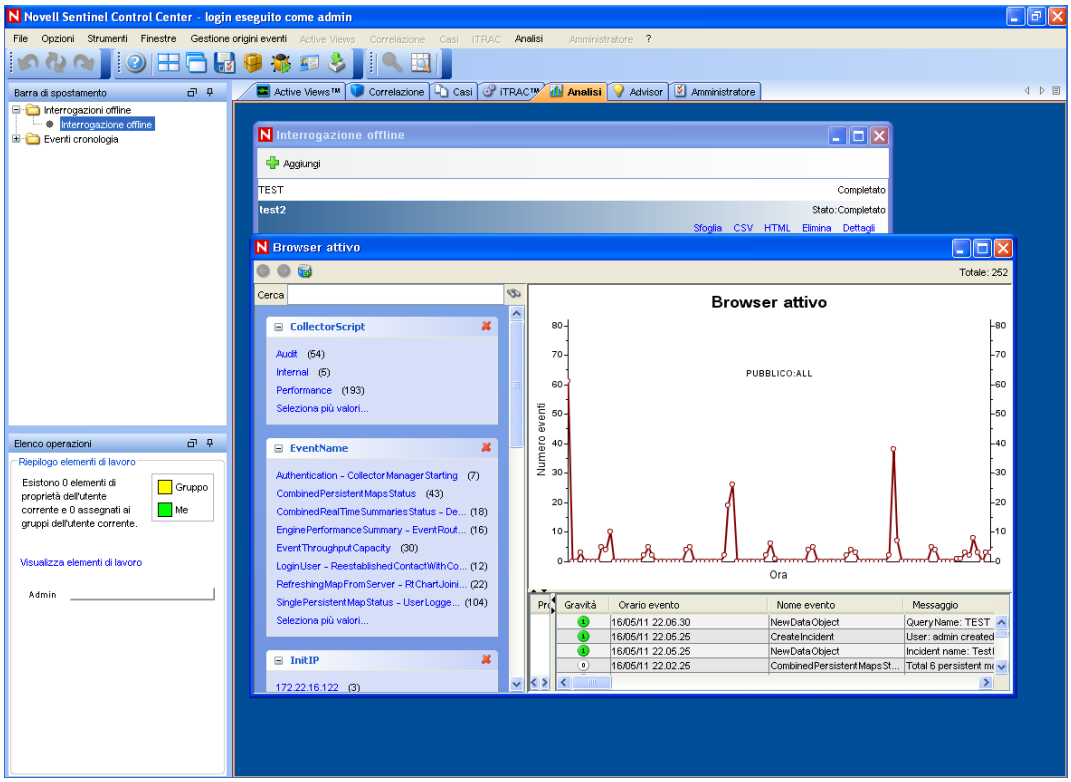
21 Fare clic sulla scheda *Analisi*.

22 Fare clic su *interrogazioni offline* nel menu *Analisi* o nel riquadro di spostamento.

23 Nella finestra Interrogazione offline fare clic su *Aggiungi*.

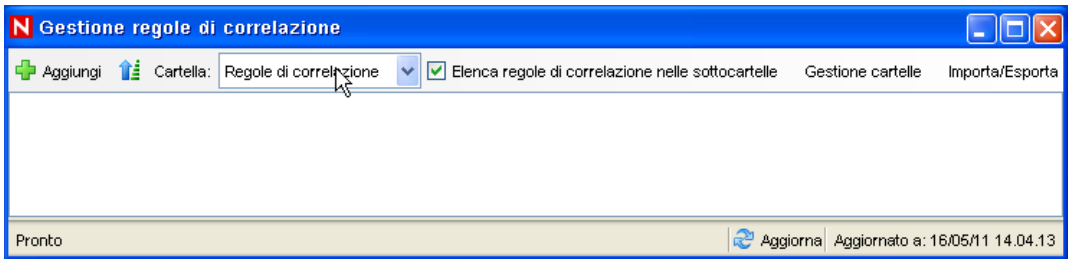
24 Specificare un nome, selezionare un filtro, un periodo di tempo, quindi fare clic su *OK*.

