AUTHORIZED DOCUMENTATION

Guida all'installazione - Volume I

July, 2008

Novell® Sentinel®

6.1

www.novell.com

Note legali

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
USA
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.

Note legali di terze parti

Il prodotto potrebbe includere i seguenti programmi open source disponibili in conformità alla licenza LGPL. Il testo della licenza è disponibile nella directory Licenze.

edtFTPj-1.2.3 è concesso in licenza in base alla Lesser GNU Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.enterprisedt.com/products/edtftpj/purchase.html (http://www.enterprisedt.com/products/edtftpj/purchase.html).

Enhydra Shark, concesso in licenza in base a Lesser General Public License disponibile all'indirizzo: http://shark.objectweb.org/license.html (http://shark.objectweb.org/license.html).

Esper. Copyright © 2005-2006, Codehaus.

FESI è concesso in licenza in base a Lesser GNU Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.lugrin.ch/fesi/index.html (http://www.lugrin.ch/fesi/index.html).

jTDS-1.2.2.jar è concesso in licenza in base a Lesser GNU Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://jtds.sourceforge.net/ (http://jtds.sourceforge.net/).

MDateSelector. Copyright © 2005, Martin Newstead, concesso in licenza in base a Lesser General Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://web.ukonline.co.uk/mseries (http://web.ukonline.co.uk/mseries).

Tagish Java Authentication e Authorization Service Module, concessi in licenza in base a Lesser General Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://free.tagish.net/jaas/index.jsp (http://free.tagish.net/jaas/index.jsp).

Il prodotto potrebbe includere il seguente software sviluppato da The Apache Software Foundation http://www.apache.org/ (http://www.apache.org/) e concesso in licenza in base ad Apache License, Versione 2.0 (la "Licenza"). Il testo relativo alla licenza è disponibile nella directory delle licenze o all'indirizzo http://www.apache.org/licenses/LICENSE-2.0 (http://www.apache.org/licenses/LICENSE-2.0). Eccetto dove previsto dalle leggi vigenti o dove espressamente indicato in un accordo scritto, il software distribuito ai sensi della Licenza, viene fornito "COSÌ COM'È" SENZA GARANZIE O CONDIZIONI DI ALCUN TIPO, esplicite o implicite. Consultare la Licenza per le disposizioni specifiche che regolano le autorizzazioni e le limitazioni ai sensi della Licenza.

Apache Axis e Apache Tomcat, Copyright © 1999-2005, Apache Software Foundation. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.apache.org/licenses/. (http://www.apache.org/licenses/.)

Apache FOP.jar, Copyright 1999-2007, Apache Software Foundation. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.apache.org/licenses/ (http://www.apache.org/licenses/).

Apache Lucene, Copyright © 1999 - 2005, Apache Software Foundation. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.apache.org/licenses/ (http://www.apache.org/licenses/).

Bean Scripting Framework (BSF), concesso in licenza da Apache Software Foundation Copyright © 1999-2004. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://xml.apache.org/dist/LICENSE.txt (http://xml.apache.org/dist/LICENSE.txt).

Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Concesso in licenza in conformità ad Apache Software License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere https://skinlf.dev.java.net/ (https://skinlf.dev.java.net/).

Xalan e Xerces, entrambi concessi in licenza da Apache Software Foundation, Copyright © 1999-2004. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://xml.apache.org/dist/LICENSE.txt (http://xml.apache.org/dist/LICENSE.txt).

Il prodotto potrebbe includere i seguenti programmi open source disponibili in conformità alla licenza Java.

JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare http://www.java.sun.com/products/javabeans/glasgow/jaf.html (http://www.java.sun.com/products/javabeans/glasgow/jaf.html) e fare clic sul collegamento per scaricare la licenza.

Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://java.sun.com/j2se/1.5.0/docs/relnotes/SMICopyright.html (http://java.sun.com/j2se/1.5.0/docs/relnotes/SMICopyright.html).

JavaMail. Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare http://www.java.sun.com/products/javamail/downloads/index.html (http://www.java.sun.com/products/javamail/downloads/index.html) e fare clic sul collegamento per scaricare la licenza.

Il prodotto potrebbe includere i seguenti programmi open source e di terze parti.

ANTLR. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare http://www.antlr.org (http://www.antlr.org).

Boost. Copyright © 1999, Boost.org.

Concurrent, pacchetto di utility. Copyright © Doug Lea. Utilizzato senza le classi CopyOnWriteArrayList e ConcurrentReaderHashMap.

ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004.

ILOG, Inc. Copyright © 1999-2004.

Java Ace, Douglas C. Schmidt e gruppo di ricerca presso la Washington University. Copyright © 1993-2005. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.cs.wustl.edu/~schmidt/ACE-copying.html (http://www.cs.wustl.edu/~schmidt/ACE-copying.html) e http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html (http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html).

Java Service Wrapper. Componenti protetti da copyright come indicato di seguito: Copyright © 1999-2004 Tanuki Software e Copyright © 2001 Silver Egg Technology. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://wrapper.tanukisoftware.org/doc/english/license.html (http://wrapper.tanukisoftware.org/doc/english/license.html).

JIDE. Copyright © 2002 to 2005, JIDE Software, Inc.

JLDAP. Copyright © 1998-2005 The OpenLDAP Foundation. Tutti i diritti riservati. Portions Copyright © 1999 - 2003 Novell, Inc. Tutti i diritti riservati.

Monarch Charts. Copyright © 2005, Singleton Labs.

OpenSSL, OpenSSL Project. Copyright © 1998-2004. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.openssl.org (http://www.openssl.org).

Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.

Rhino. L'utilizzo è soggetto alla Mozilla Public License 1.1. Per ulteriori informazioni, vedere http://www.mozilla.org/rhino/ (http://www.mozilla.org/rhino/).

SecurityNexus. Copyright © 2003 - 2006. SecurityNexus, LLC. Tutti i diritti riservati.

Sonic Software Corporation. Copyright © 2003-2004. Il software SSC contiene software di protezione concesso in licenza da RSA Security, Inc.

Tao (con wrapper ACE), Douglas C. Schmidt e gruppo di ricerca presso la Washington University, University of California, Irvine e Vanderbilt University. Copyright © 1993-2005. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://www.cs.wustl.edu/~schmidt/ACE-copying.html (http://www.cs.wustl.edu/~schmidt/ACE-copying.html) e http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html (http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html).

Tinyxml. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere http://grinninglizard.com/tinyxmldocs/index.html (http://grinninglizard.com/tinyxmldocs/index.html).

XML Pull Parser. Questo prodotto comprende software sviluppato da Indiana University Extreme! Lab (http://www.extreme.indiana.edu/ (http://www.extreme.indiana.edu/)).

yWorks. Copyright © 2003-2006, yWorks.

NOTA: al momento della pubblicazione della presente documentazione i collegamenti indicati sopra risultano attivi. Qualora i collegamenti risultassero non più validi o le relative pagine Web non più attive, contattare Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Sommario

Prefazione

Sentinel™ è una soluzione di gestione degli eventi e delle informazioni di sicurezza che riceve le informazioni da numerose fonti all'interno di un'azienda, le standardizza, assegna loro priorità e le presenta all'utente affinché possa intraprendere le opportune azioni in base alle minacce, ai rischi e alle norme.

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 sei differenti volumi. ovvero:

- Guida all'installazione di Sentinel 6.1
- Sentinel 6.1 User Guide
- Sentinel 6.1 User Reference Guide
- La documentazione relativa al prodotto è disponibile all'indirizzo http://www.novell.com/documentation/sentinel6/index.html

Volume I: Guida all'installazione di Sentinel 5

In questa guida viene descritto come installare i seguenti componenti di Sentinel:

- Sentinel Communication Server
- Servizio DAS (Data Access Service)
- Sentinel Control Center
- Motore di correlazione di Sentinel
- Gestione servizi di raccolta
- Crystal Reports Server
- Advisor
- Generatore servizi di raccolta
- Gestione dati Sentinel
- Sentinel Solution Designer

Volume II – Sentinel User Guide

Nella guida viene descritto come utilizzare i componenti e le funzionalità di Sentinel:

- Operazione della console Sentinel
- Funzioni di Sentinel
- Architettura di Sentinel
- Comunicazione di Sentinel
- Arresto/Avvio di Sentinel
- Valutazione delle vulnerabilità
- Monitoraggio degli eventi
- Filtro degli eventi
- Correlazione degli eventi
- Gestione dati Sentinel
- Configurazione eventi per rilevanza aziendale
- Servizio di mappatura
- Rapporti cronologici
- Gestione host Servizio di raccolta
- Casi
- Situazioni
- Gestione utenti
- Workflow
- Pacchetti soluzione

Volume III – Collector Builder User Guide

Nella guida viene illustrato come utilizzare il Generatore servizi di raccolta:

- Funzionamento del Generatore servizi di raccolta
- Gestione servizi di raccolta
- Servizi di raccolta
- Gestione host Servizio di raccolta
- Creazione e manutenzione di servizi di raccolta

Volume IV – Sentinel User Reference Guide

Nella guida vengono illustrati i seguenti argomenti avanzati:

- Linguaggio di script per i servizi di raccolta
- Comandi per l'esecuzione dell'analisi sintattica dei servizi di raccolta
- Funzioni di amministratore dei servizi di raccolta
- Tag META di Sentinel e dei servizi di raccolta
- Motore di correlazione di Sentinel
- Autorizzazioni utente
- Opzioni della riga di comando di correlazione
- Schema database Sentinel

Volume V - Sentinel Third-Party Integration Guide

Nella guida viene illustrato come utilizzare Sentinel con applicazioni di terze parti:

- Remedy
- HP OpenView Operations
- HP Service Desk

Volume VI - Sentinel Patch Installation Guide

Nella guida viene descritto come eseguire l'upgrade da una versione di Sentinel a quella successiva.

- Installazione delle patch da Sentinel 4.x a 6.0
- Installazione delle patch da Sentinel 5.1.3 a 6.0

Convenzioni della documentazione

Nel presente manuale vengono utilizzate le convenzioni seguenti:

- Note e avvisi

  Nota: le note forniscono informazioni aggiuntive che potrebbero essere utili o a titolo di riferimento.

  Avviso: gli avvisi forniscono informazioni aggiuntive che aiutano a identificare e interrompere l'esecuzione nel sistema di azioni che causano danni o perdite di dati.

- I comandi sono visualizzati con il font courier. Ad esempio:

  ```
  useradd -g dba -d /export/home/oracle -m -s /bin/csh oracle
  ```

- Accedere a Start > Programmi > Pannello di controllo per eseguire questa azione: più azioni in un passaggio.
- Riferimenti

  Per ulteriori informazioni, vedere “Nome sezione” (se nello stesso capitolo).

  Per ulteriori informazioni, vedere “Nome capitolo” (se nella stessa guida).

  Per ulteriori informazioni, vedere Nome sezione in Nome capitolo, *Nome della guida* (se in una guida differente).

Nella documentazione di Novell, il simbolo maggiore di (>) viene utilizzato per separare le azioni di uno stesso passo di procedura e gli elementi in un percorso di riferimenti incrociati.

Un simbolo di marchio di fabbrica (®, TM, e così via) indica un marchio di fabbrica Novell. Un asterisco (*) indica un marchio di fabbrica di terze parti.

Quando un nome di percorso può essere scritto con una barra rovesciata (\) per alcune piattaforme o con una barra (/) per altre piattaforme, verrà riportato con una barra rovesciata. Gli utenti di piattaforme che prevedono l'uso di barre, ad esempio Linux o UNIX, dovranno utilizzare questo carattere come richiesto dal software.

Come contattare Novell

- Sito Web: http://www.novell.com (http://www.novell.com)
- Supporto tecnico Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- Supporto autonomo: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Sito per il download delle patch: http://download.novell.com/index.jsp (http://download.novell.com/index.jsp)
- Supporto 24 ore su 24, 7 giorni su 7: http://www.novell.com/company/contact.html. (http://www.novell.com/company/contact.html.)
- Per Servizi di raccolta/Connettori/Rapporti/Correlazione/Aggiornamenti rapidi/TIDS: http://support.novell.com/products/sentinel (http://support.novell.com/products/sentinel).

Introduzione 1

Nelle seguenti sezioni vengono descritti i concetti di base del prodotto. Nella parte restante della *Sentinel User Guide* vengono fornite informazioni più dettagliate sull'architettura, il funzionamento e le procedure amministrative.

In questa guida si presume che l'utente abbia familiarità con la sicurezza di rete, l'amministrazione dei database e i sistemi operativi Windows* e UNIX*.

1.1 Panoramica di Sentinel

Sentinel™ è una soluzione di gestione degli eventi e delle informazioni di sicurezza che riceve le informazioni da numerose fonti all'interno di un'azienda, le standardizza, assegna loro priorità e le presenta all'utente affinché possa intraprendere le opportune azioni in base alle minacce, ai rischi e alle norme.

Sentinel automatizza i processi di raccolta log, analisi e creazione di rapporti per assicurare che i controlli IT siano in grado di supportare in modo efficace i requisiti di rilevamento e verifica 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 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 una GUI più sensibile, identifica i problemi di sicurezza o di conformità e controlla le attività di correzione allo scopo di snellire i processi precedenti maggiormente 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 di Oracle.

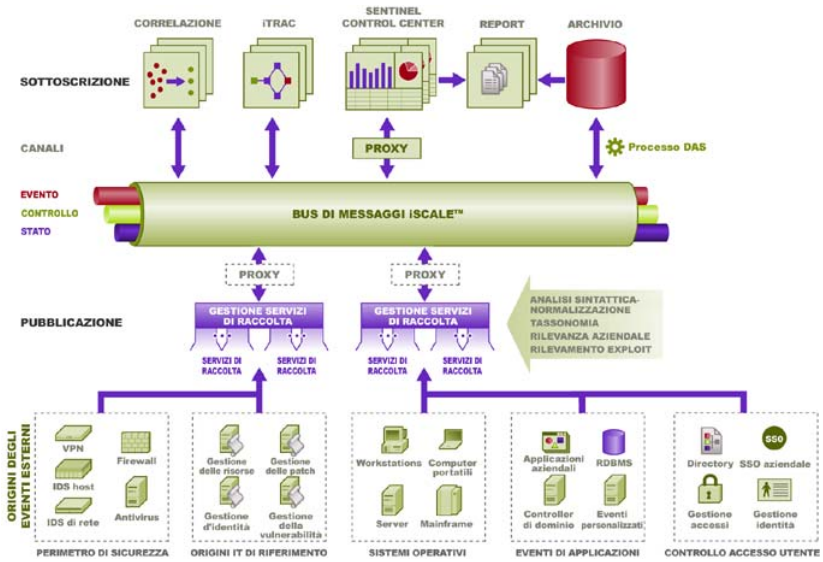
Vantaggi di Sentinel:

- Gestione integrata, automatica e in tempo reale della sicurezza e monitoraggio della conformità in tutti i sistemi e reti

- Struttura che consente alle norme aziendali di influenzare le norme e le azioni del dipartimento IT
- Documentazione e creazione automatica di rapporti sulla sicurezza, sui sistemi e sugli eventi di accesso all'interno dell'azienda
- Gestione incorporata dei casi e correzione
- Capacità di dimostrare e monitorare la conformità con le norme interne e le normative locali quali Sarbanes-Oxley, HIPAA, GLBA, FISMA e altre. Il contenuto richiesto per l'implementazione di tali controlli è distribuito e implementato semplicemente mediante i pacchetti soluzione.

Di seguito viene descritta un'architettura concettuale di Sentinel che illustra i componenti necessari per gestire la conformità e la sicurezza.

Figura 1-1 *Architettura concettuale di Sentinel*



1.2 Interfacce utente di Sentinel

Sentinel include numerose interfacce utente facili da utilizzare:

- Sentinel Control Center
- Gestione dati Sentinel
- Sentinel Solution Designer
- Generatore servizi di raccolta Sentinel

1.2.1 Sentinel Control Center

Il modulo Sentinel Control Center offre un dashboard integrato per la gestione della sicurezza che consente agli analisti di identificare velocemente le nuove tendenze o i nuovi attacchi, di elaborare e interagire con le informazioni grafiche in tempo reale e di rispondere ai casi. Le funzioni principali di Sentinel Control Center includono:

- **Active Views:** analisi e visualizzazione in tempo reale

- **Casi:** Creazione e gestione dei casi
- **Correlazione:** Definizione e gestione delle regole di correlazione
- **iTRAC:** Gestione dei processi per la documentazione, l'applicazione e il controllo dei processi di risoluzione dei casi
- **Generazione di rapporti:** Cronologia dei rapporti e delle misurazioni
- **Gestione dell'origine evento:** Distribuzione e monitoraggio del Servizio di raccolta

1.2.2 Gestione dati Sentinel

La Gestione dati Sentinel (SDM) consente di gestire il database di Sentinel. Nel modulo SDM è possibile eseguire le operazioni seguenti:

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

1.2.3 Sentinel Solution Designer

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

1.2.4 Generatore servizi di raccolta Sentinel

Generatore servizi di raccolta Sentinel consente di creare Servizi di raccolta nel linguaggio esclusivo di Sentinel per l'elaborazione degli eventi. È possibile creare e personalizzare i modelli in modo che il Servizio di raccolta possa analizzare sintatticamente i dati.

1.3 Componenti del server Sentinel

Sentinel è costituito da diversi componenti:

- Servizio DAS (Data Access Service)
- Sentinel Communication Server
- Database di Sentinel
- Gestione servizi di raccolta Sentinel
- Motore di correlazione
- iTRAC™
- Crystal Reports Server *
- Advisor e Rilevamento exploit di Sentinel (facoltativi)

1.3.1 Server Sentinel

Il servizio DAS (Data Access Service) è il componente principale utilizzato per comunicare con il database di Sentinel. Il servizio DAS e altri componenti del server funzionano congiuntamente per memorizzare gli eventi ricevuti dalle Gestioni servizi di raccolta nel database, filtrare i dati, elaborare le visualizzazioni Active View, eseguire interrogazioni del database ed elaborare i risultati e gestire le attività amministrative, ad esempio l'autenticazione e l'autorizzazione utente.

1.3.2 Sentinel Communication Server

Il bus messaggio iSCALE™ è in grado di spostare migliaia di pacchetti di messaggi in un secondo tra i componenti di Sentinel. Ciò consente di ridimensionare in modo indipendente i componenti e di integrare le applicazioni esterne in conformità agli standard.

1.3.3 Database di Sentinel

Il prodotto Sentinel è progettato attorno a un database back-end in cui vengono memorizzati gli eventi di sicurezza e tutti i metadati di Sentinel. Gli eventi vengono memorizzati in formato normalizzato, insieme ai dati sulle risorse e le vulnerabilità, informazioni sull'identità, stato dei casi e del workflow e altri tipi di dati.

1.3.4 Gestione servizi di raccolta Sentinel

Gestione servizi di raccolta gestisce la raccolta dei dati, monitora i messaggi di stato del sistema ed applica i filtri agli eventi in base alle richieste. 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 può connettersi direttamente al bus messaggio oppure utilizzare un proxy SSL.

1.3.5 Motore di correlazione

Grazie alla correlazione sono disponibili nuove funzioni di gestione degli eventi di sicurezza, le quali consentono di automatizzare l'analisi del flusso di eventi in ingresso per individuare eventuali schemi di interesse. La correlazione consente di definire regole per l'identificazione di minacce critiche e modelli di attacco complessi, al fine di poter stabilire una priorità per gli eventi, nonché reagire e gestire i casi in modo efficace.

1.3.6 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, mediante una regola di correlazione o manualmente, possono essere associati a un workflow iTRAC.

1.3.7 Crystal Reports Server

I servizi completi di generazione di rapporti all'interno del Sentinel Control Center sono forniti da Crystal Reports Server di Business Objects*. Sentinel integra rapporti predefiniti strutturati per soddisfare le richieste più comuni di generazione di rapporti da parte delle organizzazioni che monitorano i comportamenti di sicurezza e conformità. Crystal Reports Developer consente inoltre di sviluppare rapporti nuovi o personalizzati rispetto allo schema di visualizzazione dei rapporti pubblicati di Sentinel.

1.3.8 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 in tempo reale delle istruzioni o a informazioni sulla prevenzione dal proprio ambiente, consentono un rilevamento efficiente dell'exploit e la possibilità di agire tempestivamente in caso di attacco a un sistema vulnerabile.

1.4 Plug-in di Sentinel

Sentinel supporta una serie di plug-in per ampliare e migliorare le funzionalità del sistema. Alcuni di questi plug-in vengono installati automaticamente. È possibile scaricare plug-in e aggiornamenti aggiuntivi all'indirizzo: http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html).

Per poter scaricare alcuni plug-in, ad esempio l'integratore Remedy* e il connettore Mainframe IBM*, è necessaria una licenza aggiuntiva.

1.4.1 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 tipi di dispositivi elencati di seguito:

- 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 ed eseguiti su Sentinel 6.0 SP1 e versioni successive mediante gli strumenti di sviluppo JavaScript standard e il SDK del Servizio di raccolta. È possibile creare o modificare Servizi di raccolta esclusivi mediante Sezione 1.2.4, “Generatore servizi di raccolta Sentinel”, a pagina 15un'applicazione autonoma inclusa nel sistema Sentinel.

1.4.2 Connettori e integratori

I connettori garantiscono la connettività dalla 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.

1.4.3 Regole di correlazione e azioni

Le regole di correlazione identificano schemi importanti nel flusso degli eventi. In caso di attivazione di 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.

1.4.4 Rapporti

Gli utenti possono eseguire un'ampia varietà di rapporti dashboard e operativi da Sentinel Control Center mediante Crystal Report Server. In Sentinel 6.1 e versioni successive, i rapporti vengono generalmente distribuiti mediante i pacchetti soluzione.

1.4.5 Workflow iTRAC

I workflow iTRAC forniscono processi coerenti e ripetibili per la gestione dei casi. In Sentinel 6.1 e versioni successive, i modelli del workflow vengono generalmente distribuiti mediante i pacchetti soluzione.

1.4.6 Pacchetti soluzione

I pacchetti soluzione sono serie 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 ha inoltre creato "pacchetti di servizi di raccolta" che includono contenuti focalizzati su una specifica origine evento, ad esempio Windows Active Directory.

1.5 Supporto della lingua

I componenti Sentinel sono localizzati per le lingue seguenti:

- Inglese

- Portoghese (Brasile)
- Francese
- Italiano
- Tedesco
- Spagnolo
- Giapponese
- Cinese (tradizionale)
- Cinese (semplificato)

Alcune eccezioni:

- L'interfaccia e gli script del Generatore servizi di raccolta sono solo in lingua inglese ma possono essere eseguiti sui sistemi operativi nelle altre lingue elencate in precedenza.
- I Servizi di raccolta JavaScript possono essere modificati per l'analisi sintattica di dati ASCII o Unicode (byte doppio), ma i Servizi di raccolta pubblicati sul sito Sentinel Content sono attualmente scritti solo in lingua inglese. I Servizi di raccolta scritti nella lingua esclusiva del Servizio di raccolta sono in grado di elaborare solo i dati ASCII e ASCII esteso.
- Gli eventi interni per la verifica delle operazioni Sentinel sono solo in lingua inglese.

Requisiti di sistema

2

2.1 Software supportato

Per garantire prestazioni e affidabilità ottimali, Novell consiglia di installare tutti i componenti Sentinel su software approvato la cui qualità sia completamente assicurata e certificata. Per informazioni aggiornate sui requisiti minimi, verificare la disponibilità di aggiornamenti sul sito della documentazione Novell (http://www.novell.com/documentation/sentinel61).

Nella tabella riportata di seguito vengono elencati i livelli di patch utilizzati per eseguire la verifica Sentinel. Per comodità ai fini del presente documento, le piattaforme vengono indicate con il nome breve nella colonna a sinistra. Nei casi in cui la lunghezza dei bit non è rilevante ai fini del documento, è possibile eliminarla dal nome breve.

Tabella 2-1 *Informazioni sul livello di patch*

Nome breve	Nome completo e livello di patch
SLES 10 (a 32 bit)	SUSE® Linux Enterprise Server 10 SP1 (a 32 bit)
SLES 10 (a 64 bit)	SUSE Linux Enterprise Server 10 SP1 (a 64 bit)
RHEL 4 (a 32 bit)	Red Hat Enterprise Linux 4 Nahant Update-4 (a 32 bit)
RHEL 4 (a 64 bit)	Red Hat Enterprise Linux 4 Nahant Update-4 (a 64 bit)
Solaris 10 (a 64 bit)	Sun Solaris 10 6/06 s10s_u2wos_09a (SPARC a 64 bit)
Windows 2003 (a 32 bit)	Windows 2003 SP2, Standard o Enterprise Edition (a 32 bit)
Windows 2003 (a 64 bit)	Windows 2003 SP1, Standard o Enterprise Edition (a 64 bit)
Windows 2008 (a 64 bit)	Windows 2008 SP1, Standard Edition (a 64 bit)
SLED 10 (a 32 bit)	SUSE® Linux Enterprise Desktop 10 SP1 (32-bit)
Windows XP (32-bit)	Windows XP SP2 (a 32 bit)
Windows Vista (a 32 bit)	Windows Vista SP1 (a 32 bit)
Oracle 10 (a 32 bit)	Oracle* 10g Enterprise Edition con partizionamento (v 10.2.0.3 - 5901891 include la patch critica n. 5881721, la patch di sicurezza 6864068) (a 32 bit), in esecuzione su SuSE Linux Enterprise Server 10 (a 32 bit)
Oracle 10 (a 64 bit)	Oracle 10g Enterprise Edition con partizionamento (v 10.2.0.3 - 5901891 include la patch critica n. 5881721, la patch di sicurezza 6864068), in esecuzione su (a 64 bit)
SQL Server 2005 (a 32 bit)	Microsoft SQL Server 2005 SP2, Standard o Enterprise Edition (a 32 bit)

Nome breve	Nome completo e livello di patch
SQL Server 2005 (a 64 bit)	Microsoft SQL Server 2005 SP2, Standard o Enterprise Edition (a 64 bit)
SQL Server 2008 (a 64 bit)	CTP di febbraio 2008 di Microsoft SQL Server 2008 (a 64 bit)
SLES 9 (a 32 bit)	SuSE Linux Enterprise Server 9 SP2 (a 32 bit)

Verificare la disponibilità di aggiornamenti e patch di sicurezza presso i rispettivi fornitori. Queste correzioni HotFix e patch di sicurezza non hanno in genere alcun impatto sul funzionamento di Sentinel, pertanto non sono supportate. Poiché le release principali o secondarie di un database o di un sistema operativo comportano in genere modifiche di maggior entità, la presente release supporta soltanto le versioni riportate sopra.

2.1.1 Piattaforme supportate del database

Le combinazioni di database e sistema operativo descritte di seguito sono contrassegnate come certificate o supportate. Le combinazioni certificate sono state testate mediante la suite di test completa di Novell Engineering. Si prevede che le combinazioni supportate siano completamente funzionali.

Tabella 2-2 *Piattaforme supportate del database*

	Oracle 10 (32)	Oracle 10 (64)	SQL Server 2005 (32)	SQL Server 2005 (64)	MS SQL 2008 (64)
SLES 10 (32)	Supportata	Non supportata	Non supportata	Non supportata	Non supportata
SLES 10 (64)	Non supportata	Certificata	Non supportata	Non supportata	Non supportata
RHEL 4 (32)	Supportata	Non supportata	Non supportata	Non supportata	Non supportata
RHEL 4 (64)	Non supportata	Supportata	Non supportata	Non supportata	Non supportata
Solaris 10 (32)	Supportata	Non supportata	Non supportata	Non supportata	Non supportata
Solaris 10 (64)	Non supportata	Supportata	Non supportata	Non supportata	Non supportata
Windows 2003 (32)	Non supportata	Non supportata	Supportata	Non supportata	Non supportata
Windows 2003 (64)	Non supportata	Non supportata	Non supportata	Certificata	Non supportata
Windows 2008 (64)	Non supportata	Non supportata	Non supportata	Non supportata	Supportata

Il database Sentinel è supportato sulle piattaforme a 32 bit negli ambienti di sviluppo o di prova. Tuttavia, al fine di ottenere prestazioni ottimali, Novell consiglia le piattaforme a 64 bit per i database di produzione.

Sentinel è stato testato con la versione beta della CTP di febbraio 2008 di Microsoft SQL Server 2008 (a 64 bit). Non sono stati segnalati problemi noti alla data di pubblicazione, ma eventuali modifiche apportate al database prima del rilascio ufficiale potrebbero influenzare le operazioni Sentinel.

Nota: Tutti i database devono essere installati su un sistema operativo certificato dal fornitore del database e da Novell per l'utilizzo con i componenti Sentinel. Oracle deve essere eseguito su Linux* o Solaris, non in Windows.

2.1.2 Componenti di Sentinel

I componenti del server Sentinel includono Communication Server, il motore di correlazione, Data Access Service (DAS) e il servizio di sottoscrizione dei dati Advisor che risiede nello stesso computer del servizio DAS.

Le applicazioni utente Sentinel elencate nella tabella seguente includono Sentinel Control Center, Gestione dati Sentinel e Sentinel Solution Designer.

Anche Collector Manager, Collector Builder e Crystal Reports Server dispongono di requisiti di piattaforma specifici.

Le combinazioni tra software e sistema operativo descritte di seguito sono contrassegnate come certificate (C) o supportate (S). Le combinazioni certificate sono state testate mediante la suite di test completa di Novell Engineering. Si prevede che le combinazioni supportate siano completamente funzionali.

Tabella 2-3 *Combinazioni tra software e sistema operativo*

	Componenti del server Sentinel	Applicazioni utente Sentinel	Gestione servizi di raccolta	Generatore servizi di raccolta	Crystal Reports Server
SLES 10 (32)	Supportata	Supportata	Certificata	Non supportata	Non supportata
SLES 10 (64)	Certificata	Supportata	Supportata	Non supportata	Non supportata
RHEL 4 (32)	Supportata	Supportata	Supportata	Non supportata	Certificata
RHEL 4 (64)	Supportata	Supportata	Supportata	Non supportata	Non supportata
Solaris 10 (32)	Supportata	Supportata	Certificata	Non supportata	Non supportata
Solaris 10 (64)	Certificata	Supportata	Supportata	Non supportata	Non supportata
Windows 2003 (32)	Supportata	Supportata	Certificata	Supportata	Certificata
Windows 2003 (64)	Certificata	Supportata	Supportata	Supportata	Non supportata
Windows 2008 (64)	Supportata	Supportata	Supportata	Supportata	Non supportata
SLED 10	Non supportata	Certificata	Non supportata	Non supportata	Non supportata
Windows XP	Non supportata	Certificata	Non supportata	Supportata	Non supportata
Windows Vista	Non supportata	Supportata	Non supportata	Supportata	Non supportata
SLES 9 (32)	Non supportata	Non supportata	Non supportata	Non supportata	Certificata

Il server supportato per la generazione di rapporti è Crystal Reports Server XI R2. Per poter utilizzare Crystal è necessario un server Web e un database CMS (Central Management Server), oltre al database Sentinel. Crystal Reports Server può essere eseguito sulle seguenti piattaforme nell'ambiente Sentinel:

- Red Hat Enterprise Linux 4 (a 32 bit)
  - Database Crystal CMS su MySQL
  - Server Web su Apache Tomcat
  - Database Sentinel su Oracle consigliato; altre configurazioni non testate
- SuSE Linux Enterprise Server 9 SP2 (a 32 bit)
  - Database Crystal CMS su MySQL
  - Server Web su Apache Tomcat
  - Database Sentinel su Oracle consigliato; altre configurazioni non testate
- Windows 2003 SP1 Server, Standard o Enterprise Edition (a 32 bit)
  - Database CSM di Crystal su Microsoft SQL Server 2005
  - Server Web su Microsoft IIS con .NET
  - Database Sentinel su SQL Server consigliato; altre configurazioni non testate

Novell ha testato i rapporti di pubblicazione ed esecuzione dall'interfaccia di Sentinel utilizzando le seguenti versioni di Crystal:

- **In Linux:** Crystal Reports Server XI R2 SP2
- **In Windows:** Crystal Reports Server XI R2 SP3

Questi Service Pack possono essere scaricati dalla sezione Download del sito Web SAP all'indirizzo

https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads).

Per ulteriori informazioni sui requisiti di sistema, i numeri di versione supportati e i problemi noti per queste piattaforme, vedere la documentazione del fornitore.

2.1.3 Eccezioni al supporto piattaforme e avvertenze

Le seguenti piattaforme non sono supportate dai rispettivi fornitori e non saranno pertanto supportate da Novell:

- Crystal Reports Server XI R2 non supporta attualmente Crystal su Solaris o SUSE Linux Enterprise Server 10, di conseguenza Novell non supporta queste combinazioni.
- Oracle non supporta attualmente Oracle 10 (a 32 bit) su Solaris 10 a 32 bit

Anche se le seguenti configurazioni di piattaforme possono essere supportate dai rispettivi fornitori, Novell consiglia di non utilizzare tali configurazioni nell'ambiente Sentinel:

- Sentinel su SUSE Linux Enterprise Server 10 eseguito con il file system ReiserFS
- Database Oracle su Microsoft Windows
- Crystal Reports Server su Microsoft Windows 2000
- Crystal Reports Server con MSDE come database

Anche se Novell consiglia di eseguire il database Sentinel e il motore di generazione di rapporti sulle piattaforme la cui qualità è stata completamente assicurata da Novell, sia il database Oracle sia Crystal Reports Server sono supportati su piattaforme aggiuntive dai rispettivi fornitori. Se un cliente desidera utilizzare una di queste piattaforme aggiuntive, Novell fornirà supporto con alcune avvertenze.

- Poiché l'installazione e la configurazione del database Sentinel sono specifici in base alla piattaforma, per l'esecuzione dell'installazione e l'impostazione iniziale di Sentinel, rivolgersi a Novell Consulting o a un partner qualificato.
- Il programma di installazione standard potrebbe non funzionare come previsto su una piattaforma non testata.
- Non appena il sistema Sentinel è funzionale, tutti i problemi correlati al database o alla generazione di rapporti che non possono essere duplicati sulle piattaforme supportate interne devono essere risolti dal fornitore appropriato.

Per garantire la completa funzionalità, Novell consiglia inoltre di installare il database e il servizio DAS con lo stesso sistema operativo (non necessariamente sullo stesso computer) (ad esempio, non è possibile utilizzare l'autenticazione di Windows se il servizio DAS è installato in un ambiente misto in cui DAS è su Windows e il database è Oracle oppure DAS è su UNIX o Linux e il database è SQL Server).

Il Generatore servizi di raccolta viene eseguito solo sulla piattaforma Windows.

2.2 Raccomandazioni hardware

Durante l'installazione su Linux o Windows, il server Sentinel e i componenti del database possono essere eseguiti su hardware x86 (a 32 bit) o x86-64 (a 64 bit), con alcune eccezioni basate sul sistema operativo, come descritto in precedenza. Sentinel è certificato su hardware AMD Opteron e Intel Xeon. I server Itanium non sono supportati.

Per Solaris, è supportata l'architettura SPARC.

Avviso: Date le alte prestazioni di Sentinel, Novell consiglia di eseguire Sentinel su hardware dedicato in ambienti di produzione anziché su computer virtuali.

2.2.1 Architettura

L'architettura di Sentinel è estremamente scalabile e se si prevedono percentuali elevate di eventi, è possibile distribuire i componenti tra più computer in modo da garantire prestazioni ottimali del sistema.

Durante la progettazione di un sistema Sentinel è necessario tenere presenti numerosi fattori. Di seguito viene fornito un elenco parziale di fattori da tenere presenti durante lo sviluppo di una progettazione:

- Frequenza degli eventi (eventi al secondo o EPS)
- Posizione geografica/rete delle origini eventi e larghezza di banda tra le reti
- Hardware disponibile
- Sistemi operativi preferiti
- Piani per scalabilità futura

- Quantità prevista di filtri applicati agli eventi
- Norme locali di mantenimento dei dati
- Numero desiderato e complessità delle regole di correlazione
- Numero previsto di casi al giorno
- Numero previsto di workflow che saranno gestiti al giorno
- Numero di utenti che accedono al sistema
- Vulnerabilità e infrastruttura delle risorse

Il fattore più significativo nella progettazione del sistema Sentinel è la frequenza degli eventi: quasi ogni componente dell'architettura Sentinel verrà influenzato da un aumento delle frequenze degli eventi. In un ambiente con una frequenza elevata degli eventi, il carico maggiore verrà esercitato sul database, il quale dipende molto da I/O e potrebbe contemporaneamente gestire inserimenti di centinaia o migliaia di eventi al secondo, la creazione di oggetti da parte di più utenti, gli aggiornamenti dei processi del workflow e semplici interrogazioni cronologiche da Sentinel Control Center e rapporti a lungo termine da Crystal Reports Server. Novell pertanto consiglia quanto segue:

- Installare il database senza altri componenti di Sentinel.
- È opportuno che il server del database sia dedicato alle operazioni Sentinel. Applicazioni aggiuntive o processi ETL (Extract Transform Load) potrebbero influenzare le prestazioni del database.
- Il server del database deve avere una matrice di storage ad alta velocità che soddisfi il requisito I/O in base alle frequenze di inserimento degli eventi.
- È necessario che un amministratore di database dedicato valuti e gestisca periodicamente i seguenti aspetti del database:
  - Dimensioni
  - Operazioni I/O
  - Spazio su disco
  - Memoria
  - Indicizzazione
  - Log delle transazioni

Negli ambienti con una frequenza di eventi ridotta (ad esempio, eps < 25), le precedenti raccomandazioni sono meno rigide in quanto il database e altri componenti utilizzano una quantità inferiore di risorse.