25 Fare clic su *Sfoglia* per visualizzare l'elenco di eventi e i dettagli associati nella finestra Browser attivo.

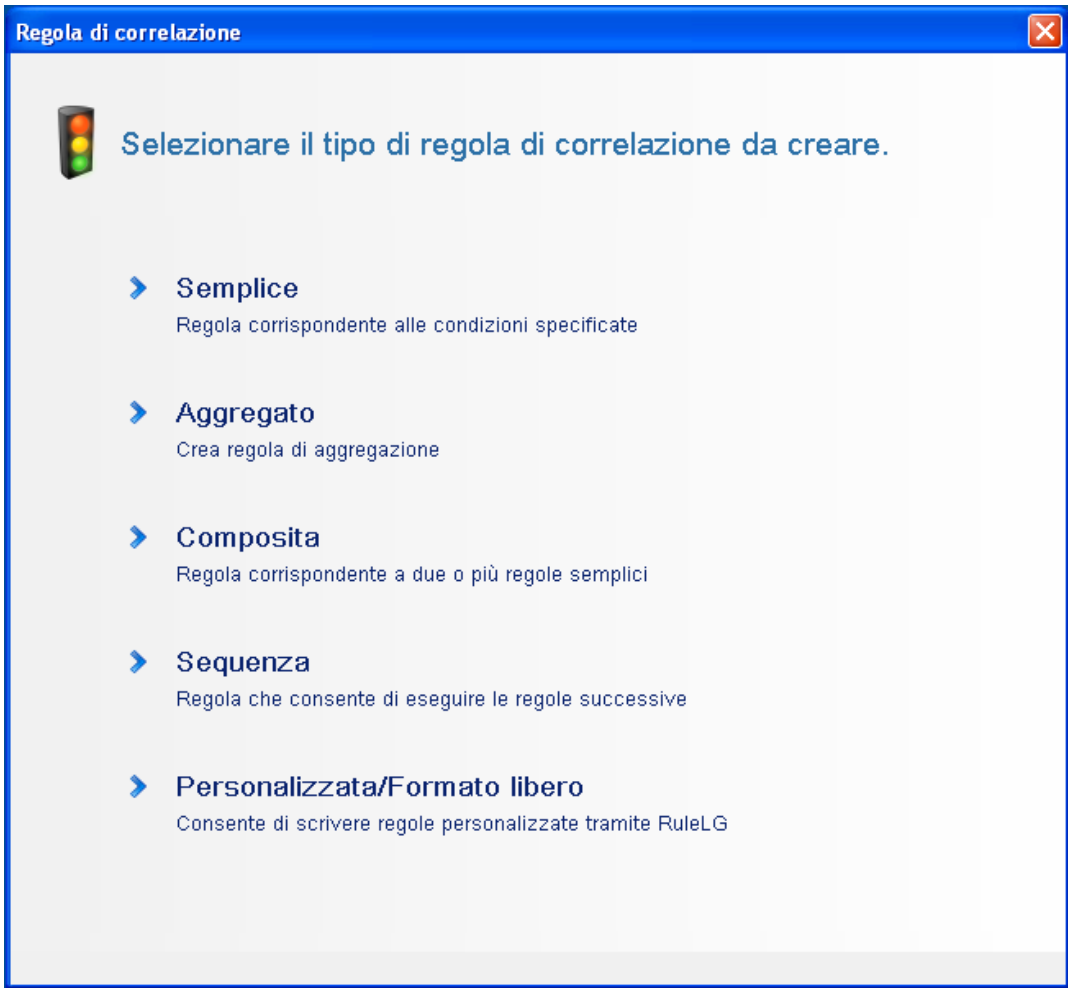


È possibile visualizzare i dettagli relativi a servizio di raccolta, IP di destinazione, gravità, porta del servizio di destinazione e risorsa.

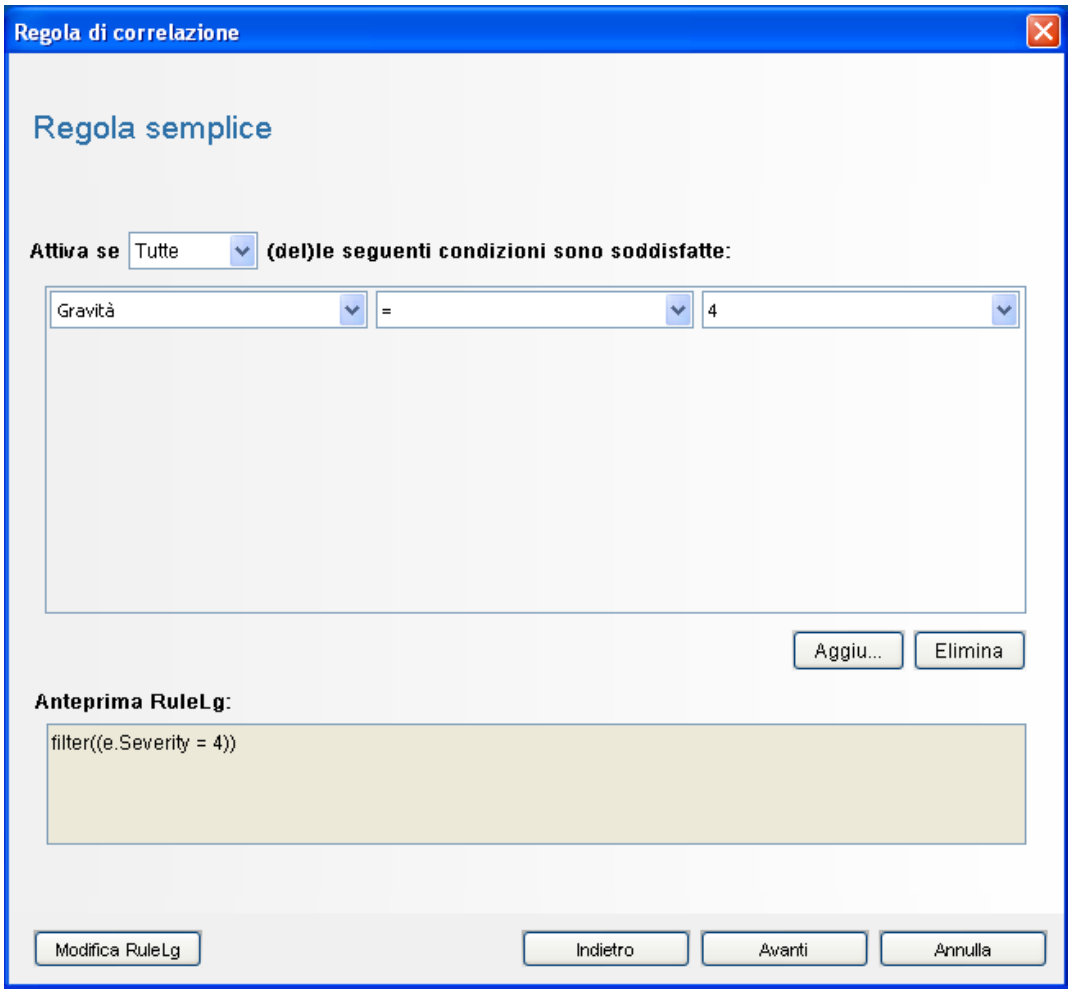
26 Selezionare la scheda *Correlazione*. Viene visualizzata Gestione regole di correlazione.