In questa sezione vengono fornite raccomandazioni generali sull'hardware da utilizzare come riferimento per la progettazione del sistema Sentinel. In generale, le raccomandazioni di progettazione si basano sugli intervalli di frequenza degli eventi. Tali raccomandazioni si basano tuttavia sui presupposti seguenti:

- La frequenza dell'evento è al limite superiore dell'intervallo EPS.
- La dimensione media dell'evento è 600 byte.
- Tutti gli eventi sono memorizzati nel database, ovvero non sono impostati filtri per la rimozione degli eventi.
- I dati significativi relativi a trenta giorni verranno memorizzati in linea nel database.

- Lo spazio per la memorizzazione dei dati di Advisor non è incluso nelle specifiche delle tabelle seguenti.
- Per default, il server Sentinel dispone di 5 GB di spazio su disco per eseguire la memorizzazione temporanea nella cache degli eventi che non vengono inseriti nel database.
- Per default, il server Sentinel dispone inoltre di 5 GB di spazio su disco per gli eventi che non vengono scritti nei file degli eventi di aggregazione.

  Nota: la sottoscrizione facoltativa ad Advisor richiede 50 GB aggiuntivi di spazio su disco sul server del database.

Le raccomandazioni hardware per un'implementazione di Sentinel possono variare in base alla singola implementazione. Pertanto si consiglia di consultare i Servizi Novell Consulting prima di finalizzare l'architettura Sentinel. Le seguenti raccomandazioni possono essere utilizzate a titolo di riferimento.

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

Per impedire colli di bottiglia del traffico di rete, gli host distribuiti devono essere connessi agli altri host del server Sentinel tramite un singolo switch ad alta velocità (GIGE).

Novell consiglia di installare Crystal Reports Server in un computer dedicato, soprattutto se il database è di grandi dimensioni o se si fa un utilizzo intenso della funzionalità di generazione di rapporti. Crystal può essere installato sullo stesso computer del database se il database è di piccole dimensioni, l'utilizzo della generazione di rapporti è minimo e il database è installato in Windows o Linux (non Solaris). Le configurazioni suggerite di seguito rappresentano implementazioni di piccole, medie e grandi dimensioni ma si basano su Sentinel 5.1.3. Le raccomandazioni aggiornate verranno pubblicate sul sito della documentazione Novell all'indirizzo http://www.novell.com/documentation/sentinel61 (http://www.novell.com/documentation/sentinel61) al completamento dei test.

Tabella 2-4 *Configurazione con due computer, utilizzata per 1-500 EPS*

1-500 EPS: configurazione con due computer			
Componenti	**RAM**	**Spazio**	**CPU**
Computer 1: server Sentinel/ Gestione servizi di raccolta ◆ Motore di correlazione ◆ DAS ◆ Communication Server ◆ Advisor ◆ Gestione servizi di raccolta/ Servizi di raccolta ◆ Database ◆ Crystal Reports Server (facoltativo per Windows/ Linux)	6 GB	300 GB	Windows o Linux - 2 x Dual Core Intel® Xeon® 5150 (2.66 GHz) oppure Sun Solaris - 4 x UltraSPARC IIIi (1.5 GHz)
Computer 2: Report Server ◆ Crystal Reports Server	2 GB	20 GB	Windows o Linux - 1 x Dual Core Intel® Xeon® 5150 (2.66 GHz)

Tabella 2-5 *Configurazione con tre computer, utilizzata per 500-1500 EPS*

500 – 1500 EPS: configurazione con tre computer			
Componenti	**RAM**	**Spazio**	**CPU**
Computer 1: server Sentinel/Gestione servizi di raccolta ◆ Motore di correlazione ◆ DAS ◆ Communication Server ◆ Advisor ◆ Gestione servizi di raccolta/Servizi di raccolta	4 GB	90 GB	Windows o Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) oppure Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Computer 2: Database ◆ Database ◆ Crystal Reports Server (facoltativo per Windows/Linux)	4 GB+	1 TB+	Windows o Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) oppure Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Computer 3: Report Server (necessario solo se Sentinel/Database sono su Solaris) ◆ Crystal Reports Server	2 GB	20 GB	Windows o Linux - 1 x Dual Core Intel® Xeon® 5150 (2.66 GHz)

Tabella 2-6 *Configurazione con 4-5 computer, utilizzata per 1500-3000 EPS*

1500 - 3000 EPS: configurazione con 4-5 computer			
Componenti	**RAM**	**Spazio**	**CPU**
Computer 1: server Sentinel ◆ Motore di correlazione ◆ DAS ◆ Communication Server ◆ Advisor	4 GB	90 GB	Windows o Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) oppure Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Computer 2: Database ◆ Database ◆ Crystal Reports Server (facoltativo per Windows/Linux)	8 GB+	3 TB+	Windows o Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) oppure Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Computer 3: Gestione servizi di raccolta ◆ Gestione servizi di raccolta/Servizi di raccolta	2 GB	20 GB	Windows o Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) oppure Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Computer 4: Report Server ◆ Crystal Reports Server	4 GB	20 GB	Windows o Linux - 1 x Dual Core Intel® Xeon® 5150 (2.66 GHz)
Computer 5: istanza aggiuntiva di DAS_Binary (necessaria se EPS > 2000) Per le istruzioni sulla configurazione, vedere Capitolo 6, “Aggiunta di componenti di Sentinel”, a pagina 83.	2 GB	40 GB	Windows o Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+

Installazione di Sentinel 6.1

3

3.1 Panoramica sul programma di installazione

In questa sezione viene descritto come installare i componenti principali del sistema Sentinel. Il programma di installazione consente di eseguire un'installazione semplice o personalizzata. L'installazione semplice consente di installare tutti i componenti su un solo computer per eseguire dimostrazioni o programmi di formazione. Per l'installazione semplice vengono utilizzate numerose impostazioni di default minime. Per tale motivo, non è adatta per l'ambiente di produzione. L'installazione personalizzata può essere utilizzata per installare uno o più componenti Sentinel alla volta e per le installazioni distribuite di produzione.

Oltre ai componenti Sentinel, numerose altre applicazioni possono far parte del sistema Sentinel:

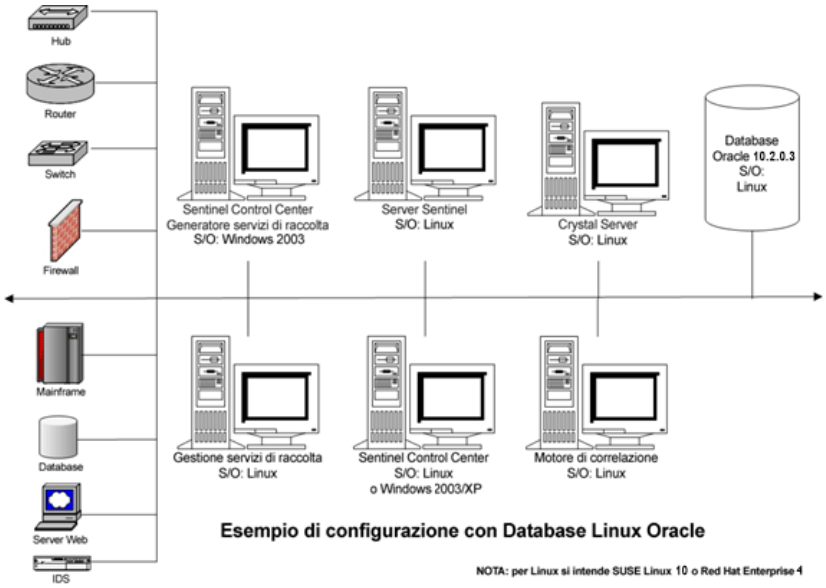
- **Database:** Il database in cui vengono memorizzati gli eventi, gli eventi correlati e le informazioni di configurazione è una parte essenziale del sistema Sentinel. Per installare il database, attenersi alle procedure consigliate da Oracle e Microsoft relative all'installazione di database, alla loro struttura di directory e così via.
- **Crystal Reports Server:** Crystal (e il server Web e database associati) viene utilizzato per eseguire rapporti dalla libreria dei rapporti di Novell o rapporti personalizzati. Per l'installazione dei componenti Crystal è necessario eseguire un programma di installazione separato. Per ulteriori informazioni sull'installazione di Crystal, vedere le sezioni Capitolo 8, “Crystal Reports per Windows”, a pagina 97 e Capitolo 9, “Crystal Reports per Linux”, a pagina 125.
- **Crystal Reports Developer:** Questa applicazione viene utilizzata per creare e modificare i rapporti.
- **Advisor:** Advisor fornisce informazioni in tempo reale sugli attacchi e le vulnerabilità, compreso il rilevamento in tempo reale degli exploit per determinare le minacce in corso contro i sistemi vulnerabili. Questo modulo è facoltativo. Per ulteriori informazioni su Advisor e sul programma di installazione per l'istantanea dei dati principali di Advisor, vedere Capitolo 4, “Configurazione di Advisor”, a pagina 63.
- **Integrazione con applicazioni di terze parti:** Sentinel si integra con HP OpenView Service Desk.

Nota: L'integrazione di Remedy Service Desk era disponibile in precedenza come un'opzione del programma di installazione. In Sentinel 6.1, l'integrazione di Remedy si ottiene mediante un plug-in Integratore e non è più inclusa nel programma di installazione di Sentinel. Se si dispone dell'opportuna licenza, è possibile scaricare Remedy Integrator e l'azione associata dal sito Web di contenuto all'indirizzo http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html).

3.2 Configurazioni di Sentinel

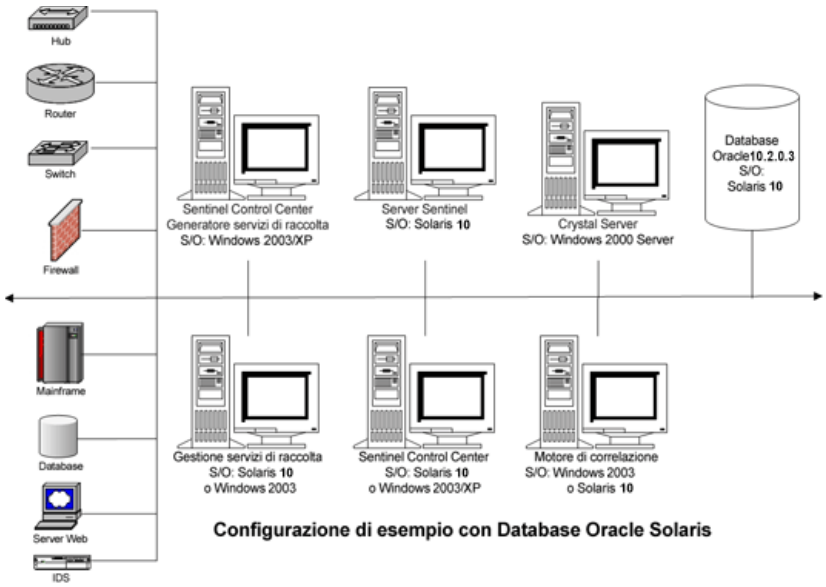
Di seguito vengono descritte alcune configurazioni tipiche di Sentinel. Su Linux

Figura 3-1 *Configurazione di Sentinel su Linux*



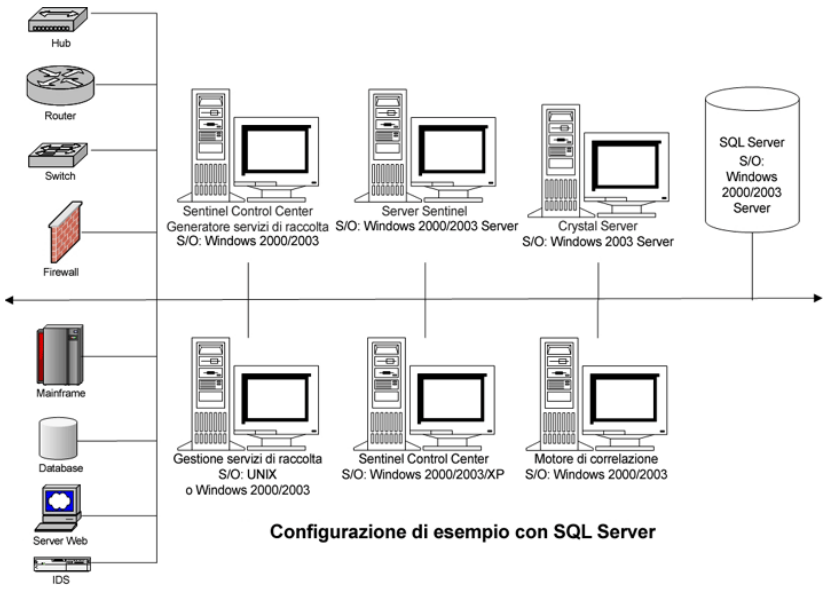
3.2.1 In Solaris

Figura 3-2 *Configurazione di Sentinel su Solaris*



3.2.2 In Windows

Figura 3-3 *Configurazione di Sentinel su Windows*



3.3 Prerequisiti generali di installazione

Di seguito vengono illustrati i vari passaggi che è necessario eseguire prima di installare Sentinel. Per ulteriori informazioni su molti di questi prerequisiti (compreso l'elenco delle piattaforme certificate), vedere Capitolo 2, “Requisiti di sistema”, a pagina 21.

- Assicurarsi che ogni computer nell'architettura Sentinel soddisfi i requisiti minimi di sistema.
- Assicurarsi che i sistemi operativi per tutti i componenti del sistema siano piattaforme certificate e che il sistema operativo sia stato "rafforzato" applicando le procedure consigliate di sicurezza.
- Se l'installazione viene eseguita su SUSE Linux Enterprise Server 10, accertarsi che SLES utilizzi il file system ext3.
- Se l'installazione di Gestione servizi di raccolta viene eseguita su un computer a 64 bit, accertarsi 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.
- È necessario installare il pacchetto SUNWxcu4 sul computer Solaris prima di installare Sentinel 6.1.
- Accertarsi che sia installato un database certificato Sentinel. Se si utilizza Oracle, è necessaria l'Enterprise Edition con partizionamento per garantire il funzionamento dell'archivio dati. Per ulteriori informazioni sulle versioni certificate, vedere Capitolo 2, “Requisiti di sistema”, a pagina 21.
- Richiedere i numeri di serie e i codici di licenza di Sentinel, Crystal Reports Server e Crystal Reports Developer al Customer Center di Novell (https://secure-www.novell.com/center/regadmin). Se è stato acquistato il feed dei dati facoltativo per il rilevamento degli exploit di Advisor, verificare nel Customer Center che tale sottoscrizione ai dati sia elencata insieme agli altri prodotti Novell.
- Installare e configurare un server SMTP per poter inviare notifiche e-mail dal sistema Sentinel.
- Creare una directory con caratteri solo ASCII (senza caratteri speciali) dalla quale eseguire il programma di installazione.
- Fornire i privilegi di Power User a "utente di dominio".

Le installazioni complete di Sentinel mediante il programma di installazione devono essere sempre eseguite su sistemi "puliti". Se Sentinel 6 è stato già installato su uno dei computer, Novell consiglia di seguire le procedure di disinstallazione illustrate in Capitolo 10, “Disinstallazione di Sentinel”, a pagina 141. Per informazioni sulla disinstallazione delle precedenti versioni di Sentinel, vedere le guide di installazione rilevanti sul sito Web della documentazione di Novell (http://www.novell.com/documentation/).

Nota: Le istruzioni relative all'upgrade da una versione precedente di Sentinel 6 a Sentinel 6.1 sono incluse nel programma di installazione delle patch.

3.3.1 Trasmissione dei privilegi di Power User agli "utenti di dominio"

Importante: Se si installa Sentinel come utente di dominio, dove l'utente non fa parte del gruppo di amministratori nel computer Active Directory e del computer locale, l'utente di dominio deve essere un Power User per poter avviare i Servizi Sentinel.

Per fornire i privilegi di Power User agli utenti di dominio:

1. Fare clic con il pulsante destro del mouse su Risorse del computer e selezionare Gestione.
2. Nella finestra Gestione computer, selezionare Locale > Utenti e gruppi > Gruppi.
3. Fare doppio clic su Power User e aggiungere l'utente di dominio nel formato "dominio/utente di dominio" nel sistema locale in cui è installato Sentinel utilizzando questo utente di dominio.

3.3.2 Prerequisiti di installazione del database di Sentinel

Prima di installare i componenti del database di Sentinel, è necessario attenersi ai passaggi descritti di seguito e raccogliere le informazioni seguenti.

Prerequisiti di installazione del database di Linux/Solaris per Sentinel

- Se l'installazione viene eseguita su SLES 10, il file system per il sistema operativo deve essere ext3.
- Su Linux/Solaris, è necessario che il database di Oracle sia installato e in esecuzione.
- Su Linux/Solaris, è necessario che il client JDBC Oracle (`ojdbc14.jar`) sia installato sul computer dal quale si sta eseguendo il programma di installazione. Se il programma di installazione di Sentinel viene eseguito sul computer del database, è necessario che il programma di installazione del database abbia già installato un client JDBC compatibile. Se il programma di installazione di Sentinel viene eseguito su un altro computer, è necessario creare manualmente l'istanza del database e installare manualmente il client JDBC compatibile sul computer mediante il programma di installazione. Anche se i driver Oracle aggiornati devono essere compatibili con le versioni precedenti, sono stati eseguiti test Sentinel sui driver forniti con il database di Oracle (ad esempio, i driver 10.2.0.3 sono stati testati con il database 10.2.0.3).

  Nota: Sentinel non è in grado di avviare il database di Oracle 10 a causa di errori negli script `dbstart` e `dbshut` di Oracle. È necessario modificare gli script `dbstart` e `dbshut` dopo aver installato Sentinel. Per ulteriori informazioni sulla modifica di questi script, vedere Sezione 3.8.7, “Modifica degli script Oracle dbstart e dbshut”, a pagina 60.

Nota: ai fini delle prestazioni, in caso di installazione in RAID e se l'ambiente RAID lo consente, si consiglia vivamente di configurare il sistema in modo che il log delle transazioni punti al disco di scrittura più veloce a disposizione, ovvero un disco fisico separato in cui vengono memorizzati i file del database.

- Si consiglia di consentire al programma di installazione di Sentinel di creare l'istanza del database di Oracle per Sentinel.
- Se necessario, la creazione dell'istanza del database può essere eseguita manualmente. Per assicurarsi che l'istanza sia compatibile con Sentinel, vedere Sezione B.2, "Creazione di istanza Oracle manuale (facoltativo)", a pagina 157. Se si sceglie questa opzione, è necessario eseguire lo script fornito da Novell `createEsecDBA.sh` e utilizzare il programma di installazione di Sentinel per aggiungere gli oggetti del database all'istanza del database di Oracle creata manualmente. Per ulteriori informazioni, vedere Sezione 3.6, "Installazione personalizzata", a pagina 45.

Nota: se si utilizza un'istanza di database Oracle esistente o creata manualmente, è necessario che sia vuota ad eccezione della presenza dell'utente del database di Sentinel.

- Richiedere le credenziali di login per l'utente del sistema operativo Oracle (default: oracle).
- Richiedere le credenziali di login per SYSTEM e SYS.
- Verificare che siano impostate le seguenti variabili di ambiente per il sistema operativo Oracle:
  - ORACLE_HOME (ad esempio, echo $ORACLE_HOME potrebbe produrre /opt/oracle/product/10gR2/db)
  - ORACLE_BASE (ad esempio, echo $ORACLE_BASE produce /opt/oracle)
  - PATH (deve includere $ORACLE_HOME/bin)
- Determinare un numero di porta del listener Oracle appropriato (il valore di default è 1521).
- Su Linux/Solaris, creare directory per le seguenti ubicazioni per la memorizzazione:
  - Directory dati
  - Directory indice
  - Directory dati di riepilogo
  - Directory indice di riepilogo
  - Directory temporanea e di annullamento operazioni
  - Directory di redo log membro A
  - Directory di redo log membro B
  - Directory archivio

Nota: È necessario che tali directory siano accessibili in scrittura dall'utente Oracle. Per rendere queste directory accessibili in scrittura all'utente Oracle, eseguire i comandi seguenti per ogni directory come utente radice:

chown –R oracle:dba <percorso_directory>

chmod –R 770 <percorso_directory>

- Dopo aver installato il database di Sentinel su Oracle, il database conterrà gli utenti seguenti:

- **esecdba:** Proprietario schema database. Il privilegio DBA non viene concesso all'utente del database di Sentinel per motivi di sicurezza. Per utilizzare Enterprise Manager, è pertanto necessario creare un utente con privilegi DBA.
- **esecapp:** Utente applicazione database. Corrisponde all'utente dell'applicazione utilizzata per la connessione al database.
- **esecadm:** Utente del database che corrisponde all'amministratore di Sentinel. Non corrisponde allo stesso conto utente utilizzato dall'utente amministratore di Sentinel del sistema operativo.
- **esecrpt:** Utente rapporti database
- **SYS:** Utente database SYS
- **SYSTEM:** Utente database SYSTEM

Prerequisiti di installazione del database di Windows per Sentinel

- Il database di SQL Server deve essere installato e in esecuzione.
- Sul sistema operativo del database, è necessario che sia disponibile il comando sc per avviare il servizio SQL Server Agent. In caso contrario, è necessario avviare manualmente il servizio SQL Server Agent per garantire il corretto funzionamento del partizionamento e dell'archiviazione dei dati. È inoltre necessario pianificare un riavvio mediante un'altra utility.
- Richiedere le credenziali di login per l'utente database amministratore di sistema
  - Se il database consente l'autenticazione SQL, l'utente amministratore del database di default è sa.
  - Se il database è solo in modalità di autenticazione di Windows, è necessario eseguire il programma di installazione dopo aver eseguito l'accesso a Windows come utente database amministratore di sistema.
- Impostare il servizio MSSQLSERVER per l'esecuzione del login mediante l'account di sistema locale.
- Determinare il nome dell'istanza di SQL Server, se applicabile.

  Nota: Se all'istanza viene assegnato un nome durante l'installazione di SQL Server, utilizzare tale nome quando viene richiesto il nome dell'istanza SQL Server durante l'installazione del database di Sentinel e/o dei componenti DAS. Se all'istanza non viene assegnato un nome durante l'installazione di SQL Server, lasciare il nome dell'istanza vuoto durante l'installazione, ovvero se si immette il nome host, non aggiungere"“\<nome_istanza>" al nome host del database.

- Creare directory per i seguenti percorsi di memorizzazione:
  - Directory dati
  - Directory indice
  - Directory dati di riepilogo
  - Directory indice di riepilogo
  - Directory log
  - Directory archivio
- Determinare il numero di porta dell'istanza SQL Server (il valore di default è 1433).

Il sistema Sentinel utilizza numerosi conti per l'installazione e il funzionamento del sistema. Tali conti sono presenti nel database di Sentinel e potrebbero utilizzare l'autenticazione di SQL Server o di Windows. Per utilizzare l'autenticazione di Windows per uno o più utenti Sentinel durante l'installazione di Sentinel, è necessario che sia presente il corrispondente utente di dominio di Windows prima di installare il database di Sentinel.

L'utente di dominio deve disporre dei privilegi di "Power User" per poter avviare i Servizi Sentinel. Per ulteriori informazioni, vedere Sezione 3.3.1, “Trasmissione dei privilegi di Power User agli "utenti di dominio"”, a pagina 35.

È possibile assegnare i seguenti utenti Sentinel a un utente di dominio di Windows:

- Amministratore del database di Sentinel, utilizzato come proprietario dello schema (denominato esecdba per default se si utilizza l'autenticazione di SQL, se si utilizza l'autenticazione di Windows, potrebbe essere qualsiasi account di dominio)
- Utente dell'applicazione di Sentinel, utilizzato dalle applicazioni Sentinel per connettersi al database (denominato esecapp per default se si utilizza l'autenticazione di SQL, se si utilizza l'autenticazione di Windows, potrebbe essere qualsiasi account di dominio)
- Amministratore Sentinel, utilizzato come amministratore per l'accesso a Sentinel Control Center (denominato esecadm per default se si utilizza l'autenticazione di SQL, se si utilizza l'autenticazione di Windows, potrebbe essere qualsiasi account di dominio)
- Utente dei rapporti di Sentinel utilizzato per la creazione di rapporti (denominato esecrpt per default se si utilizza l'autenticazione di SQL, se si utilizza l'autenticazione di Windows, potrebbe essere qualsiasi account di dominio)

Nota: Per default, il database contiene l'utente amministratore del database di Sentinel, l'utente dell'applicazione di Sentinel e l'utente amministratore Sentinel.

Sentinel non supporta la gestione in cluster di Microsoft o l'elevata disponibilità per Windows.

Dopo aver installato il database di Sentinel su SQL Server mediante l'autenticazione locale, il database conterrà i seguenti utenti:

- **esecdba:** Proprietario schema database. Il privilegio DBA non viene concesso all'utente del database di Sentinel per motivi di sicurezza. Per utilizzare Enterprise Manager, è pertanto necessario creare un utente con privilegi DBA.
- **esecapp:** Utente applicazione database. Corrisponde all'utente dell'applicazione utilizzata per la connessione al database.
- **esecadm:** Utente del database che corrisponde all'amministratore di Sentinel. Non corrisponde allo stesso conto utente utilizzato dall'utente amministratore di Sentinel del sistema operativo.
- **esecrpt:** Utente rapporti database
- **sa:** utente amministratore di sistema del database

3.3.3 Impostazioni della modalità di autenticazione su Microsoft SQL

In Windows, è necessario installare SQL Server con l'autenticazione in modalità mista per accedere a Sentinel Control Center utilizzando l'autenticazione di Windows o SQL Server. Se si installa SQL Server con l'autenticazione di Windows, sarà possibile effettuare il login solo mediante l'autenticazione di Windows.

Per modificare le impostazioni della modalità di autenticazione:

1. In Microsoft SQL Server Management Studio, fare clic con il pulsante destro del mouse sul server per il quale si desidera modificare le impostazioni.
2. Selezionare Proprietà e fare clic su Protezione.
3. Dalle opzioni della modalità di autenticazione SQL Server e Windows o autenticazione di Windows, selezionare l'opzione desiderata per l'autenticazione.

3.3.4 Prerequisiti di installazione del server Sentinel

Se il database di Sentinel non viene installato sullo stesso computer del server Sentinel, è necessario installare il database di Sentinel prima di installare gli altri componenti Sentinel.

3.3.5 Prerequisiti di installazione di Advisor

Per installare Advisor, è necessario acquistare le soluzioni facoltative per il rilevamento exploit di Sentinel e la sottoscrizione ai dati di Advisor. Al termine, eLogin Novell dispone dell'autorizzazione per scaricare e aggiornare i dati di Advisor.

Se si sceglie Download Internet diretto, aprire la porta 443 in uscita. Prevedere l'installazione del software Crystal Reports Server nel sistema per l'esecuzione dei rapporti.

Nota: Se si intende utilizzare Advisor solo per il rilevamento dell'exploit, non sarà necessario installare il software Crystal Reports Server. Per ulteriori informazioni sulle procedure di installazione, vedere Capitolo 4, “Configurazione di Advisor”, a pagina 63.

3.4 Installazione del database

È necessario rivolgersi a un DBA esperto per l'installazione di Oracle o SQL Server. In aggiunta alle raccomandazioni dal DBA, Novell fornisce inoltre alcune raccomandazioni per l'installazione di Oracle. Tali raccomandazioni interessano le aree seguenti:

- Impostazione dei valori del kernel
- Su Solaris e RHEL 4:
  - Creazione di un gruppo e di un conto utente per Oracle
  - Impostazione delle variabili di ambiente
  - Verifica del layout di Solaris
- Installazione di Oracle
- Applicazione delle patch a Oracle (se richiesto)

3.4.1 Impostazione dei valori del kernel

Avviso: ESCLUSIONI DI GARANZIA: I valori del kernel suggeriti in questa sezione si riferiscono solo ai valori minimi. Modificare queste impostazioni solo se le impostazioni di sistema sono inferiori ai valori minimi consigliati e solo dopo aver contattato l'amministratore di sistema e aver consultato la documentazione Oracle.

Per impostare i valori del kernel in Linux:

1. Eseguire il login come utente radice.
2. Creare una copia di backup di `/etc/sysctl.conf`.
3. Mediante un editor di testo, modificare i parametri del kernel aggiungendo il testo seguente alla fine del file "`/etc/sysctl.conf`":

   Nota: Le impostazioni kernel indicate di seguito sono le impostazioni minime consigliate. Tali impostazioni possono essere aumentate se l'hardware del computer può supportarle.

   Per determinare l'opzione correntemente impostata per un particolare parametro del kernel, eseguire il comando:

   ```
   sysctl <kernel_parameter>
   ```

   Per controllare ad esempio il valore corrente del parametro del kernel "kernel.sem", eseguire il comando: `sysctl kernel.sem`

   Solo su SUSE LINUX 10 SP2:

   ```
   # Oracle requires MLOCK privilege for hugetlb memory.
   vm.disable_cap_mlock=1
   ```

   Su REDHAT LINUX 4

   ```
   # Kernel settings for Oracle
   kernel.core_uses_pid = 1
   kernel.shmall = 2097152
   kernel.shmmax = 2147483648
   kernel.shmmni = 4096
   kernel.sem = 250 32000 100 128
   fs.file-max = 65536
   net.ipv4.ip_local_port_range = 1024 65000
   net.core.rmem_default = 262144
   net.core.rmem_max = 262144
   net.core.wmem_default = 262144
   net.core.wmem_max = 262144
   ```

4. Per caricare le modifiche nel file `/etc/sysctl.conf`, eseguire il comando seguente:

   ```
   sysctl -p
   /sbin/sysctl –p (on RedHat Linux4)
   ```

5. Impostare i file handle e i limiti dei processi aggiungendo il testo seguente alla fine del file "`/etc/security/limits.conf`". "nproc" rappresenta il limite massimo per il numero di processi e "nofile" il limite massimo per il numero di file aperti. I valori seguenti sono quelli consigliati. È possibile modificarli se necessario. Nel testo seguente si presume che l'ID utente di Oracle sia "oracle".

   ```
   # Settings added for Oracle
   oracle          soft    nofile  65536
   oracle          hard    nofile  65536
   oracle          soft    nproc   16384
   oracle          hard    nproc   16384
   ```

Per impostare i valori del kernel in Solaris 10:

Per Oracle 10g:

noexec_user_stack=1	semsys:seminfo_semvmx=32767
semsys:seminfo_semmni=100	shmsys:shminfo_shmmax=4294967295
semsys:seminfo_semmns=1024	shmsys:shminfo_shmmni=100
semsys:seminfo_semmsl=256	

1. Per default, le istanze di Oracle vengono eseguite come utente oracle del gruppo DBA. Viene creato un progetto con il nome `group.dba` da utilizzare come progetto di default per l'utente oracle. Eseguire il comando ID per verificare il progetto di default per l'utente oracle.

```
# su - oracle
$ id -p
uid=100(oracle) gid=100(dba) projid=100(group.dba)
$ exit
```

2. Per impostare la dimensione massima della memoria condivisa su 2 GB, eseguire il comando projmod

```
# projmod -sK "project.max-shm-memory=(privileged,2G,deny)"
group.dba
```

   In alternativa, aggiungere il controllo della risorsa project.max - `shm-memory=(privileged,2147483648,deny)` dell'ultimo campo delle voci del progetto per il progetto Oracle.

3. Al termine di tutti i passaggi, il file /etc/project dovrebbe contenere gli elementi descritti di seguito:

```
# cat /etc/project
```

4. Di seguito viene riportato l'output del comando:

```
system:0::::
user.root:1::::
noproject:2::::
default:3::::
group.staff:10::::
group.dba:100:Oracle default
project:::project.max-shmmemory=(privileged,2147483648,deny
```

5. Per verificare che il controllo risorsa sia attivo, eseguire i comandi ID e prctl:

```
# su - oracle
$ id -p
uid=100(oracle) gid=100(dba) projid=100(group.dba)
$ prctl -n project.max-shm-memory -i process $$
process: 5754: -bash
NAME PRIVILEGE VALUE FLAG ACTION RECIPIENT
project.max-shm-memory
privileged 2.00GB – deny
```

Nota: Per ulteriori informazioni, vedere la documentazione Oracle relativa all'installazione di Solaris 10.

3.4.2 Creazione di un gruppo e di un conto utente per Oracle (solo Solaris)

Per creare un gruppo e un conto utente e impostare le variabili di ambiente:

1. Eseguire il login come utente radice.
2. Creare un gruppo UNIX e un conto utente UNIX per il proprietario del database Oracle.
   - Aggiungere un gruppo dba (come utente radice):
     ```
     groupadd -g 400 dba
     ```
   - Aggiungere l'utente oracle (come root) per la shell csh:
     ```
     useradd -g dba -d /export/home/oracle -m -s /bin/csh oracle
     ```
   - Aggiungere l'utente oracle (come root) per la shell bash:
     ```
     useradd -g dba -d /export/home/oracle -m -s /bin/bash oracle
     ```

3.4.3 Impostazione delle variabili di ambiente per Oracle (solo Solaris)

Per impostare le variabili di ambiente:

1. Eseguire il login come utente radice.
2. Per impostare le variabili di ambiente necessarie per Oracle nella shell csh, è consigliabile aggiungere le informazioni seguenti nel file `local.cshrc`:
   ```
   setenv ORACLE_HOME /opt/oracle
   setenv ORACLE_SID ESEC
   setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
   setenv DISPLAY :0.0
   set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /
   usr/ucb/etc.)
   if ( $?prompt ) then
   set history=32
   endif
   ```
3. Per impostare le variabili di ambiente necessarie per Oracle nella shell bash, è consigliabile aggiungere le informazioni seguenti nel file `.profile` nella directory $ORACLE_HOME.
   ```
   setenv ORACLE_HOME /opt/oracle
   setenv ORACLE_SID ESEC
   setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
   setenv DISPLAY :0.0
   set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /
   usr/ucb/etc.)
   if ( $?prompt ) then
   set history=32
   endif
   ```

3.4.4 Installazione di Oracle

Per eseguire l'installazione di Oracle, vedere Appendice B, “Installazione di Oracle”, a pagina 153
In questa sezione vengono specificate le impostazioni di installazione consigliate per le operazioni Sentinel. Vengono inoltre descritte le procedure per la creazione dell'istanza Oracle. Novell

consiglia di creare l'istanza utilizzando il programma di installazione di Sentinel ma fornisce istruzioni nel caso in cui le norme aziendali richiedano la creazione manuale dell'istanza da parte del DBA.

3.5 Installazione semplice

L'opzione Installazione semplice è un'opzione unica che consente di installare contemporaneamente i Servizi Sentinel, Gestione servizi di raccolta e Applicazioni di Sentinel con il database sullo stesso computer. Questo tipo di installazione è solo a scopo dimostrativo o di formazione e se ne sconsiglia pertanto l'utilizzo negli ambienti di produzione.

Dopo aver eseguito l'installazione del database e aver soddisfatto i prerequisiti specificati nella sezione precedente, è possibile procedere con l'installazione di Sentinel. Se si sceglie l'opzione Installazione semplice, si presuppone l'utilizzo di una determinata procedura e di alcune impostazioni di default:

- In Windows, l'autenticazione SQL è consentita sul database di SQL Server.
- La stessa password viene utilizzata per l'amministratore del database di Sentinel, l'amministratore Sentinel, l'utente dell'applicazione Sentinel e l'utente dei rapporti di Sentinel.
- Advisor è configurato per l'utilizzo del Download Internet diretto.
- Advisor è impostato per scaricare nuove informazioni ogni 12 ore.
- Le notifiche e-mail di Advisor sono abilitate.
- La dimensione del database è 10 GB.

Per installare Sentinel:

1. Accedere come utente root in Solaris/Linux o utente Administrator in Windows.
2. Inserire e montare il CD di installazione di Sentinel.
3. Avviare il programma di installazione passando alla directory di installazione sul CD-ROM e
   - In Windows, eseguire `setup.bat`
   - In Solaris/Linux:

     Per la modalità GUI:

     ```
     ./setup.sh
     ```

     Oppure per la modalità testuale ("console seriale"):

     ```
     ./setup.sh –console
     ```

   Nota: Non è possibile eseguire il programma di installazione su UNIX da un percorso della directory contenente uno spazio.

4. Nel riquadro successivo, fare clic sulla freccia giù e selezionare una delle lingue seguenti.

Inglese	Italiano
Francese	Portoghese (Brasile)
Tedesco	Spagnolo
Cinese semplificato	Giapponese
Cinese tradizionale	

5 Dopo aver letto la schermata introduttiva, 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 il percorso di installazione. Fare clic su Avanti.

Nota: Non è possibile eseguire l'installazione in una directory con caratteri speciali o caratteri non ASCII. Quando ad esempio si installa Sentinel 6.1 su Windows x86-64, il percorso di default sarà C:\Programmi (x86). È necessario modificare il percorso di default per evitare i caratteri speciali e continuare l'installazione.