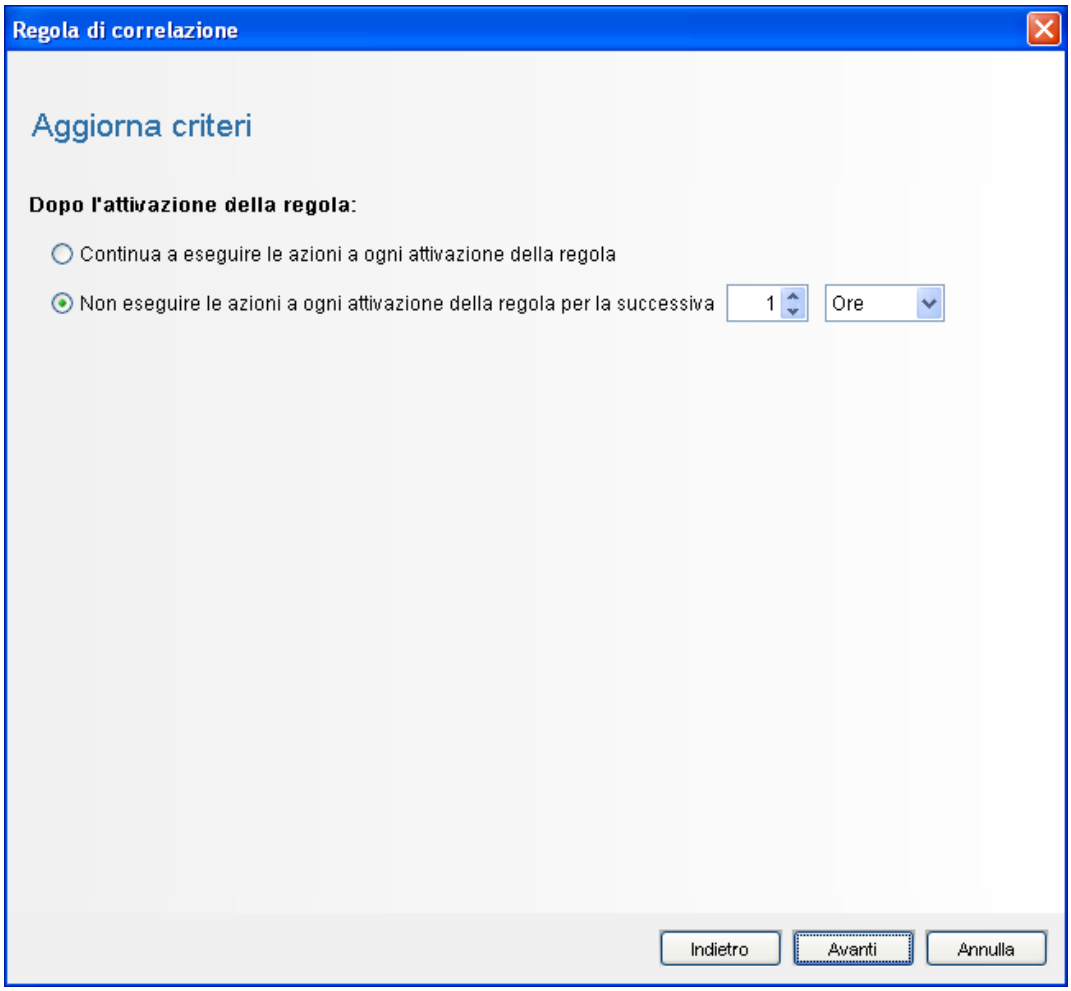
27 Fare clic su *Aggiungi*. Viene visualizzata la procedura guidata delle regole di correlazione



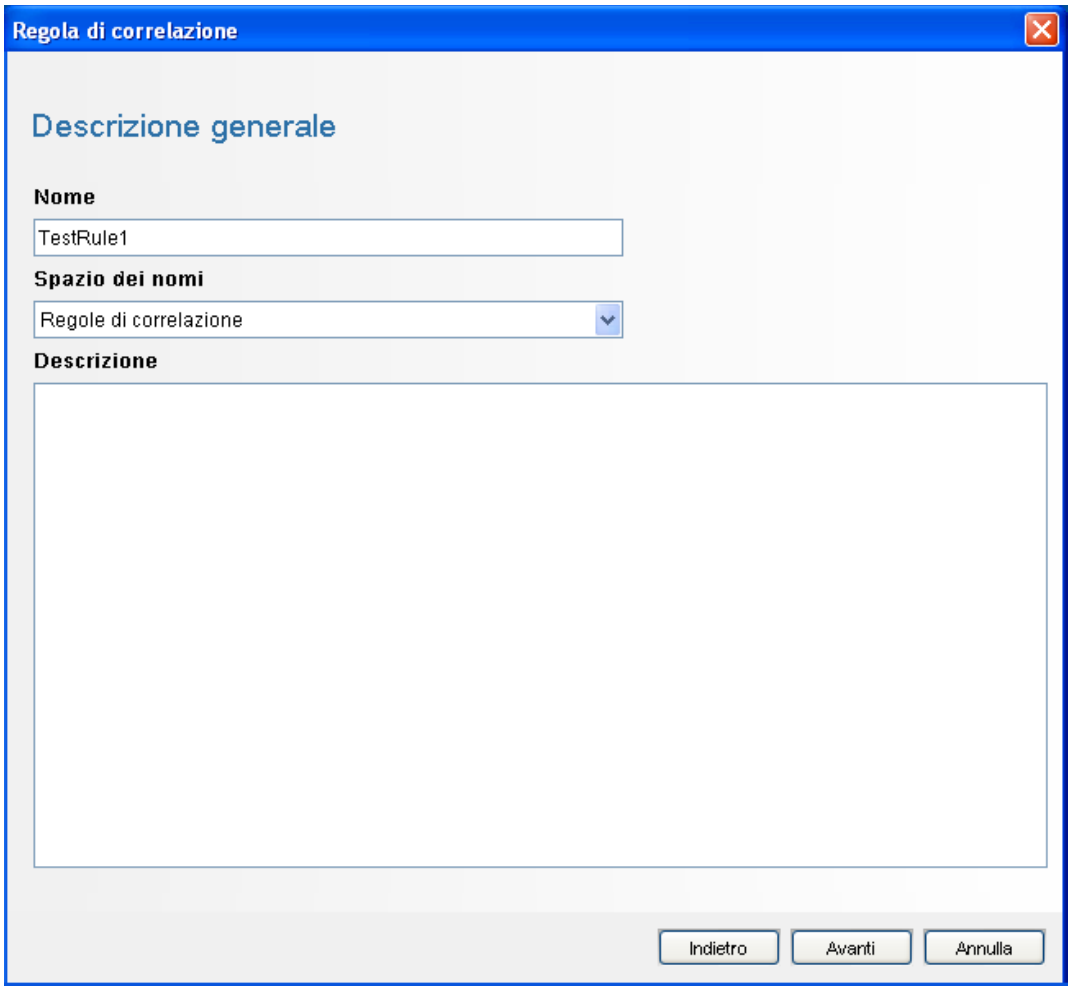
28 Fare clic su *Semplice*. Viene visualizzata la finestra Regola semplice.



29 Utilizzare i menu a discesa per impostare i criteri su Gravità=4, quindi fare clic su *Avanti*. Viene visualizzata la finestra Aggiorna criteri.



30 Selezionare *Nessuna azione ogni volta che si genera la regola*, utilizzare il menu a discesa per impostare il periodo di tempo a 1 minuto, quindi fare clic su *Avanti*. Viene visualizzata la finestra Descrizione generale.