---

8 Selezionare Semplice. Fare clic su Avanti.

9 In questa finestra, fornire le informazioni di configurazione e fare clic su Avanti.

- Numero di serie
- Codice di licenza
- SMTP Server:
  - Sentinel invia e-mail tramite questo server.
- E-mail:
  - Il messaggio e-mail inviato da Sentinel viene visualizzato come se fosse inviato da questo indirizzo e-mail.
- Password di sistema globale
- La password inserita qui è valida per tutti gli utenti di default. Sono inclusi sia l'utente amministratore di Sentinel che gli utenti del database. Per ulteriori informazioni sull'elenco degli utenti del database di default creati durante l'installazione, vedere Sezione 3.8.2, “Database di Sentinel”, a pagina 58.
- Nome utente e password di Advisor (facoltativo)
  - Per installare Advisor, specificare una eLogin e una password Novell associate alla licenza Advisor. Specificare nuovamente la password Advisor nella finestra di conferma della password.

Nota: I nomi utente e le password forniti per Advisor prima di Sentinel 6.0 SP2 non sono più validi. È necessario utilizzare le credenziali eLogin e la password Novell associate alla licenza Advisor. Alcune organizzazioni dispongono di più di un utente con credenziali eLogin Novell. Per i download di Advisor è necessario utilizzare quelle ottenute all'acquisto di Advisor.

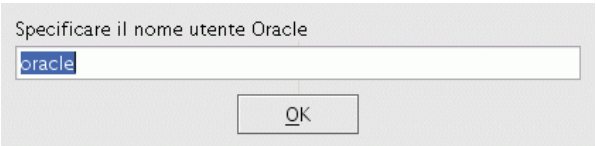
---

10 Per la configurazione del database:

- Selezionare la piattaforma del database di destinazione.

In Solaris/Linux, viene richiesto di specificare il nome utente Oracle. Fornire il nome utente e fare clic su OK.

Figura 3-4 *Specificare il campo nome utente Oracle*



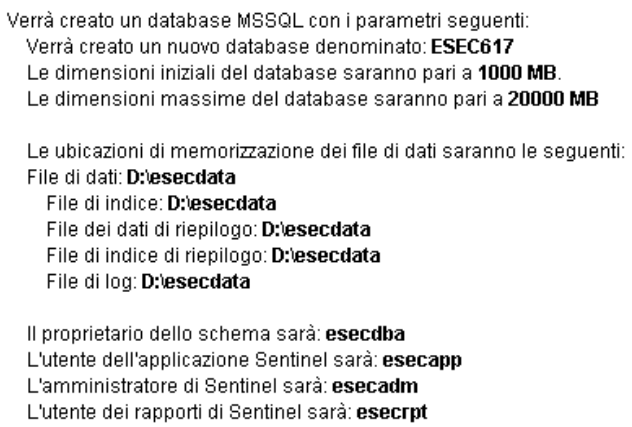
Fornire il nome del database

- Su Linux/Solaris, specificare il file del driver JDBC Oracle.
- In Windows, fornire le credenziali utente del database e il nome dell'istanza SQL Server.

Fare clic su Avanti.

Nota: Su Linux/Solaris, il programma di installazione esegue il backup dei file `tnsnames.ora` e `listener.ora` esistenti nella directory $ORACLE_HOME/network/admin. Il file `listener.ora` verrà sovrascritto con le informazioni di connessione del database di Sentinel, le quali verranno aggiunte al file `tnsnames.ora`. Se sullo stesso server del database di Sentinel sono presenti altri database, l'amministratore deve fondere manualmente le informazioni dai file `listener.ora` di cui è stato eseguito il backup nel nuovo file e riavviare il listener Oracle per consentire alle altre applicazioni di continuare a connettersi al database.

Figura 3-5 *Riepilogo dei parametri del database*



11. Riepilogo delle visualizzazioni selezionate dei parametri del database. Fare clic su Avanti.
12. Riepilogo delle visualizzazioni di installazione. Fare clic su Installa
13. Al termine dell'installazione, fare clic su Fine.
14. Riavviare il computer. I servizi pianificati, ad esempio lo scaricamento di Advisor, funzioneranno solo dopo aver riavviato il computer.

3.6 Installazione personalizzata

L'opzione Installazione personalizzata consente di effettuare un'installazione completamente distribuita, con maggior controllo sulla memoria e altre impostazioni di installazione. L'opzione Installazione personalizzata può essere utilizzata per installare uno o più componenti di Sentinel, tra cui:

- Componenti del database di Sentinel
- Servizi Sentinel
  - Communication Server
  - Advisor
  - Motore di correlazione

- Servizio DAS (Data Access Server)
- Servizio di raccolta Sentinel (Gestione servizi di raccolta)

- Applicazioni
  - Sentinel Control Center
  - Gestione dati Sentinel
  - Sentinel Solution Designer
- Integrazione di terze parti
  - HP OpenView Service Desk

Dopo aver soddisfatto i prerequisiti specificati nella sezione precedente, è possibile procedere con l'installazione di Sentinel.

I componenti del database di Sentinel devono sempre essere installati per primi. È possibile installare contemporaneamente altri componenti se l'architettura del sistema include più componenti sul computer del database. Nella procedura descritta di seguito vengono illustrati i passaggi necessari per l'installazione di tutti i componenti sullo stesso computer. Un'installazione distribuita includerà un sottoinsieme dei passaggi seguenti.

Per installare Sentinel:

1. Accedere come utente root in Solaris/Linux o utente Administrator in Windows.

   Nota: L'installazione del componente Database di Sentinel in Windows quando l'istanza MS SQL Server di destinazione è in modalità solo di autenticazione di Windows richiede l'accesso a Windows come utente amministratore di sistema del database.

2. Inserire e montare il CD di installazione di Sentinel.
3. Avviare il programma di installazione passando alla directory di installazione sul CD-ROM e
   - In Windows, eseguire `setup.bat`
   - In Solaris/Linux:

     Per la modalità GUI:

     `./setup.sh`

     Oppure per la modalità testuale ("headless"):

     `./setup.sh –console`

     Nota: Non è possibile eseguire il programma di installazione su UNIX da un percorso della directory contenente uno spazio.
4. Nel riquadro successivo, fare clic sulla freccia giù e selezionare una delle lingue seguenti.

Inglese	Italiano
Francese	Portoghese (Brasile)
Tedesco	Spagnolo
Cinese semplificato	Giapponese
Cinese tradizionale	

5 Dopo aver letto la schermata introduttiva, fare clic su Avanti.

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

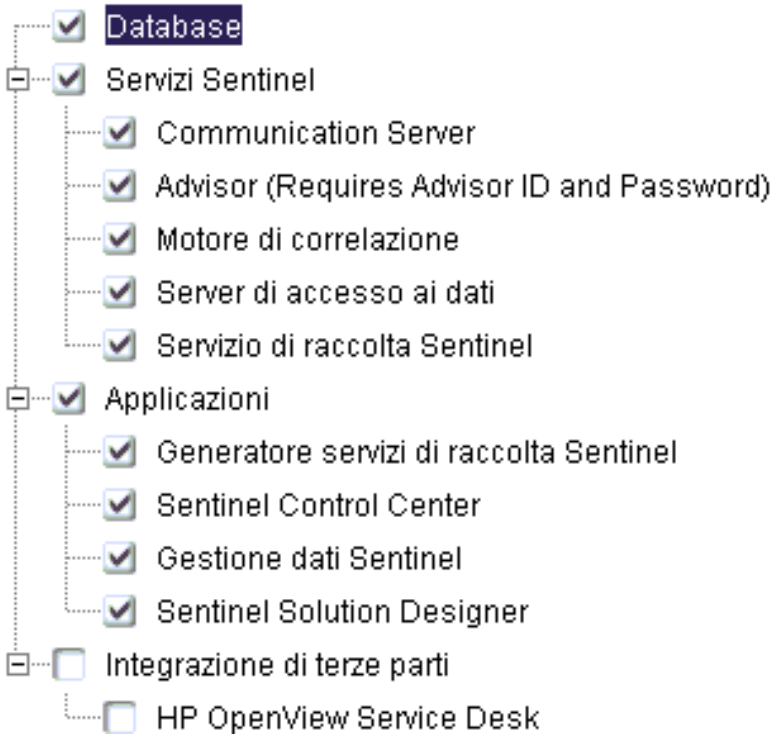
7 Accettare la directory di installazione di default o fare clic su Sfoglia per specificare il percorso di installazione. Fare clic su Avanti.

Nota: Non è possibile eseguire l'installazione in una directory con caratteri speciali o caratteri non ASCII.

---

8 Selezionare Personalizzata. Fare clic su Avanti.

9 Selezionare i componenti di Sentinel da installare.



Sono disponibili le seguenti opzioni:

Componente	Descrizione
Database	Installa gli oggetti del database di Sentinel (tabelle, visualizzazioni, procedure memorizzate e così via) in un'istanza del database. Eventualmente crea prima l'istanza del database.
Communication Server	Installa il bus messaggio (iSCALE) e il proxy DAS
Motore di correlazione	Installa il motore di correlazione.
Advisor	Installa i componenti correlati al servizio di sottoscrizione ai dati di Advisor. Richiede una licenza Advisor e deve risiedere sullo stesso computer di DAS.

Componente	Descrizione
Servizio DAS (Data Access Server)	Installa i componenti che comunicano con il database di Sentinel. Richiede un codice di licenza Sentinel e un numero di serie (obbligatori se si installa Advisor).
Servizio di raccolta Sentinel	Installa la Gestione servizi di raccolta che gestisce le connessioni alle origini eventi, l'analisi sintattica dei dati, la mappatura e così via.
Sentinel Control Center	Installa la console principale per gli analisti della sicurezza o della conformità.
Gestione dati Sentinel (Sentinel Data Manager, SDM)	Installa SDM, utilizzato per le attività di gestione manuale del database.
Solution Designer	Installa Solution Designer
HP OpenView Service Desk	Installa l'integrazione con HP OpenView Service Desk. Richiede una licenza.

Nota: Quando si seleziona o deseleziona un componente, nell'interfaccia si verifica un ritardo.

Nota: Se nessuna delle funzioni secondarie dei Servizi Sentinel è selezionata, deselezionare anche la funzione Servizi Sentinel. Verrà visualizzata in grigio (non disponibile) con un segno di spunta bianco se è ancora selezionata ma tutte le relative funzioni secondarie sono state deselezionate.

Nota: Come parte dell'installazione del componente del database di Sentinel, il programma di installazione inserirà i file nella cartella %ESEC_HOME%\ unist\db.

Nota: Se si utilizza la modalità "console", nella pagina di selezione dei componenti non verranno visualizzati tutti i componenti contemporaneamente. Seguire le istruzioni riportate sullo schermo per visualizzare e modificare i componenti secondari selezionati. Non tutti i componenti secondari sono selezionati per default. Per ulteriori informazioni, vedere il Sezione 3.6.1, “Installazione della console in Linux/Solaris”, a pagina 56.

10 Se è stato selezionato di installare il servizio DAS, verrà richiesto quanto segue:

- Numero di serie
- Codice di licenza

11 Su linux/Solaris, specificare il nome utente dell'amministratore Sentinel del sistema operativo e l'ubicazione della relativa home directory. Si tratta del nome dell'utente proprietario del prodotto Sentinel installato. Se l'utente non è già esistente, ne verrà creato uno insieme alla home directory nella directory specificata.

- Nome utente amministratore Sentinel sistema operativo – Il valore di default è esecadm
- Home directory utente amministratore Sentinel sistema operativo – Il valore di default è "/export/home" Se esecadm è il nome utente, la home directory dell'utente sarà /export/home/esecadm.

Nota: Per soddisfare i severi requisiti relativi alle configurazioni di sicurezza dello standard Common Criteria Certification.

Nota: L'utente esecadm verrà creato senza dover impostare una password. Per eseguire il login come questo utente, è prima necessario impostare la relativa password.

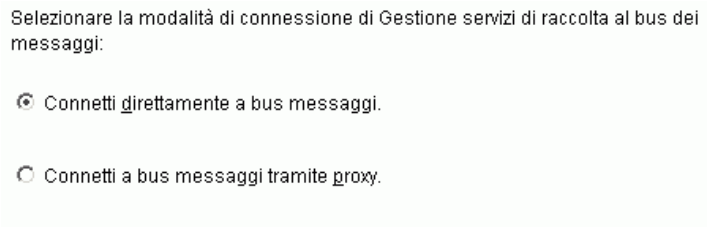
12 Se si sceglie di installare Sentinel Control Center, verrà richiesto di impostare lo spazio massimo di memoria da allocare a Sentinel Control Center. Specificare le dimensioni massime dell'heap JVM (MB) da utilizzare solo per Sentinel Control Center.

- **Dimensioni dell'heap JVM (MB):** per default questo valore è pari a 256 e il valore massimo è 1024 MB.

13 Se viene selezionata l'installazione di Gestione servizi di raccolta ma non quella di Data Access Server (DAS), sono disponibili due opzioni per stabilire la comunicazione tra le istanze di Gestione servizi di raccolta di Sentinel e il server Sentinel. È possibile selezionare una comunicazione diretta tramite un bus messaggi o una comunicazione tramite proxy. Per ulteriori informazioni su queste due opzioni, vedere il Capitolo 7, “Layer di comunicazione (iSCALE)”, a pagina 91.

Nota: Se viene selezionata la comunicazione tramite proxy, non appena termina l'installazione vengono richieste informazioni per la registrazione del servizio Gestione servizi di raccolta come client attendibile. A tale scopo è necessario che Communication Server sia in esecuzione.

Se Communication Server non è disponibile, selezionare il tipo di comunicazione diretta tramite bus messaggi e successivamente configurare manualmente una comunicazione tramite proxy eseguendo Passo 26 a pagina 55 (Configurazione della comunicazione tramite proxy).



14 Viene chiesto di specificare la porta o il server host per Communication Server. Immettere le informazioni richieste e fare clic su Avanti.

- **Porta bus messaggi:** la porta sulla quale rimane in ascolto il server di comunicazione. I componenti che si connettono direttamente al server di comunicazione utilizzano questa porta.

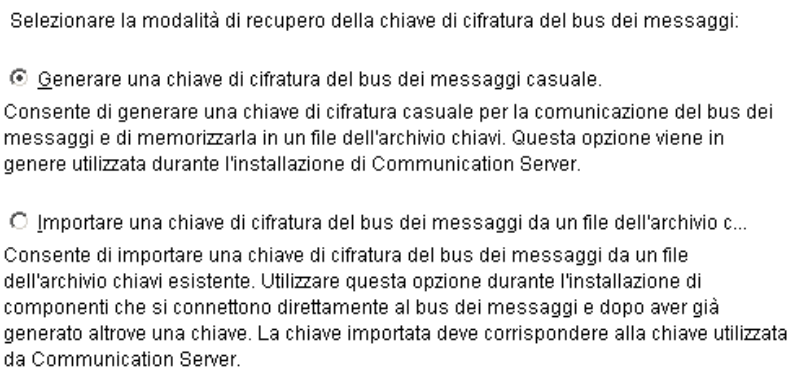
- **Porta proxy di Sentinel Control Center:** la porta sulla quale rimane in ascolto il server proxy SSL (proxy DAS) per accettare il nome utente e la password attraverso connessioni autenticate. Poiché Sentinel Control Center richiede l'immissione di un nome utente e di una password, utilizza questa porta per connettersi al server Sentinel.
- **Porta di autenticazione certificato di Gestione servizi di raccolta:** la porta sulla quale il server proxy SSL (proxy DAS) rimane in ascolto per accettare il certificato attraverso connessioni autenticate. Poiché Gestione servizi di raccolta non può richiedere l'immissione di un nome utente e di una password, utilizza questa porta per connettersi al server Sentinel se è configurato per connettersi attraverso il proxy.

Nota: Per consentire le comunicazioni, il numero di porta deve essere lo stesso su ogni computer del sistema Sentinel. Annotare il numero di queste porte per installazioni future su altri computer.

---

15 Se si installa un componente che stabilisce una connessione diretta al bus messaggi o se si installa Communication Server, verrà chiesto di indicare come ottenere la chiave di cifratura condivisa del bus messaggi:

- Generazione di una chiave di cifratura casuale
- Importazione di una chiave di cifratura del bus messaggi dal file dell'archivio chiavi. Verrà chiesto di selezionare l'ubicazione di un file .keystore esistente.



Nota: Tutti i componenti che si connettono direttamente al bus messaggi devono condividere la stessa chiave di cifratura. Novell consiglia di generare una chiave di cifratura casuale quando si installa Communication Server e di importare questa chiave durante l'installazione di componenti su altri computer. I componenti che si connettono attraverso il proxy non richiedono una chiave di cifratura condivisa del bus messaggi.

Il file .keystore verrà collocato in $ESEC_HOME/config (Linux/Solaris) o %ESEC_HOME%\config (Windows).

---

16 Selezionare la piattaforma server del database di destinazione. Fare clic su Avanti. Se si sceglie di installare DAS e i componenti del database di Sentinel sono già installati, verrà chiesto di immettere le seguenti informazioni per il database di Sentinel. Queste informazioni saranno utilizzate per configurare DAS in modo che venga diretto al database di Sentinel.

- **Nome host del database o indirizzo IP:** nome o indirizzo IP del database di Sentinel esistente dove sono memorizzate le informazioni riguardanti gli eventi e la configurazione.

- **Nome database:** il nome dell'istanza del database di Sentinel per cui configurare il componente DAS per la connessione (impostazione di default: ESEC).
- **Porta database:** (default: Microsoft SQL Server:1433 e Oracle:1521)
- **Utente del database dell'applicazione Sentinel:** specificare il login per l'utente dell'applicazione Sentinel (per default, esecapp) e la password assegnata a questo utente durante l'installazione del database di Sentinel.

Fare clic su Avanti.

17 Se si sceglie di installare il database, configurarlo per l'installazione:

In Windows:

- Selezionare Microsoft SQL Server 2005 o Microsoft SQL Server 2008 come piattaforma server di database di destinazione.
  - **Creare un nuovo database con oggetti di database:** creare un nuovo database Microsoft SQL e popolare il nuovo database con oggetti di database
  - **Aggiungi oggetti di database a un database vuoto esistente:** aggiungere oggetti di database solo a un database Microsoft SQL 2005 esistente. Il database esistente deve essere vuoto.
  - Specificare la directory log di installazione del database.

  Fare clic su Avanti.
- Se viene creato un nuovo database, specificare le directory esistenti da utilizzare per la memorizzazione di:
  - Directory dati
  - Directory indice
  - Directory dati di riepilogo
  - Directory indice di riepilogo
  - Directory log

  Fare clic su Avanti.
- Se viene creato un nuovo database, selezionare l'opzione di supporto del set di caratteri del database, ovvero Unicode o solo ASCII. Se il programma di installazione è eseguito in una lingua asiatica, per default viene selezionata l'opzione Unicode. Se il programma di installazione è eseguito in una lingua non asiatica, il sistema chiede di selezionare solo ASCII o Unicode. Selezionare un formato per il database e fare clic su OK.

  Nota: L'installazione di un database Unicode richiede maggiore spazio sul disco rigido rispetto all'installazione di un database solo ASCII.