31 Assegnare alla regola il nome *RegolaTest1*, immettere una descrizione e fare clic su *Avanti*.

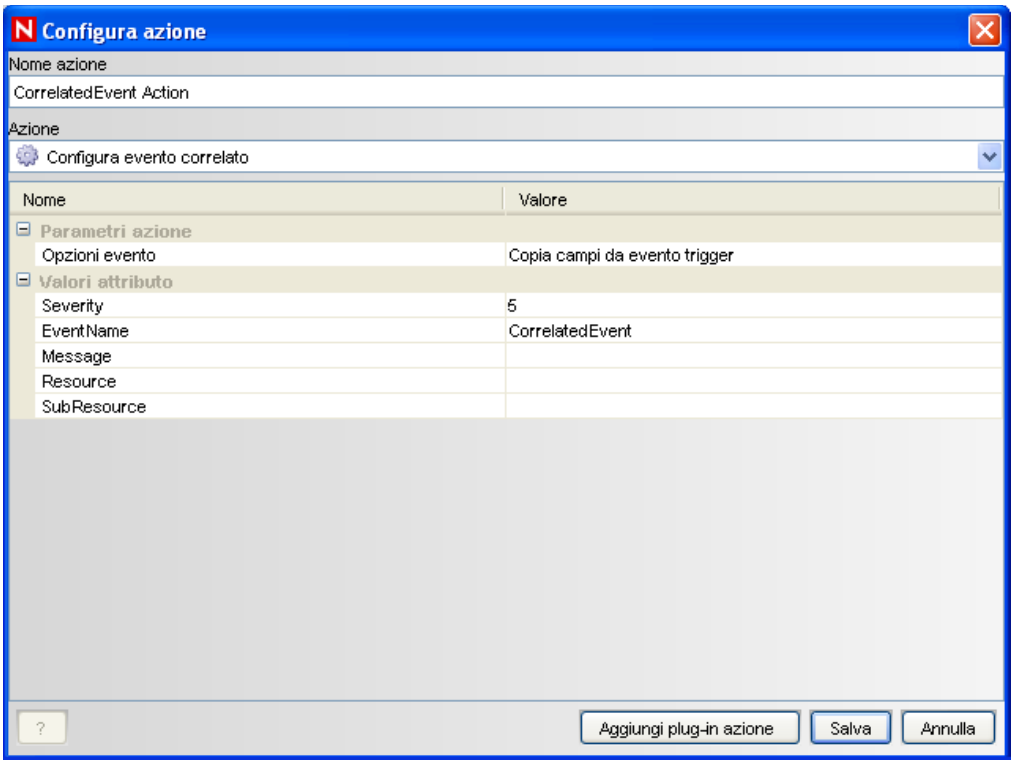
32 Selezionare *No, non creare un'altra regola* e fare clic su *Avanti*.

33 Creare un'azione da associare alla regola creata:

33a Eseguire una delle seguenti operazioni:

- Selezionare *Strumenti* > *Gestione azioni* > *Aggiungi*.
- Nella finestra Distribuisci regola, fare clic su *Aggiungi azione*. Per ulteriori informazioni, vedere da Passo 34 a Passo 35 a pagina 81.

Viene visualizzata la finestra Configura azione



33b In questa finestra specificare quanto segue:

- Specificare il nome dell'azione come Azione EventoCorrelato.
- Selezionare *Configura evento correlato* dall'elenco a discesa *Azione*.
- Impostare le *Opzioni evento*.
- Impostare la *Gravità* a 5.
- Specificare il *NomeEvento*, come EventoCorrelato.
- Specificare un messaggio, se necessario.

Per ulteriori informazioni sulla creazione di un'azione, vedere “Creating Actions” in *Sentinel Rapid Deployment User Guide* (in lingua inglese).

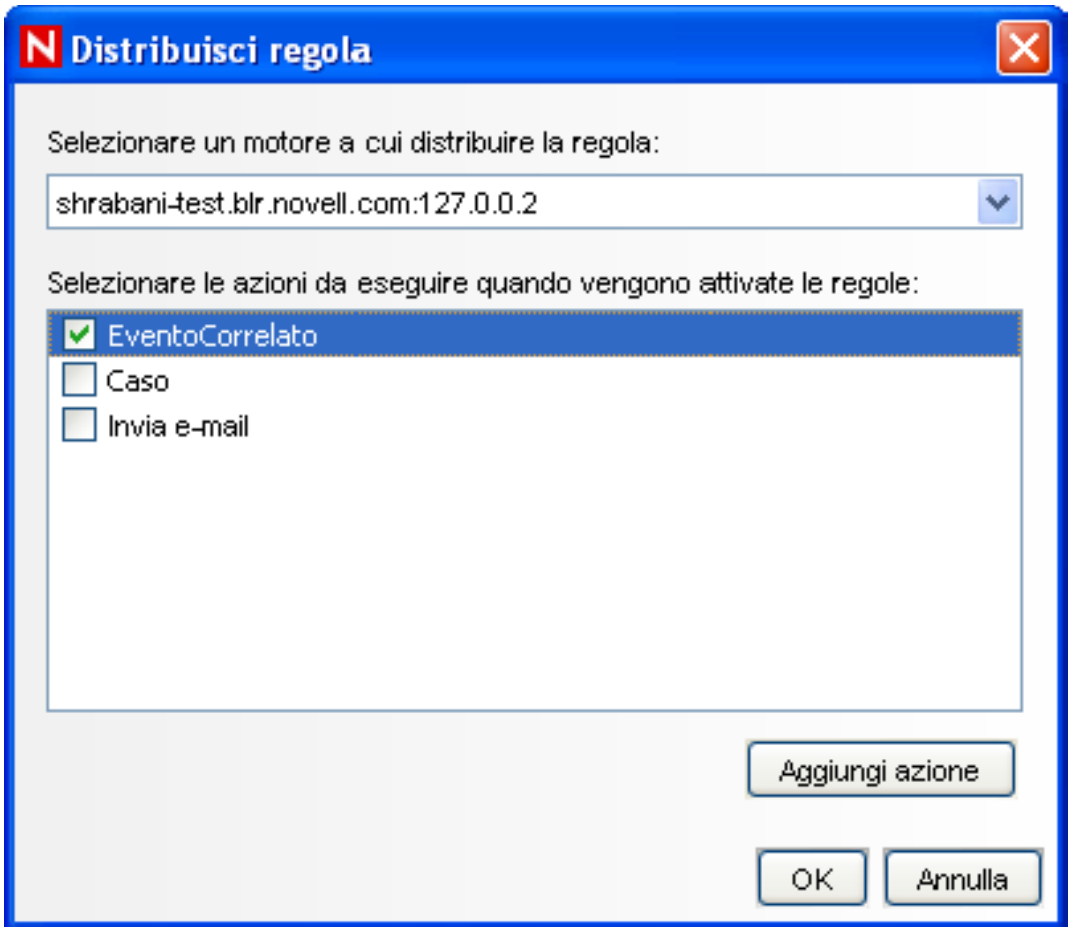
33c Fare clic su *Salva*.

34 Aprire la finestra Gestione regole di correlazione.

35 Selezionare una regola, quindi fare clic sul collegamento *Distribuisci regole*. Viene visualizzata la finestra Distribuisci regola.