- Se si crea un nuovo database, selezionare un'opzione per le dimensioni del database. Fare clic su Avanti.
- Se si crea un nuovo database e viene selezionata una dimensione personalizzata del database, specificare le seguenti dimensioni per il database personalizzato:
  - **Dimensioni massime database:** spazio massimo sul disco rigido occupato dal database. Man mano che si accumulano i dati, le dimensioni del database cresceranno automaticamente fino a raggiungere questo valore. Indipendentemente dal valore specificato in questo campo, il database avrà dimensioni iniziali di 1000 MB.

- **Dimensioni file di log:** dimensioni del file di log delle transazioni.
- **Dimensioni massime file di database:** nessun file singolo di database potrà superare queste dimensioni.

Fare clic su Avanti.

In Linux/Solaris:

- Selezionare la versione del server del database Oracle di destinazione e selezionare una delle seguenti opzioni:
  - **Creare un nuovo database con oggetti di database:** creare una nuova istanza di database Oracle e popolare il nuovo database con oggetti di database
  - **Aggiungi oggetti di database a un database vuoto esistente:** aggiungere oggetti di database solo a un'istanza di un database Oracle esistente. Il database esistente deve essere vuoto a parte la presenza dell'utente esecdba.
  - Specificare la directory log di installazione del database.

  Fare clic su Avanti.
- Specificare il nome utente Oracle o accettare il nome utente di default. Fare clic su OK.
- Se si è scelto di creare un nuovo database, immettere le seguenti informazioni:
  - **Percorso del file del driver JDBC Oracle:** specificare il percorso completo del file jar, normalmente è `$ORACLE_HOME/jdbc/lib/ojdbc14.jar` (non utilizzare però variabili di ambiente in questo campo).
  - **Nome host:** nome host del computer locale, dove è installato il database Oracle. Il programma di installazione supporta solo la creazione di una nuova istanza di database sull'host locale.
  - **Nome database:** nome dell'istanza di database da creare.
- Se si è scelto di aggiungere oggetti di database a un database Oracle vuoto esistente, viene chiesto di immettere le seguenti informazioni:
  - **Percorso del file del driver JDBC Oracle:** specificare il percorso completo del file jar, normalmente è `$ORACLE_HOME/jdbc/lib/ojdbc14.jar` (non utilizzare però variabili di ambiente in questo campo).
  - **Indirizzo IP o nome host del database:** nome host o indirizzo IP del computer dove è installato il database Oracle. Può essere il nome host locale o un nome host remoto.
  - **Nome database:** nome dell'istanza di database Oracle vuota esistente (default, ESEC) Questo database deve essere visualizzato come un nome di servizio nel file `tnsnames.ora` (all'interno della directory $ORACLE_HOME/network/admin/) del computer dal quale si sta eseguendo il programma di installazione.
  - **Porta database:** il valore di default è 1521
  - **Password:** per l'utente amministratore del database di Sentinel (DBA), specificare la password per l'utente "esecdba". Il campo Nome utente visualizzato non può essere modificato.

Nota: Se il nome del database non è specificato nel file `tnsnames.ora`, il programma di installazione non genera un errore in questa fase dell'installazione (poiché verifica la connessione utilizzando una connessione JDBC diretta), ma quando il programma di installazione del database prova a connettersi al database attraverso sqlplus l'installazione del database non potrà essere portata a termine. Se l'installazione del database non riesce

in questa fase dell'installazione, senza uscire dal programma di installazione modificare il nome del servizio per il database nel file `tnsnames.ora` del computer corrispondente, quindi ritornare alla prima finestra del programma di installazione e continuare con l'installazione. In questo modo verrà rieseguita l'installazione del database utilizzando i nuovi valori specificati nel file `tnsnames.ora`.

Nota: Il programma di installazione eseguirà il backup di eventuali file `tnsnames.ora` e `listener.ora` nella directory $ORACLE_HOME/network/admin. Il file `listener.ora` verrà sovrascritto con le informazioni di connessione del database di Sentinel, che verranno aggiunte al file `tnsnames.ora`. Se sono presenti altri database sullo stesso server del database di Sentinel, l'amministratore dovrà aggiungere manualmente le informazioni contenute nelle copie di backup dei file `listener.ora` al nuovo file e riavviare il listener Oracle affinché le altre applicazioni possano continuare a connettersi al database.

- Se si crea una nuova istanza di database, specificare l'allocazione di memoria (RAM) Oracle e la porta del listener o accettare i valori di default.
- Se si crea una nuova istanza di database, specificare le password da impostare per gli utenti di database di default SYS e SYSTEM. Fare clic su Avanti.
- Se si crea una nuova istanza di database, selezionare un'opzione per le dimensioni del database. Fare clic su Avanti.
- Se si crea una nuova istanza di database e viene selezionata una dimensione personalizzata del database, specificare le seguenti dimensioni per il database personalizzato:
  - **Dimensioni database massime:** spazio massimo sul disco rigido occupato dal database. Man mano che si accumulano i dati, le dimensioni del database cresceranno automaticamente fino a raggiungere questo valore. Indipendentemente dal valore specificato in questo campo, il database avrà dimensioni iniziali di 5000 MB.
  - **Dimensioni file di log:** dimensioni di ciascun file di redo log
  - **Dimensioni massime file di database:** nessun singolo file di database potrà superare queste dimensioni.
- Se si crea una nuova istanza di database, specificare le directory esistenti da utilizzare per la memorizzazione del database:
  - Directory dati
  - Directory indice
  - Directory dati di riepilogo
  - Directory indice di riepilogo
  - Directory temporanea e di annullamento operazioni
  - Directory di redo log membro A
  - Directory di redo log membro B

  Fare clic su Avanti.

Nota: Per consentire il recupero e migliorare le prestazioni, è consigliabile che tali ubicazioni si trovino su dispositivi di I/O diversi.

Per migliorare le prestazioni, il redo log deve rimandare al disco di scrittura più veloce disponibile.

Il programma di installazione non crea queste directory. È quindi necessario crearle esternamente prima di superare questo punto dell'installazione e l'utente Oracle deve disporre di diritti di scrittura su queste directory. Per ulteriori informazioni, vedere la Sezione 3.3.2, “Prerequisiti di installazione del database di Sentinel”, a pagina 35.

18 Se si sceglie di installare il componente del database, configurare le partizioni del database.

- Selezionare l'opzione per l'abilitazione della gestione automatica delle partizioni del database per consentire a Gestione dati Sentinel di occuparsi dell'archiviazione e della partizione del database.
- Per partizioni di dati, specificare una directory esistente per i file archivio.
- Specificare l'ora di inizio per l'aggiunta di partizioni e dati di archiviazione. Queste operazioni non dovrebbero sovrapporsi poiché utilizzano risorse condivise.

Fare clic su Avanti.

19 Se si sceglie di installare il componente del database, fornire informazioni di autenticazione per:

- Utente amministratore del database di Sentinel
- Utente di database dell'applicazione Sentinel
- Utente amministratore di Sentinel
- Utente dei rapporti di Sentinel (solo in Windows)

Nota: Se viene installato anche il componente DAS, è richiesta l'immissione della password dell'utente del database dell'applicazione Sentinel anche se è selezionata l'autenticazione Windows. Ciò è richiesto per installare il servizio Sentinel in modo che esegua il login come utente del database dell'applicazione Sentinel. Se viene utilizzata l'autenticazione Windows, non è necessario specificare una password per altri utenti.

Fare clic su Avanti.

20 Se si sceglie di installare il componente del database, viene visualizzato un riepilogo dei parametri specificati per il database. Fare clic su Avanti.

21 Se si decide di installare componenti del server Sentinel, verrà chiesto di specificare la quantità di memoria (RAM) da allocare a questi componenti. Il programma di installazione terrà conto dei requisiti del sistema operativo e del database per stabilire le opzioni di allocazione di memoria da visualizzare. È possibile specificare l'allocazione di memoria in due modi:

- **Configurazione memoria automatica:** selezionare la quantità di memoria totale da allocare al server Sentinel. Il programma di installazione determina automaticamente la distribuzione ottimale della memoria tra i componenti tenendo conto dei requisiti previsti per il sistema operativo e il database.

  Importante: È possibile modificare il valore Xmx nel file `configuration.xml` per modificare la RAM allocata ai processi del server Sentinel. Il file `configuration.xml` è situato in `$ESEC_HOME/config` (Linux/Solaris) o `%ESEC_HOME%\config` (Windows).

- **Configurazione memoria personalizzata:** fare clic sul pulsante Configura... per impostare accuratamente i valori di allocazione della memoria. Questa opzione è disponibile solo se il computer dispone di quantità di memoria sufficiente.

22 Se si sceglie di installare Advisor, verrà chiesto di selezionare il tipo di aggiornamento desiderato:

- **Download Internet diretto:** con questa configurazione, gli aggiornamenti Novell vengono scaricati automaticamente dal sito Web di Novell a intervalli regolari (ogni 6 o 12 ore). Utilizzare questa opzione se il computer ha accesso diretto a Internet.
- **Autonoma:** con questa configurazione, per aggiornare Advisor è necessario scaricare manualmente i file dal sito Web di Novell. Utilizzare questa opzione se il computer non ha accesso diretto a Internet.

23 Se si è scelto di installare Advisor ed è stata selezionata l'opzione Download Internet diretto, specificare il nome utente Novell eLogin e la password associati alla licenza di Advisor e indicare con quale frequenza si desidera aggiornare i dati di Advisor (ogni 6 o 12 ore). Fare clic su Avanti.

24 Se si è scelto di installare Advisor, fornire le seguenti informazioni:

- Indirizzo del mittente, che verrà visualizzato nelle notifiche e-mail riguardanti Advisor
- Indirizzo del destinatario, per l'invio di notifiche e-mail riguardanti Advisor

---

Nota: Dopo l'installazione, è possibile modificare l'indirizzo di e-mail di Advisor modificando la sezione AdvisorService del file `advisor_client.xml` nella directory $ESEC_HOME/config. Per ulteriori informazioni, vedere "Advisor Tab" nella *Sentinel User Guide*.

- Selezionare Sì o No a seconda che si desideri ricevere o meno e-mail relative alla riuscita degli aggiornamenti di Advisor.

Nota: Indipendentemente dall'opzione selezionata, gli errori verranno sempre notificati.

Nota: Se si è scelto di installare HP Service Desk, verrà chiesto di immettere ulteriori informazioni.

---

25 Fare clic su Avanti. Verrà visualizzata una finestra contenente un riepilogo delle opzioni selezionate. Fare clic su Installa.

26 Se si è scelto di installare Gestione servizi di raccolta e se quest'ultimo è stato configurato per una comunicazione di tipo proxy, verrà chiesto di immettere il nome utente e la password di un utente Sentinel autorizzato a registrare un client attendibile (ad esempio: esecadm). Per poter completare questa operazione, è necessario che Communication Server sia in esecuzione e che vengano specificati un nome utente e una password validi. La registrazione di un client attendibile richiede l'accettazione del certificato SSL di Communication Server e il caricamento del certificato SSL di Gestione servizi di raccolta su Communication Server. Quando viene avviata la connessione con Communication Server, viene chiesto di accettare il certificato del server. Dopo aver esaminato gli attributi del certificato, selezionare "Accetta in modo permanente". Il programma di installazione caricherà automaticamente il certificato di Gestione servizi di raccolta su Communication Server.

27 Dopo l'installazione, verrà chiesto di riavviare il computer o di rieseguire il login e avviare manualmente Servizi Sentinel Fare clic su Fine per riavviare il sistema. (i servizi pianificati, come ad esempio gli aggiornamenti di Advisor, funzioneranno solo dopo il riavvio).

Nota: Per default, il programma di installazione di Sentinel disattiva la registrazione degli archivi. Per il recupero del database è consigliabile abilitare la registrazione degli archivi dopo l'installazione e prima di iniziare a ricevere i dati degli eventi di produzione. È inoltre opportuno pianificare il backup dei log di archiviazione per liberare spazio sulla destinazione del log di archiviazione ed evitare che il database interrompa l'accettazione degli eventi.

3.6.1 Installazione della console in Linux/Solaris

Se si utilizza la modalità “console”, la pagina di selezione dei componenti del programma di installazione non visualizzerà tutti i componenti insieme. Seguire le istruzioni riportate sullo schermo per visualizzare e modificare i componenti secondari selezionati.

Di seguito è riportato un esempio di utilizzo della pagina di selezione dei componenti in modalità console.

```
Sentinel 6.1 - InstallShield Wizard
Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
   To select/deselect a feature or to view its children, type its
number:
     1.  [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0] 1

Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
   To select/deselect a feature or to view its children, type its
number:
     1.  [x] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0] 2
    1. Deselect 'Sentinel Services'
    2. View 'Sentinel Services' subfeatures
    Enter command [1] 2

Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
    - Sentinel Services

      To select/deselect a feature or to view its children, type its
number:
        1.  [ ] Communication Server
        2.  [ ] Advisor (Requires Advisor ID and Password)
        3.  [x] Correlation Engine
        4.  [x] Data Access Server
```

```
        5.  [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] 1

Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1.  [x] Communication Server
        2.  [ ] Advisor (Requires Advisor ID and Password)
        3.  [x] Correlation Engine
        4.  [x] Data Access Server
        5.  [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] 2

Select the features for "Sentinel 6.1" you would like to install:
   Sentinel 6.1
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1.  [x] Communication Server
        2.  [x] Advisor (Requires Advisor ID and Password)
        3.  [x] Correlation Engine
        4.  [x] Data Access Server
        5.  [x] Sentinel Collector Service
       Other options:
        -1. View this feature's parent
        0. Continue installing
```

3.7 Installazione di Sentinel da parte di un utente di dominio

Per installare Sentinel in veste di utente di dominio:

1. Mappare un utente di dominio a un qualsiasi utente di Sentinel (esecdba, esecadm, esecrpt).
2. Eseguire le operazioni descritte nella Sezione 3.3.1, “Trasmissione dei privilegi di Power User agli "utenti di dominio"”, a pagina 35 per concedere privilegi di power user.
3. Installare Sentinel 6.0 in veste di utente amministratore. Vedere la Sezione 3.6, “Installazione personalizzata”, a pagina 45 per installare Sentinel.
4. Quando il programma di installazione chiede l'immissione delle credenziali dell'utente esecdba, esecadm e esecrpt, specificare l'utente di dominio creato nel formato “dominio\utente dominio”, immettere la password e continuare l'installazione.

3.8 Configurazione postinstallazione

3.8.1 Configurazione dell'integratore SMTP per l'invio di notifiche di Sentinel

In Sentinel 6.1, un'azione `SendEmail` di JavaScript funziona con un integratore SMTP per inviare i messaggi di posta da diversi contesti all'interno dell'interfaccia Sentinel ai destinatari dei messaggi. I destinatari e i contenuti dei messaggi vengono configurati nei parametri dell'azione.

Un'istanza di azione singola del plug-in azione `SendEmail` viene creata automaticamente in tutte le installazioni di Sentinel. Questa azione viene utilizzata internamente da Sentinel per inviare la posta nelle seguenti situazioni:

- All'attivazione di una regola di correlazione distribuita con un'azione di invio della posta "Send Email". L'azione a cui si fa riferimento 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).
- Il flusso di lavoro include un passaggio o attività di posta configurata per l'invio della posta elettronica.
- L'utente apre una richiesta e sceglie di eseguire un'attività configurata per l'invio di posta elettronica.
- L'utente fa clic con il pulsante destro del mouse su un evento e seleziona Email.
- L'utente apre una richiesta e seleziona Email Incident (Invia richiesta tramite posta).
- Durante il download di Advisor viene inviata una notifica.

L'azione `SendEmail` non richiede alcuna configurazione, ma è necessario che l'integratore SMTP sia configurato con dati di connessione validi per poter funzionare.

3.8.2 Database di Sentinel

Tranne nel caso in cui il DBA desideri gestire l'archiviazione del database utilizzando una procedura personalizzata, la gestione delle partizioni automatica del database (archiviazione, rilascio e aggiunta di partizioni) deve essere abilitata durante l'installazione al fine di contenere le dimensioni dei dati di evento. La gestione automatica delle partizioni può inoltre essere configurata dopo l'installazione utilizzando Gestione dati Sentinel.

Per default, Sentinel Data Manager non è in grado di scrivere nel file system per l'archiviazione dei dati. È possibile abilitare la scrittura nel file system modificando il file <OracleSID>.ora per il database.

Nota: Per default, il programma di installazione imposta tutti gli spazi tabelle sulla modalità di aumento automatico. Per default, le dimensioni di crescita del file sono impostate su 200, ma le dimensioni massime del file dipendono dal valore specificato durante l'installazione.

Per abilitare la scrittura nella directory di archiviazione di Oracle:

1. Accedere al computer del database.

2 Passare alla directory $ORACLE_HOME/dbs.

3 Aprire il file init<OracleSID>.ora in un editor di testo.

4 Modificare il parametro UTL_FILE_DIR per specificare il percorso della directory nella quale archiviare i dati di Sentinel. È necessario utilizzare una delle seguenti opzioni:

- UTL_FILE_DIR = *

  oppure

- UTL_FILE_DIR = [percorso di directory specifico]

5 Salvare il file e uscire.

3.8.3 Servizio di raccolta

Durante l'installazione del Servizio di raccolta, verrà configurato un servizio di raccolta denominato servizio di raccolta generale. Per default, vengono creati 5 eventi al secondo. Tale servizio di raccolta può essere utilizzato per verificare l'installazione. È possibile scaricare altri servizi di raccolta dal sito Web di Novell (http://support.novell.com/products/sentinel/collectors.html).

3.8.4 Aggiornamento del codice di licenza (passaggio 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 il codice di licenza sul sistema in modo da evitare la reinstallazione.

Per aggiornare il codice di licenza (UNIX):

1 Accedere al computer dove è installato il componente DAS come utente amministratore di Sentinel del sistema operativo (per default, esecadm).

2 Dal prompt dei comandi, modificare la directory in $ESEC_HOME/bin

3 Immettere il comando seguente:

```
./softwarekey.sh
```

4 Immettere il numero 1 per impostare il codice primario. Premere Invio.

Per aggiornare il codice di licenza (Windows):

1 Accedere al computer dove è installato il componente DAS come utente con diritti di amministratore.

2 Dal prompt dei comandi, modificare la directory in %ESEC_HOME%\bin

3 Immettere il comando seguente:

```
.\softwarekey.bat
```

4 Immettere il numero 1 per impostare il codice primario. Premere Invio.

3.8.5 Avvio del servizio Gestione servizi di raccolta

Per avviare il servizio Gestione servizi di raccolta:

1 Avviare Sentinel 6.1

2 Fare clic sulla scheda Amministratore > Visualizzazione server. È anche possibile fare clic su Visualizzazione server nel riquadro di spostamento.