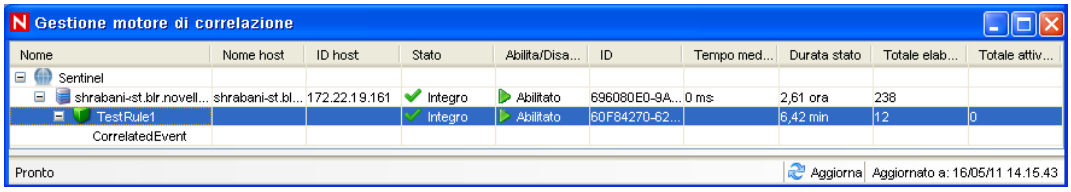
36 Nella finestra Distribuisci regola, selezionare il motore di distribuzione della regola.

37 Selezionare l'azione creata al Passo 33 a pagina 80 da associare alla regola, quindi fare clic su *OK*.



38 Selezionare *Gestione motore di correlazione*.

In Motore di correlazione è possibile visualizzare l'avvenuta distribuzione e abilitazione della regola.



39 Attivare un evento di gravità 4, come un'autenticazione non riuscita, per generare la regola di correlazione.

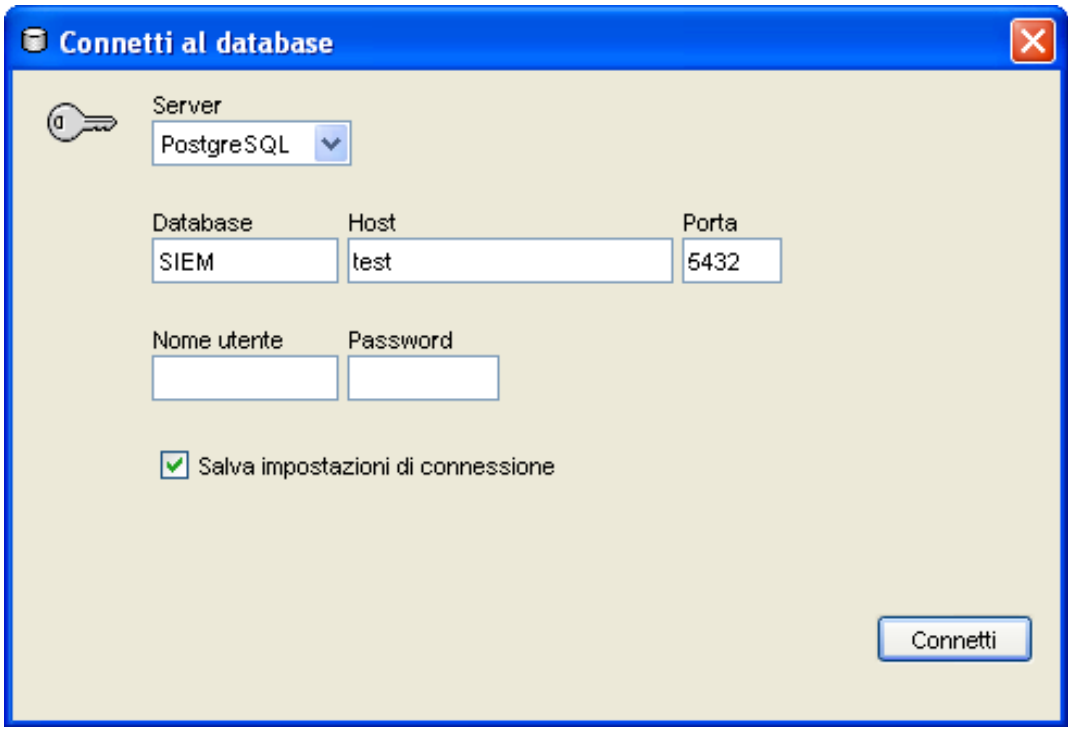
Ad esempio, aprire una finestra di login di Sentinel Control Center, quindi specificare credenziali utente errate per generare un evento simile.

40 Fare clic sulla scheda *Active Views*, quindi verificare se l'evento correlato è stato generato.

41 Chiudere Sentinel Control Center.

42 Nella pagina Applicazioni fare clic su *Avvia Gestione dati Sentinel*.

43 Eseguire il login a Gestione dati Sentinel utilizzando l'utente amministrativo del database specificato durante l'installazione (dbauser per default).



44 Fare clic su ogni scheda per verificare che sia possibile accedervi.

45 Chiudere la Gestione dati Sentinel.

Se tutti questi passaggi sono stati portati a termine senza errori, è stata completata la verifica di base dell'installazione del sistema Sentinel.

6.2 Pulizia successiva al test

Dopo avere completato la verifica del sistema, è necessario rimuovere gli oggetti creati per i test.

1 Eseguire il login al sistema mediante l'utente amministrativo di Sentinel specificato durante l'installazione (admin per default).

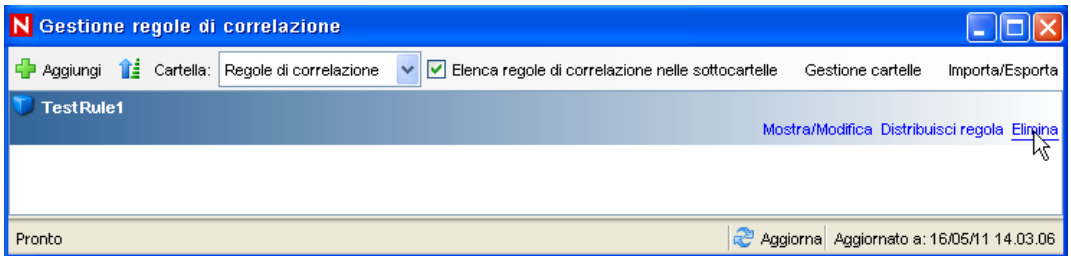
2 Selezionare la scheda *Correlazione*.

3 Aprire Gestione motore di correlazione.

4 Fare clic con il pulsante destro del mouse su *RegolaTest1* in Gestione motore di correlazione, quindi selezionare *Annulla distribuzione*.

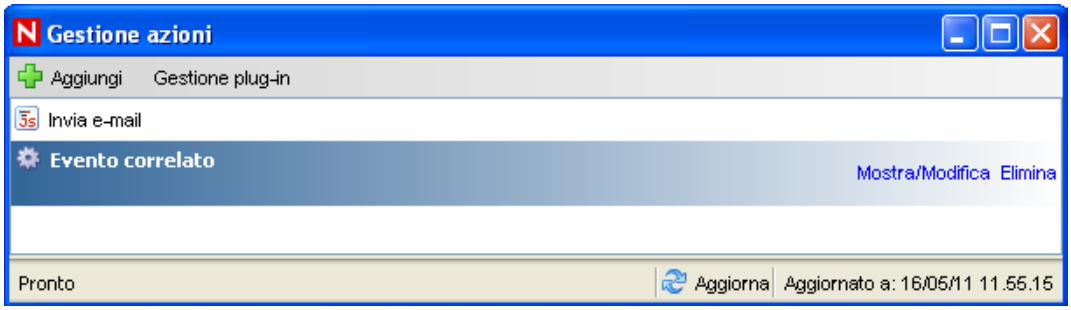
5 Aprire Gestione motore di correlazione.

6 Selezionare *RegolaTest1*, quindi fare clic su *Elimina*.



7 Selezionare *Strumenti* > *Gestione azioni* per visualizzare la finestra Gestione azioni.

8 Selezionare l'azione *EventoCorrelato*, fare clic su *Elimina*, quindi su *Sì* per confermare l'operazione.



9 Accedere al menu *Gestione origini eventi*, quindi selezionare *Visualizzazione in diretta*.

10 Nella gerarchia grafica delle origini di eventi, fare clic con il pulsante destro del mouse su *Servizio di raccolta generale*, quindi selezionare *Interrompi*.

11 Chiudere la finestra Gestione origini eventi.

12 Fare clic sulla scheda *Casi*.

13 Aprire Gestione visualizzazione caso.

14 Selezionare *CasoTest1*, fare clic con il pulsante destro del mouse e selezionare *Elimina*.

6.3 Uso dei dati reali

Per iniziare a lavorare con dati reali, è necessario importare e configurare servizi di raccolta adatti all'ambiente in uso, configurare regole personalizzate, creare workflow iTRAC e così via. Per ulteriori informazioni, vedere *Sentinel Rapid Deployment User Guide* (in lingua inglese). I pacchetti soluzione di Sentinel consentono di iniziare a lavorare rapidamente. Per ulteriori dettagli, vedere la pagina del contenuto di Sentinel (http://support.novell.com/products/sentinel/sentinel61.html) (in lingua inglese).

Disinstallazione di Sentinel Rapid Deployment 7

7.1 Disinstallazione del server Sentinel Rapid Deployment

1. Eseguire il login come utente `radice`.
2. Passare alla directory `setup`.

   `cd <directory_di_installazione>/setup`
3. Eseguire lo script `uninstall.sh` per disinstallare il server Sentinel Rapid Deployment:

   `./uninstall.sh`

   Lo script invia un messaggio per informare che Sentinel Rapid Deployment sarà completamente rimosso.
4. Specificare se si desidera mantenere o rimuovere l'utente durante la disinstallazione del server Sentinel Rapid Deployment. Premere `s` per rimuovere l'utente oppure `n` per mantenerlo.
5. Specificare se si desidera mantenere o rimuovere il gruppo durante la disinstallazione del server Sentinel Rapid Deployment. Premere `s` per rimuovere il gruppo oppure `n` per mantenerlo.
6. Immettere `y` per disinstallare o `n` per uscire dalla disinstallazione.

7.2 Disinstallazione di Gestione servizi di raccolta remota e delle applicazioni client di Sentinel

7.2.1 Linux

1. Eseguire il login come `root`.
2. (Condizionale) Se si disinstalla Gestione servizi di raccolta, interrompere i servizi Sentinel Rapid Deployment:

   `<directory_di_installazione>/bin/sentinel.sh stop`
3. Passare all'ubicazione seguente:

   `<directory_di_installazione>/_uninst`

4 Eseguire una delle seguenti operazioni:

Modalità	Comando
GUI	`./uninstall.bin`
	Continuare con Passo 5 a pagina 86.
Console	`./uninstall.bin -console`
	Continuare con le istruzioni visualizzate.

5 Selezionare una lingua e fare clic su *OK*.

6 Nella procedura guidata Sentinel UninstallShield, fare clic su *Avanti*.

7 Selezionare i componenti che si desidera disinstallare e fare clic su *Avanti*.

8 Assicurarsi che tutte le applicazioni Sentinel in esecuzione vengano interrotte e fare clic su *Avanti*.

Verrà visualizzato un riepilogo delle funzionalità selezionate per la disinstallazione.

9 Fare clic su *Disinstalla*.

10 Fare clic su *Fine*.

7.2.2 Windows

1 Eseguire il login come utente Administrator.

2 (Condizionale) Se si disinstalla Gestione servizi di raccolta, interrompere i servizi Sentinel Rapid Deployment:

`<directory_di_installazione>\bin\sentinel.bat stop`

3 Eseguire una delle seguenti operazioni:

- Selezionare *Start* > *Programmi* > *Sentinel* > *Disinstalla Sentinel*.
- Selezionare *Start* > *Esegui*, immettere `<directory_di_installazione>\_uninst`, quindi fare doppio clic su `uninstall.exe`.

4 Selezionare una lingua e fare clic su *OK*.

Viene visualizzata la procedura guidata Sentinel Rapid Deployment UninstallShield.

5 Fare clic su *Avanti*.

6 Selezionare i componenti che si desidera disinstallare e fare clic su *Avanti*.

7 Assicurarsi che tutte le applicazioni Sentinel in esecuzione vengano interrotte e fare clic su *Avanti*.

Verrà visualizzato un riepilogo delle funzionalità selezionate per la disinstallazione.

8 Fare clic su *Disinstalla*.

9 Scegliere di riavviare il sistema e fare clic su *Fine*.

7.2.3 Procedure successive alla disinstallazione

Dopo aver disinstallato l'applicazione, vengono mantenute alcune impostazioni di sistema che tuttavia è possibile eliminare manualmente. Queste impostazioni devono essere eliminate prima di eseguire un'installazione pulita di Sentinel, in particolare se durante la disinstallazione di Sentinel si sono verificati errori.

Nota: in Linux, la disinstallazione di Gestione servizi di raccolta o di applicazioni client non eliminerà l'utente amministratore di Sentinel dal sistema operativo. Se si desidera eliminare questo utente, sarà necessario procedere manualmente.

- "Linux" a pagina 87
- "Windows" a pagina 87

Linux

1. Eseguire il login come `root`.
2. Rimuovere il contenuto della `<directory_di_installazione>` in cui è installato il software Sentinel.
3. Rimuovere i seguenti file, se esistenti, nella directory `/etc/init.d`:

   `sentinel`

   Questo è applicabile solo se è installato Gestione servizi di raccolta.
4. Assicurarsi che nessun utente abbia effettuato il login come utente amministratore di Sentinel (esecadm per default), quindi rimuovere l'utente, la home directory e il gruppo esec:
   - Eseguire `userdel -r esecadm`
   - Eseguire `groupdel esec`
5. Rimuovere la directory `/root/InstallShield`.
6. Rimuovere la sezione InstallShield di `/etc/profile`.
7. Riavviare il computer.