3 Espandere la visualizzazione Server. Viene visualizzato l'elenco dei processi.

Fare clic col pulsante destro del mouse sull'istanza di Gestione servizi di raccolta che si desidera avviare, quindi selezionare Azioni > Avvia.

Oppure

1 Avviare Sentinel 6.1

2 Fare clic su Gestione origini eventi > Visualizzazione in diretta.

3 Nella finestra di Gestione origini eventi (visualizzazione in diretta), fare clic col pulsante destro del mouse sull'istanza di Gestione servizi di raccolta che si desidera avviare, quindi selezionare Avvia.

3.8.6 Gestione temporale

Novell consiglia vivamente che tutti i componenti di Sentinel, e in particolare il computer del motore di correlazione e quello di Gestione servizi di raccolta, siano connessi a un server NTP (Network Time Protocol) o a un altro tipo di server di riferimento ora. 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.

Per default, la soglia per i dati “in tempo reale” è 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 di 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 di Gestione servizi di raccolta corrisponde all'ora del sistema corrente del sistema Gestione servizi di raccolta.

3.8.7 Modifica degli script Oracle dbstart e dbshut

Sentinel non può avviare il database Oracle 10 a causa di errori negli script Oracle `dbstart` e `dbshut`. Per informazioni sugli errori degli script, visitare https://metalink.oracle.com (https://metalink.oracle.com) e consultare i codici di errore 336299.1 (“dbstart errors out when executing in 10.2.0.1.0”, 5183726 e 4665320.

Dopo l'installazione di Sentinel 6, è necessario modificare gli script `dbstart` e `dbshut` affinché Sentinel possa avviare un database Oracle 10.

Per modificare lo script dbstart in Solaris 10:

1 Aprire lo script `dbstart` per modificarlo dal percorso $ORACLE_HOME/bin/dbstart.

2 Passare alla riga 78 e sostituire il percorso con ORACLE_HOME_LISTNER=$ORACLE_HOME.

3 Aggiungere `#!/bin/bash` all'inizio per richiedere la shell Bash.

4 Verificare che "ORATAB" rimandi a ORATAB=/var/opt/oracle/oratab.

Nota: se ORATAB non si trova sul proprio computer nell'ubicazione specificata sopra, sostituire manualmente il percorso ORATAB con quello corretto.

5 Fare clic su Salva e uscire.

6 Per modificare lo script dbshut in Solaris 10:

7 Aprire lo script dbshut per modificarlo dal percorso $ORACLE_HOME/bin/dbshut.

8 Verificare che "ORATAB" rimandi a ORATAB=/var/opt/oracle/oratab.

Nota: se ORATAB non si trova sul proprio computer nell'ubicazione specificata sopra, sostituire manualmente il percorso ORATAB con quello corretto.

9 Fare clic su Salva e uscire.

Per modificare lo script dbstart in RedHat Linux ES4:

1 Aprire lo script `dbstart` per modificarlo dal percorso $ORACLE_HOME/bin/dbstart.

2 Verificare che "ORATAB" rimandi a ORATAB=/etc/oratab.

Nota: se ORATAB non si trova sul proprio computer nell'ubicazione specificata sopra, sostituire manualmente il percorso ORATAB con quello corretto.

3 Fare clic su Salva e uscire.

4 Per modificare lo script dbshut in RedHat Linux ES4:

5 Aprire lo script `dbshut` per modificarlo dal percorso $ORACLE_HOME/bin/dbshut.

6 Verificare che "ORATAB" rimandi a ORATAB=/etc/oratab.

Nota: se ORATAB non si trova sul proprio computer nell'ubicazione specificata sopra, sostituire manualmente il percorso ORATAB con quello corretto.

7 Fare clic su Salva e uscire.

Configurazione di Advisor

4

In questo capitolo vengono descritte le procedure di caricamento dei dati di Advisor, di configurazione degli aggiornamenti periodici di tali dati e di configurazione di Sentinel per eseguire i rapporti di Advisor forniti da Novell a partire dalla scheda Advisor di Sentinel Control Center.

4.1 Panoramica di Advisor

Advisor è un servizio facoltativo basato su sottoscrizione che fornisce una correlazione a livello di dispositivi tra gli eventi in tempo reale di sistemi di prevenzione e rilevamento delle intrusioni e i risultati di scansioni delle vulnerabilità aziendali. Grazie alle informazioni normalizzate sugli attacchi fornite da Advisor, questo servizio è in grado di fornire segnalazioni tempestive per consentire il rilevamento di attacchi lanciati contro sistemi vulnerabili (“rilevamento di exploit”). Fornisce inoltre informazioni per la risoluzione delle vulnerabilità.

Nota: L'installazione di Advisor è facoltativa. Questo servizio è tuttavia un componente necessario qualora si desideri utilizzare le funzionalità di rilevamento degli exploit di Sentinel e di generazione dei rapporti di Advisor. Advisor è un servizio dati basato su sottoscrizione e richiede una licenza Novell aggiuntiva.

Di seguito sono riportati i sistemi supportati e il tipo di dispositivo associato (IDS: sistema di rilevamento delle intrusioni; VULN: scanner di vulnerabilità; FW: firewall).

Tabella 4-1 *Sistemi supportati e tipo di dispositivo associato*

Sistemi supportati	Tipo di dispositivo	Valore RV31
Cisco Secure IDS	IDS	Sicura
Enterasys Dragon Host Sensor	IDS	Dragon
Enterasys Dragon Network Sensor	IDS	Dragon Network
Intrusion.com (SecureNet_Provider)	IDS	SecureNet_Provider
ISS BlackICE PC Protection	IDS	BlackICE
ISS RealSecure Desktop	IDS	RealSecure Desktop
ISS RealSecure Network	IDS	RealSecure
ISS RealSecure Server	IDS	RealSecure Server

Sistemi supportati	Tipo di dispositivo	Valore RV31
ISS RealSecure Guard	IDS	RealSecure Guard
Sourcefire Snort/Phalanx	IDS	Snort
Symantec Network Security 4.0 (ManHunt)	IDS	ManHunt
Symantec Intruder Alert	IDS	Intruder
McAfee IntruShield	IDS	IntruShield
eEYE Retina	VULN	Retina
Foundstone Foundscan	VULN	Foundstone
ISS Database Scanner	VULN	Database Scanner
ISS Internet Scanner	VULN	Internet Scanner
ISS System Scanner	VULN	System Scanner
ISS Wireless Scanner	VULN	Wireless Scanner
Nessus	VULN	Nessus
nCircle IP360	VULN	nCircle IP360
Qualys QualysGuard	VULN	QualysGuard
Cisco IOS Firewall	FW	Cisco IOS

Per consentire l'abilitazione completa del rilevamento degli exploit, i servizi di raccolta di Sentinel devono assegnare valori corretti a un certo numero di variabili. Questi servizi, forniti da Novell, assegnano valori a queste variabili per default.

- Nel servizio di raccolta IDS, è necessario che RV39 (MSSPCustomerName) sia impostato sul nome cliente MSSP.
- Nei sistemi IDS e nei servizi di raccolta delle vulnerabilità, la variabile RV31 (valore riservato) deve essere impostata sul valore riportato nella colonna RV31 della tabella sopra riportata. In questa stringa viene applicata la distinzione tra maiuscole e minuscole.
- Nel servizio di raccolta IDS, il DIP (IP di destinazione) deve essere impostato sull'indirizzo IP del computer che subisce l'attacco.
- Nel servizio IDS, RT1 (DeviceAttackName) deve essere impostato sul nome dell'attacco o sul codice dell'attacco per l'IDS in questione.

I servizi di raccolta forniti da Novell impostano queste variabili per default.

4.2 Informazioni sull'installazione di Advisor

I due componenti principali di un'installazione di Advisor provvedono a configurare gli aggiornamenti periodici ottenuti attraverso il servizio dati basato su sottoscrizione e a caricare il set di dati iniziale di Advisor.

Per caricare i dati iniziali, Novell consiglia vivamente di utilizzare l'immagine ISO dei dati di base di Advisor, disponibile attraverso il portale del servizio clienti di Novell ai clienti che hanno acquistato la sottoscrizione ai dati di Advisor. Questo programma di installazione consente di caricare circa 10 GB di dati che altrimenti andrebbero trasferiti sulla rete utilizzando il normale servizio di aggiornamento.

Per default, gli script che inizializzano i download automatici sono disabilitati. Questi script devono essere abilitati dopo il caricamento dei dati principali di Advisor.

Advisor deve essere installato sullo stesso computer dove è installato DAS (Database Access Service). Gli aggiornamenti periodici possono avvenire manualmente o automaticamente a seconda dell'opzione selezionata durante l'esecuzione del programma di installazione di Sentinel.

- **Autonoma:** aggiornamenti manuali
- **Download Internet diretto:** aggiornamenti automatici pianificati

---

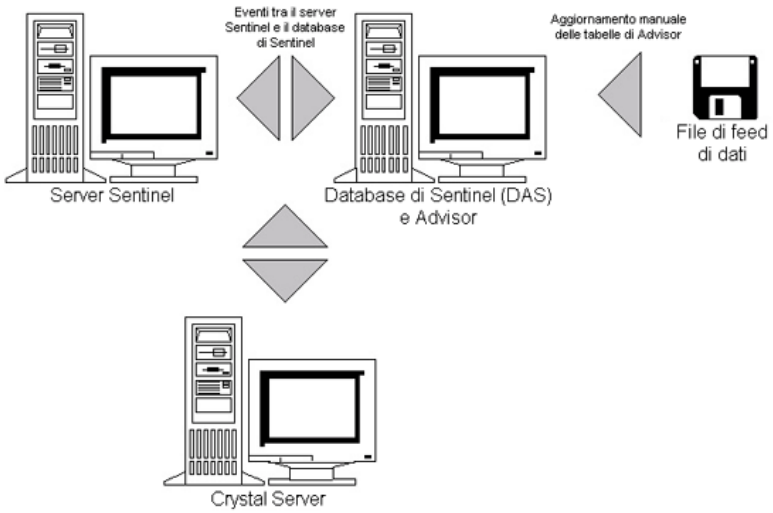
Nota: Il feed di dati di Advisor per Sentinel 6.0 SP2 o versioni successive è stato arricchito con firme aggiuntive. I cambiamenti apportati in SP2 riguardano sia lo spazio di memorizzazione richiesto, sia le procedure di installazione.

Novell consiglia uno spazio di circa 50 GB per i dati di Advisor, oltre allo spazio su disco richiesto per i dati di Sentinel.

4.2.1 Configurazione autonoma

In un'installazione autonoma, Advisor è configurato come sistema isolato che richiede aggiornamenti manuali dei dati di Advisor. In ambienti sicuri, le installazioni di Advisor spesso non dispongono di connessioni a Internet e richiedono quindi una configurazione autonoma.

Figura 4-1 *Configurazione autonoma*



Nella configurazione autonoma, i dati di Advisor possono essere scaricati manualmente da una delle seguenti ubicazioni:

- Sentinel 6.0 SP1 e versioni precedenti:

  https://advisor.novell.com/advisordata/ (https://advisor.novell.com/advisordata/)

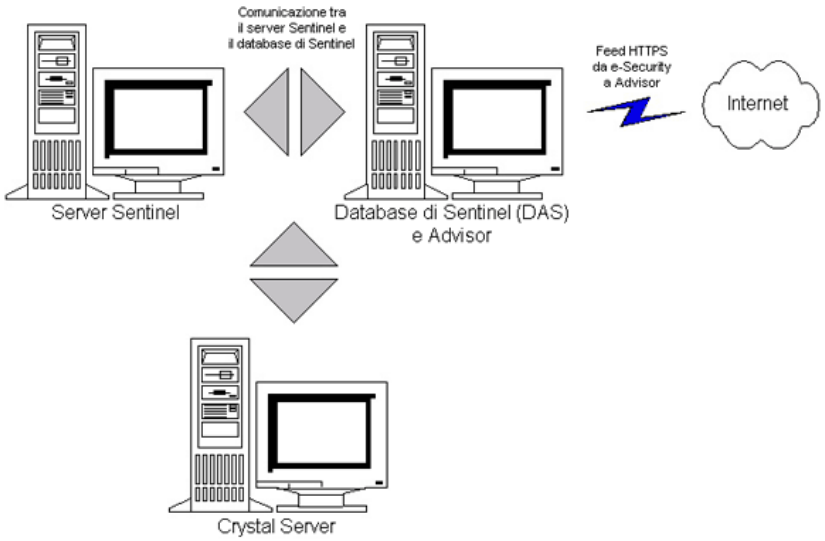
- Sentinel 6.0 SP2 e versioni successive:

  https://secure-www.novell.com/sentinel/advisor/advisordata (https://secure-www.novell.com/sentinel/advisor/advisordata)

4.2.2 Configurazione dell'installazione con download Internet diretto

In un'installazione con download Internet diretto, il computer che esegue Advisor è connesso direttamente a Internet. In questo tipo di configurazione, gli aggiornamenti dei dati di Advisor vengono scaricati automaticamente da Novell attraverso Internet a intervalli regolari (ogni 6 o 12 ore). Per ulteriori informazioni, vedere ilCapitolo 3, “Installazione di Sentinel 6.1”, a pagina 31.

Figura 4-2 *Download Internet diretto*



4.3 Installazione di Advisor

Advisor può essere installato insieme a Sentinel oppure come componente aggiuntivo.

Nota: La configurazione di Advisor per la versione 6.0 SPI di Sentinel varia notevolmente da quella per la versione 6.0 SP2. Se si utilizza la versione 6.0 SP1 o una versione precedente, consultare la documentazione della versione corrispondente disponibile sul sito http://www.novell.com/documentation/sentinel6. (http://www.novell.com/documentation/sentinel6.)

Per installare Advisor:

1. Eseguire il login come utente root in Solaris/Linux o utente Administrator in Windows.
2. Inserire e montare il CD di installazione di Sentinel.

3 Avviare il programma di installazione passando alla directory di installazione sul CD-ROM e

- In Windows, eseguire `setup.bat`
- In Solaris/Linux:

  Per la modalità GUI:

  `./setup.sh`

  Oppure per la modalità basata su testo (“console seriale”):

  `./setup.sh -console`

4 Selezionare la lingua e fare clic su OK.

5 Dopo aver letto la schermata introduttiva, fare clic su Avanti.

6 Leggere e accettare il Contratto di licenza dell'utente finale, quindi fare clic su Avanti.

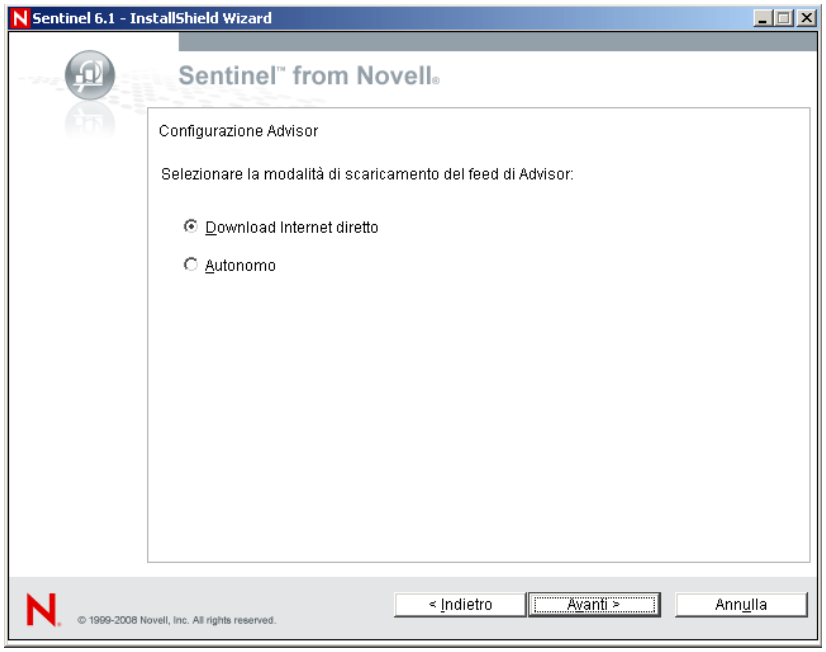
7 Accettare la directory di installazione di default o fare clic su Sfoglia per specificare il percorso di installazione. Fare clic su Avanti.

8 Selezionare Personalizzata. Fare clic su Avanti.

9 In questa finestra, fornire le informazioni di configurazione e fare clic su Avanti.

- Numero di serie
- Codice di licenza
- Password di sistema globale
- La password inserita qui è valida per tutti gli utenti di default. Sono inclusi sia l'utente amministratore di Sentinel che gli utenti del database. Per ulteriori informazioni sull'elenco degli utenti di default del database creati durante l'installazione, vedere la Sezione 3.8.2, “Database di Sentinel”, a pagina 58.

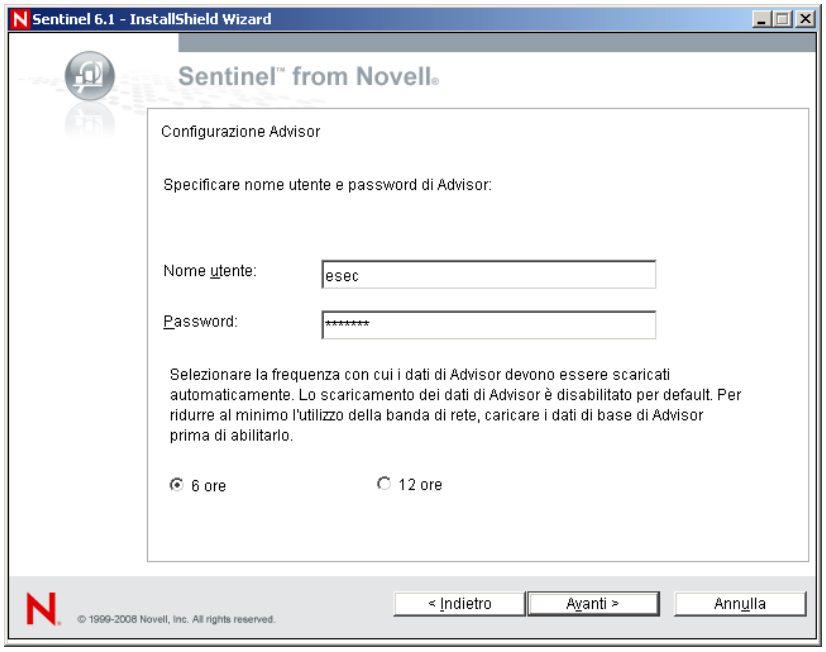
10 Selezionare una delle due opzioni disponibili: Download Internet diretto o Autonoma.



11 Se è stata selezionata la modalità di scaricamento Download Internet diretto, immettere le informazioni seguenti:

- Nome utente di Advisor
- Password di Advisor
- Frequenza di aggiornamento dei dati di Advisor

Nota: Per Sentinel 6.0 SP2 e versioni successive, il nome utente e la password di Advisor corrispondono alle credenziali eLogin Novell ottenute con l'acquisto di Advisor. I dati di login potrebbero corrispondere alle credenziali eLogin Novell ottenute con l'acquisto di Sentinel. Per ulteriori informazioni, vedere la sezione "Advisor Tab" nella *Sentinel User Guide*.