Windows

1. Eliminare la cartella `%CommonProgramFiles%\InstallShield\Universal` e tutti i suoi contenuti.
2. Eliminare la cartella `<directory_di_installazione>` (per default: `C:\Programmi\Novell\Sentinel6`).
3. Fare clic con il pulsante destro del mouse su *Risorse del computer* > *Proprietà* > *scheda Avanzate*.
4. Fare clic sul pulsante *Variabili d'ambiente*.
5. Se esistenti, cancellare le variabili seguenti:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME

- ESEC_CONF_FILE
- WORKBENCH_HOME

6. Rimuovere tutte le voci nella variabile di ambiente PATH che fanno riferimento all'installazione di Sentinel.
7. Eliminare tutti i collegamenti a Sentinel dal desktop.
8. Eliminare la cartella dei collegamenti *Start* > *Programmi* > *Sentinel* dal menu *Start*.
9. Riavviare il computer.

Aggiornamento del nome host di Sentinel Rapid Deployment

A

A.1 Server

Nel server Sentinel un nome host eventualmente modificato viene aggiornato automaticamente durante il runtime o l'installazione. Se il server non funziona correttamente dopo un aggiornamento del nome host, occorre verificare manualmente quanto segue:

- Che tutti i file `jnlp` e i file `configuration.xml` siano aggiornati al riavvio di Sentinel.
- Che la voce relativa al nome host nella tabella del database `sentinel_host` sia aggiornata.
- Che tutti i riferimenti al ciclo locale (localhost o 127.0.0.1) nel file `<directory_di_installazione>/config/configuration.xml` rimangano inalterati.

A.2 Applicazioni client

Per le applicazioni client è necessario modificare manualmente l'indirizzo IP o il nome host del server nelle seguenti ubicazioni, per puntare al server corretto:

- `<directory_di_installazione>/config/configuration.xml`.

  Sentinel Control Center e Solution Designer utilizzano queste informazioni.
- L'URL della Guida fornito nel file `<directory_di_installazione>/config/SentinelPreferences.properties`.
- Eseguire il comando seguente per aggiornare il nome host nel file `sdm.connect`:

  ```
  sdm -action saveConnection -server <postgresql> -host <hostIpaddress/
  hostName> -port <portnum> -database <databaseName/SID> [-driverProps
  <propertiesFile] {-user <dbUser> -password <dbPass> | -winAuth} -
  connectFile <filenameToSaveConnection>
  ```

Suggerimenti per la soluzione dei problemi

B

Questa sezione fornisce un elenco di suggerimenti per la risoluzione dei problemi che può essere di aiuto per risolvere alcuni dei problemi di installazione di Sentinel Rapid Deployment.

B.1 Errore nell'autenticazione del database o immissione di credenziali non valide

Causa comune: se durante la configurazione del server Sentinel Rapid Deployment per l'autenticazione LDAP si immette un nome host o un indirizzo IP del server LDAP non valido, si verifica un errore nell'autenticazione del database.

Azione: assicurarsi che il nome host o l'indirizzo IP del server LDAP immesso sia valido.

B.2 Avvio dell'interfaccia Web di Sentinel non riuscito

Causa comune: sentinel Rapid Deployment è stato installato in un computer in cui un processo Identity Audit è in esecuzione oppure non è stato disinstallato completamente.

Azione: non è possibile installare Sentinel Rapid Deployment e Novell Identity Audit sullo stesso computer. Prima di installare Sentinel Rapid Deployment sul computer in cui è installato Identity Audit, assicurarsi di disinstallare completamente Identity Audit.

Se i processi di Identity Audit non sono stati interrotti completamente, la disinstallazione di Identity Audit non potrà essere completata. In questo caso esiste la possibilità di conflitti durante l'installazione di Sentinel Rapid Deployment o l'avvio delle applicazioni relative.

1. Eseguire il comando riportato di seguito per chiudere i servizi di Identity Audit:

   ```
   /etc/init.d/identity_audit stop
   ```

2. Eseguire il comando riportato di seguito per assicurarsi che tutti i servizi di Identity Audit abbiano smesso di funzionare:

   ```
   ps -ef | grep novell
   ```

3. Interrompere manualmente i processi rimanenti, se necessario.

   ```
   kill -9 pid
   ```

4 Disinstallare Identity Audit con le autorizzazioni di utente`radice` necessarie.

   Per ulteriori informazioni, vedere Guida dell'utente di Novell Identity Audit (http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/).

B.3 Gestione servizi di raccolta remota genera un'eccezione in Windows 2008 quando è abilitato UAC

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

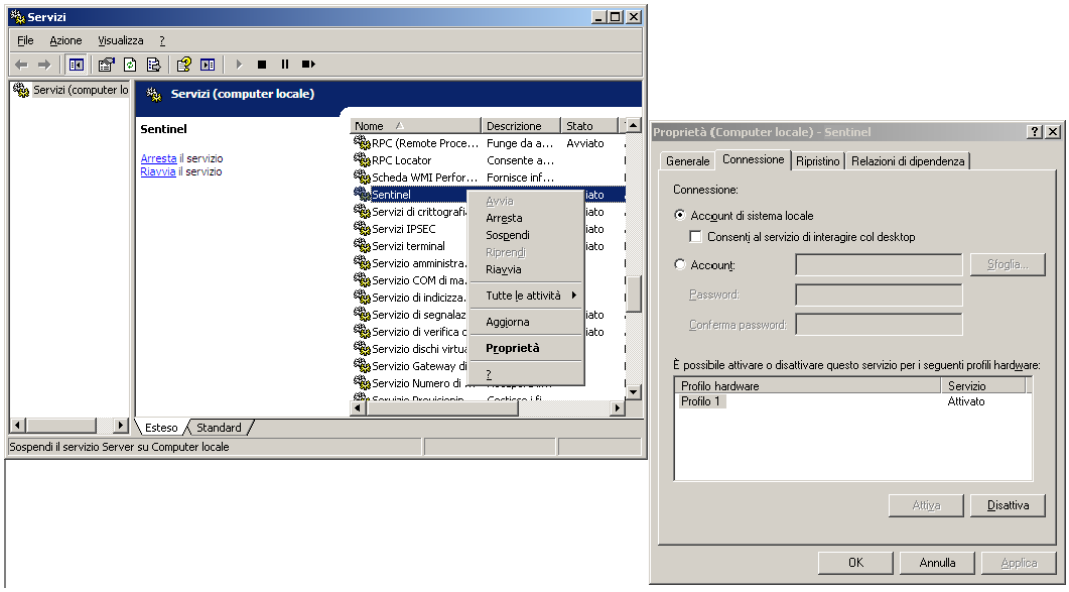
- Le mappature non vengono inizializzate.
- Non è possibile scegliere file di origine eventi nel file system del computer di Gestione servizi di raccolta (Win2008) mediante il connettore file.

Causa comune: gestione servizi di raccolta è stato installato in un sistema Windows 2008 SP1 standard edition a 64 bit. Per default, l'UAC (User Access Control) del computer è impostato a *Abilitato*.

Azione: modificare il proprietario del *login* per i servizi Sentinel Rapid Deployment sostituendolo con l'utente attuale. Per default, come proprietario dell'*Accesso* è impostato l'*Account di sistema locale*. Per cambiare l'opzione di default:

1 Eseguire `services.msc` per aprire la finestra *Servizi*.

2 Fare clic con il pulsante destro del mouse su Sentinel e selezionare *Proprietà*.



3. Nella finestra delle proprietà di Sentinel selezionate la scheda *Accesso*.
4. Selezionare *Account* e fornire le credenziali per l'utente corrente, utilizzato per installare Gestione servizi di raccolta.

B.4 Impossibile creare UUID per le istanze di Gestione servizi di raccolta con immagini

Se si crea un'immagine nel server Gestione servizi di raccolta (ad esempio, utilizzando ZENWorks Imaging) e si ripristinano le immagini su computer diversi, Sentinel Rapid Deployment non identifica singolarmente le nuove istanze di Gestione servizi di raccolta. Ciò è dovuto agli UUID duplicati.

Seguendo la procedura indicata, è necessario generare l'UUID nei sistemi di Gestione servizi di raccolta installati di recente:

1. Eliminare il file `host.id` o `sentinel.id` ubicato nella cartella `<directory_di_installazione>/data`.
2. Riavviare Gestione servizi di raccolta.

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

Best practice per l'aggiornamento del database PostgreSQL

C

È possibile ottimizzare il database in modo da migliorare le prestazioni del rispettivo server. I limiti descritti nella sessione sono consigli approssimativi. Non si tratta di limiti rigorosi. Tuttavia, in sistemi estremamente dinamici, è opportuno creare buffer incorporati e lasciare spazio per l'eventuale aumento di volume.

C.1 Modifica dei parametri di configurazione della memoria

Per ottimizzare il server del database PostgreSQL, nel file `<dir_install>/3rd party/postgresql/data/postgresql.conf` modificare i seguenti parametri di configurazione della memoria:

- **shared_buffers:** determina la quantità di memoria assegnata a PostgreSQL per la memorizzazione nella cache dei dati. Per ottenere prestazioni migliori, è possibile impostare il valore del parametro a un quarto della RAM disponibile.
- **effective_cache_size:** determina la quantità di memoria disponibile per la memorizzazione nella cache del disco nel sistema operativo e nel database. È possibile calcolare le dimensioni del parametro tenendo conto della quantità di memoria utilizzata dal sistema operativo e da altre applicazioni. È possibile allocare al parametro metà della memoria totale del sistema disponibile.
- **work_mem:** determina la quantità di memoria utilizzata dalle operazioni di ordinamento interne e dalle tabelle hash prima di passare ai file su disco temporanei. Il valore è espresso in kilobyte. Il valore di default è 1024 kilobyte (1 MB).

  Per un'interrogazione complessa, è possibile che vengano eseguite contemporaneamente diverse operazioni di ordinamento o hash. Ciascuna operazione utilizza una quantità di memoria pari al valore specificato per work_mem prima che i dati vengano inseriti nei file su disco temporanei. Se si pianificano più rapporti nel sistema Sentinel Rapid Deployment, impostare il valore tra 500 MB e 1 GB.
- **maintenance_work_mem:** determina la quantità massima di memoria da utilizzare nelle operazioni di aggiornamento del database, quali VACUUM, CREATE INDEX e ALTER TABLE ADD FOREIGN KEY. Il valore è espresso in kilobyte. Il valore di default è 16384 kilobyte (16 MB).

  L'impostazione di valori più alti potrebbe migliorare le prestazioni relative alla rimozione e al ripristino dei dump del database. Lasciare inalterato il parametro, in quanto il valore di default è sufficiente per le operazioni di Sentinel Rapid Deployment.

C.2 Riduzione dell'impatto di I/O del processo Vacuum/Analyze

È possibile migliorare le prestazioni del database PostgreSQL in diversi modi.

- I due parametri riportati di seguito controllano le operazioni di vacuum automatico, vengono commentati per default durante l'installazione del server Sentinel Rapid Deployment ed è necessario rimuovere il commento e impostare i valori.
  - **vacuum_cost_delay:** determina la durata dell'inattività del processo quando il limite di costo è stato superato. Ad esempio, è possibile impostare tale valore a 100.
  - **vacuum_cost_limit:** determina il costo accumulato che renderà il processo vacuum inattivo. Ad esempio, è possibile impostare tale valore a 10000.

    Se si impostano i parametri a un valore diverso da zero, si ridurrà l'impatto di I/O del comando vacuum e analyze sull'attività normale del database. Durante l'esecuzione dei rapporti, si potrebbe avere un lieve impatto sulle prestazioni poiché il processo vacuum richiede più tempo di prima.
- Per default, il processo `autovacuum` è impostato su true e viene eseguito periodicamente per recuperare spazio su disco e aggiornare le statistiche pianificate. Quando le dimensioni del database aumentano, `autovacuum` non è in grado di aggiornare tutti gli oggetti Database. In casi simili, se le prestazioni sono lente, eseguire lo script `AnalyzePartitions.sh` come lavoro (daemon) Cron. Il lavoro (daemon) Cron deve essere impostato dall'utente proprietario dei processi Sentinel Rapid Deployment.

  Ad esempio:

  ```
  30 11 * * * $ESEC_HOME/bin/AnalyzePartitions.sh
  ```

  Dove:

  - `30` sono i minuti.
  - `11` sono le ore.
  - `ESEC_HOME` è il percorso assoluto del database.

  Nell'esempio, lo script viene eseguito ogni giorno alle 11:30.
- Evitare di pianificare l'archiviazione durante la generazione di rapporti. Se si pianificano entrambi i processi contemporaneamente, la generazione di rapporti viene messa in attesa a causa dei bug di PostgreSQL e l'elaborazione dei dati ha inizio al termine del lavoro di archiviazione. Questa modifica incide sulle prestazioni del database.