12 Fare clic su Avanti.

Importante: Se il nome utente e la password non possono essere verificati, viene chiesto se si desidera continuare.

In Sentinel 6.0 SP2 e versioni successive, il login e la password devono corrispondere alle credenziali di login Novell ottenute con·l'autorizzazione all'utilizzo di Advisor. Una causa di errore comune è l'utilizzo del login e della password Novell errati; si potrebbe infatti trattare di credenziali di login Novell valide, ma che non sono state ottenute mediante titolarità o licenza Advisor.

---

13 Fare clic su Installa.

14 Dopo l'installazione, verrà chiesto di riavviare il computer o di rieseguire il login e avviare manualmente Servizi Sentinel. Fare clic su Fine per riavviare il sistema.

Importante: il download pianificato dei dati di Advisor funziona solo dopo il riavvio del sistema.

Suggerimento: Dopo l'installazione, è possibile modificare l'indirizzo di e-mail di Advisor modificando il file `advisor_client.xml` nella directory in the $ESEC_HOME/config. Per ulteriori informazioni, vedere “Advisor Tab” nella *Sentinel User Guide*.

4.3.1 Caricamento dei dati

Sebbene il caricamento iniziale dei dati di Advisor possa essere eseguito attraverso il servizio pianificato (Download Internet diretto) o manualmente utilizzando la configurazione autonoma, questo metodo non è consigliabile in quanto sovraccaricherebbe la rete. Pertanto, gli script `advisor.sh` e `advisor.bat` sono inizialmente disabilitati per default. Questi script devono essere abilitati dopo il caricamento dei dati utilizzando il disco Sentinel 6 Exploit Detection e·Advisor Core Data che contiene un'istantanea dei dati di Advisor. Il caricamento di questi dati diminuisce significativamente la quantità di tempo e la larghezza di banda di rete necessari per aggiornare il database.

Advisor Core Data è disponibile attraverso il portale del servizio clienti di Novell ai clienti che hanno acquistato la sottoscrizione annuale ad Advisor. L'immagine ISO è inferiore a 900 MB ma comporta il caricamento di circa 10 GB di dati nelle tabelle di Advisor.

Il caricamento dei dati iniziali può richiedere un giorno intero, a seconda delle caratteristiche dei computer e del carico sui server dei database.

Dopo il caricamento iniziale dei dati, gli aggiornamenti incrementali possono essere caricati manualmente o utilizzando la funzionalità Download Internet diretto.

Importante: Il programma di installazione dei dati per Advisor funziona solo con Sentinel 6.0 SP2 o versioni successive dopo l'installazione e l'applicazione di opportune patch per il database. Il processo di aggiornamento e il programma di installazione dei dati sostituiscono tutti i dati di Advisor che sono stati scaricati prima di Sentinel 6.0 SP2.

Per scaricare l'istantanea dei dati di Advisor:

1. Eseguire il login come utente root in Solaris/Linux o utente Administrator in Windows.
2. Inserire e montare il disco di installazione dei dati di base di Advisor per Sentinel 6.
3. Avviare il programma di installazione contenuto nella directory di installazione disponibile sul CD-ROM e
   - in Solaris/Linux, eseguire `advisor_bcp_in.sh`
   - in Windows, eseguire `advisor_bcp_in.bat`
4. Nella console, immettere le credenziali per il database:
   - In Linux, immettere il nome utente per il database (per default, esecdba), la password, nonché il SID Oracle (nome dell'istanza).
   - In Windows, immettere il nome host per il database, il nome del database (per default, ESEC) e selezionare la modalità di autenticazione per il database. Se viene utilizzata l'autenticazione SQL, è necessario immettere anche il nome utente per il database (per default, esecdba) e la password.
5. Specificare la durata della pausa in secondi tra l'elaborazione di un file e l'altro. Il valore di default è 0 secondi, ma può essere aumentato se il carico sul database è elevato, in modo da introdurre una pausa tra l'elaborazione di un file di dati e l'altro.

6 Per aumentare l'efficienza del processo di caricamento dei dati, il sistema disabilita gli indici e i vincoli nelle tabelle di Advisor e tronca queste tabelle. Viene visualizzato il seguente messaggio:

```
Disabling indexes on the Advisor tables…
Successfully disabled indexes on the Advisor tables
Disabling constraints on the Advisor tables...
Successfully disabled constraints on the Advisor tables
Truncating Advisor tables...
Successfully truncated Advisor tables
```

7 Viene avviato lo script di Advisor e i dati di massa vengono immessi nella tabella corrispondente. L'istantanea dei dati è memorizzata nel database.

8 Dopo il caricamento di tutti i file inclusi nell'istantanea, vengono abilitati i vincoli, ricreati gli indici e vengono visualizzati i seguenti messaggi:

```
Successfully enabled constraints on the Advisor tables
Successfully rebuilt indexes on the Advisor tables
```

9 Al termine del feed di massa, il sistema visualizza un messaggio dove si conferma il completamento del processo.

10 Abilitare gli aggiornamenti incrementali dei dati di Advisor.

È consigliabile pianificare aggiornamenti incrementali e periodici dei dati di Advisor (attraverso il download diretto da Internet o manualmente tramite la modalità autonoma) per aggiornare e mantenere aggiornato il database di Advisor.

4.3.2 Abilitazione degli aggiornamenti di Advisor

Per evitare il caricamento eccessivo della rete, i download incrementali di Advisor sono disabilitati per default. Questi download devono essere abilitati una volta completato il caricamento dei dati principali di Advisor.

Per abilitare i download di Advisor:

1 Aprire il file `advisor.sh` o `advisor.bat` per apportare le opportune modifiche.

Su Linux: $ESEC_HOME/bin/advisor.sh

In Windows: %ESEC_HOME%\bin\advisor.bat

2 **Per Linux:**

Aggiungere un segno di cancelletto (#) davanti al comando exit all'inizio del file per disabilitarlo.

```
# exit
```

In Windows:

Digitare rem davanti al comando exit all'inizio del file per disabilitarlo.

```
rem exit
```

3 Salvare il file.

Al successivo download manuale o pianificato verranno scaricati i dati come previsto.

4.3.3 Connessione al server di Advisor attraverso un proxy

Per connettersi al server di Advisor attraverso un server proxy per lo scaricamento dei feed, è necessario aggiornare la configurazione di Advisor. A tale scopo potrebbe essere necessario aggiungere fino a quattro nuove proprietà a ciascun file `container.xml` utilizzato da Advisor. Se il server proxy non richiede l'autenticazione, è necessario aggiungere solo le informazioni sulla porta e l'host del server proxy. Se il server proxy richiede l'autenticazione, è necessario aggiungere anche il nome utente e la password per il server proxy.

Per configurare Advisor:

1. Installare Advisor in modalità “connessione diretta”. Poiché l'attuale programma di installazione non supporta la connessione attraverso un server proxy, il controllo di autenticazione eseguito dal programma di installazione non riuscirà. È tuttavia necessario continuare con l'installazione.
2. Passare alla cartella `%ESEC_HOME%\sentinel\config`.
3. Aprire il file `advisor_client.xml` e aggiungere le seguenti righe alla sezione DownloadComponent.

   ```
   <property name="proxy_host">proxyHost</property>
   <property name="proxy_port">proxyPort</property>
   ```

   Aggiungere inoltre le seguenti proprietà, qualora il server proxy richieda l'autenticazione.

   ```
   <property name="proxy_username">proxyUser</property>
   <property name="proxy_password" />
   ```

4. Se il server proxy richiede l'autenticazione, attenersi alla procedura riportata di seguito:
   - Copiare il file `proxy_password_update.bat` nella cartella %ESEC_HOME%\sentinel\bin.
   - Per aggiornare i file container di Advisor con la password dell'utente proxy, eseguire il seguente comando:
     `%ESEC_HOME%\sentinel\bin\proxy_password_update.bat proxyPasswd`
   - Verificare che il file `advisor_client.xml` contenga ora la password proxy cifrata.
5. Eseguire `advisor.bat` per scaricare ed elaborare i dati di Advisor. È possibile verificare che Advisor sia in grado di connettersi attraverso il server proxy controllando il contenuto dei seguenti file di log : `%ESEC_HOME%\sentinel\log\Advisor_0.0.log` e `%ESEC_HOME%\sentinel\log\advisor.log`.

4.4 Rapporti di Advisor

Crystal Reports Server™ è lo strumento di generazione dei rapporti integrato con Sentinel.

Per eseguire rapporti di Crystal Reports Server in Advisor:

- Installare e configurare il server Crystal. Per ulteriori informazioni sull'installazione di Crystal Reports Server, vedere il Capitolo 8, “Crystal Reports per Windows”, a pagina 97 e il Capitolo 9, “Crystal Reports per Linux”, a pagina 125.
- Pubblicare Crystal Reports di Advisor sul server Crystal.

4.4.1 Configurazione dei rapporti di Advisor

Per eseguire i rapporti di Advisor, è necessario seguire la procedura di configurazione di Crystal Reports Server per Windows o per Linux e configurare l'URL di Advisor per i rapporti. Per ulteriori informazioni sull'importazione dei modelli dei rapporti e sulla configurazione di Sentinel Control Center per la visualizzazione dei rapporti di Advisor, vedere Capitolo 8, “Crystal Reports per Windows”, a pagina 97 e Capitolo 9, “Crystal Reports per Linux”, a pagina 125.

4.5 Manutenzione di Advisor

Di seguito sono elencati vari task per la manutenzione di Advisor descritti nella Sentinel User Guide:

- Aggiornamento manuale dei dati di Advisor: per assicurare la massima efficacia, i dati di Advisor devono essere aggiornati regolarmente in quanto vengono aggiunti continuamente dati su nuovi attacchi e vulnerabilità al feed di dati. Se gli aggiornamenti non vengono pianificati utilizzando la modalità Download Internet diretto, devono essere eseguiti manualmente.
- Sostituzione della password utilizzata da Advisor per l'aggiornamento automatico dei dati, se necessaria
- Modifica della configurazione per i messaggi e-mail di notifica di Advisor
- Modifica dell'ora di aggiornamento pianificato dei dati

Per ulteriori informazioni su tutti questi task di manutenzione, vedere “Maintaining Advisor” nella *Sentinel User Guide*.

Test dell'installazione

5

5.1 Test dell'installazione

Sentinel è installato con un servizio di raccolta di esempio che viene utilizzato per testare numerose funzionalità di base del sistema. Attraverso l'utilizzo di questo servizio di raccolta, è possibile testare Active Views, la creazione di casi, le regole di correlazione e i rapporti. La procedura riportata di seguito descrive come testare il sistema e i risultati previsti. Anche se gli eventi visualizzati non sono esattamente gli stessi, i risultati dovrebbero essere simili a quelli riportati di seguito.

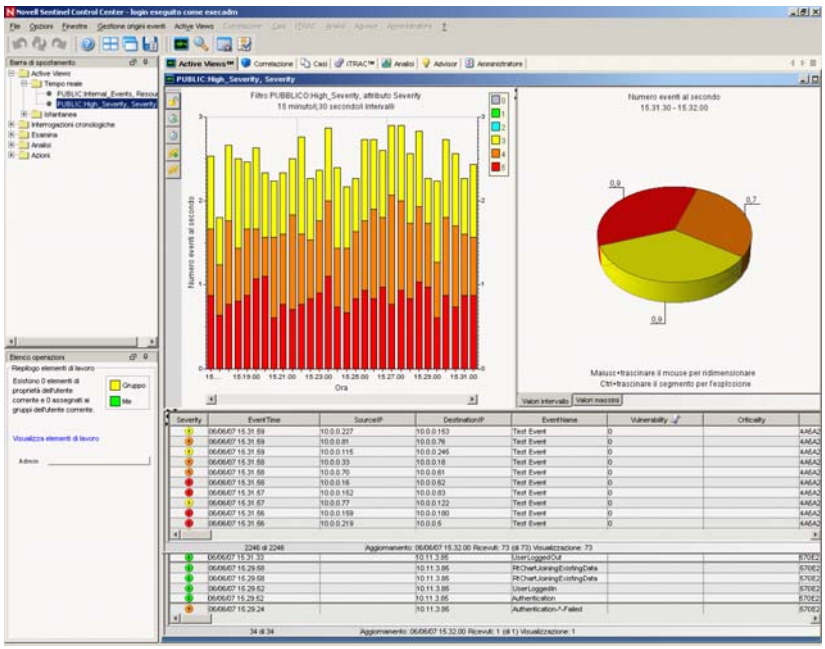
A un livello di base, questi test consentono di verificare se:

- I servizi Sentinel sono attivi e in esecuzione
- La comunicazione tramite il bus messaggi funziona
- È in corso l'invio di eventi di revisione interni
- È possibile inviare eventi da Gestione servizi di raccolta
- È in corso l'inserimento nel database di eventi che è possibile recuperare tramite Interrogazione eventi cronologici o Crystal Reports.
- È possibile creare e visualizzare casi
- Il motore di correlazione sta valutando le regole e attivando gli eventi correlati
- Gestione dati Sentinel può connettersi al database e 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. Fare doppio clic su Sentinel Control Center sul desktop.
2. Accedere al sistema utilizzando l'utente amministrativo di Sentinel specificato durante l'installazione (per default, esecadm). Verrà aperto Sentinel Control Center dove è visualizzata la scheda Active Views in cui gli eventi sono stati filtrati tramite i filtri pubblici “Eventi_Interni” e “Gravità_Alta”.



3 Scegliere Visualizzazione in diretta dal menu Gestione origini eventi.

4 Nella visualizzazione grafica, fare clic col pulsante destro del mouse sull'origine evento 5 eps e scegliere Avvia.

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

6 Passare alla scheda Active Views. Sarà presente una finestra attiva denominata PUBBLICO: Gravità_Alta, Gravità. L'avvio del servizio di raccolta e la visualizzazione dei dati in questa finestra potrebbero richiedere alcuni minuti.

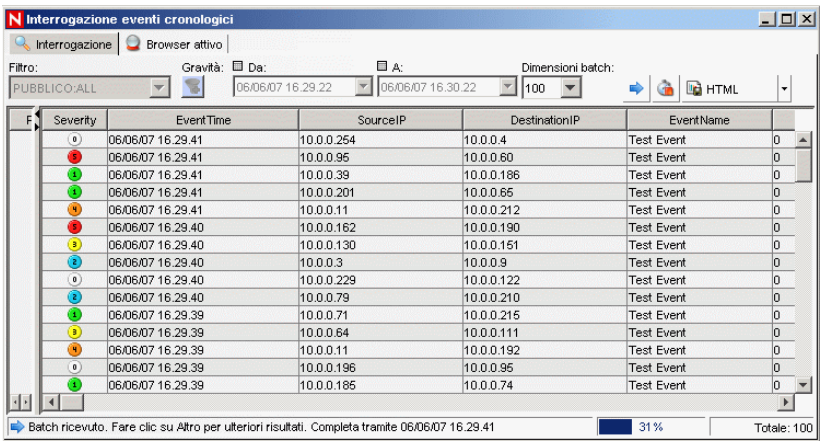
7 Fare clic sul pulsante Interrogazione eventi sulla barra degli strumenti. Verrà visualizzata la finestra Interrogazione eventi cronologici.

8 Nella finestra Interrogazione eventi cronologici, fare clic sulla freccia verso il basso Filtro per selezionare il filtro. Evidenziare il filtro Pubblico: Tutti e fare clic su Seleziona.

9 Scegliere un periodo di tempo in cui il servizio di raccolta è stato attivo. Selezionare l'intervallo di date attraverso le frecce verso il basso Da e A.

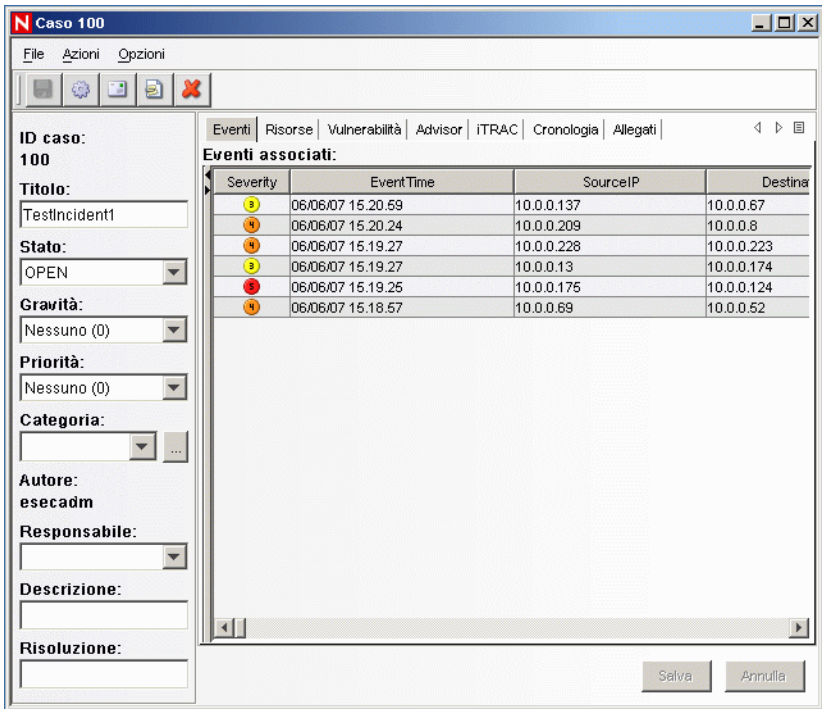
10 Selezionare una dimensione batch dall'elenco a discesa Dimensioni batch.

11 Fare clic sull'icona della lente di ingrandimento per eseguire l'interrogazione.



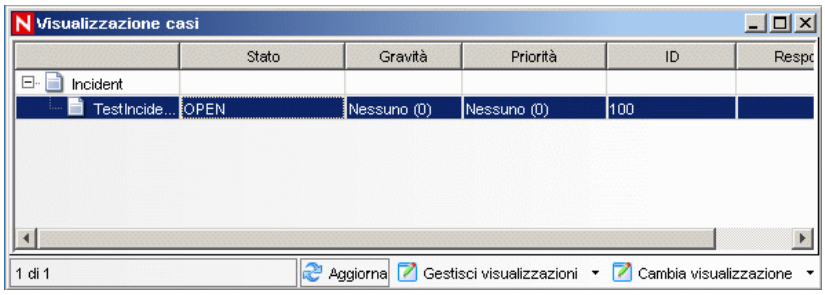
12 Tenere premuto CTRL o MAIUSC e selezionare più eventi dalla finestra Interrogazione eventi cronologici.

13 Fare clic con il pulsante destro del mouse e scegliere Crea caso.

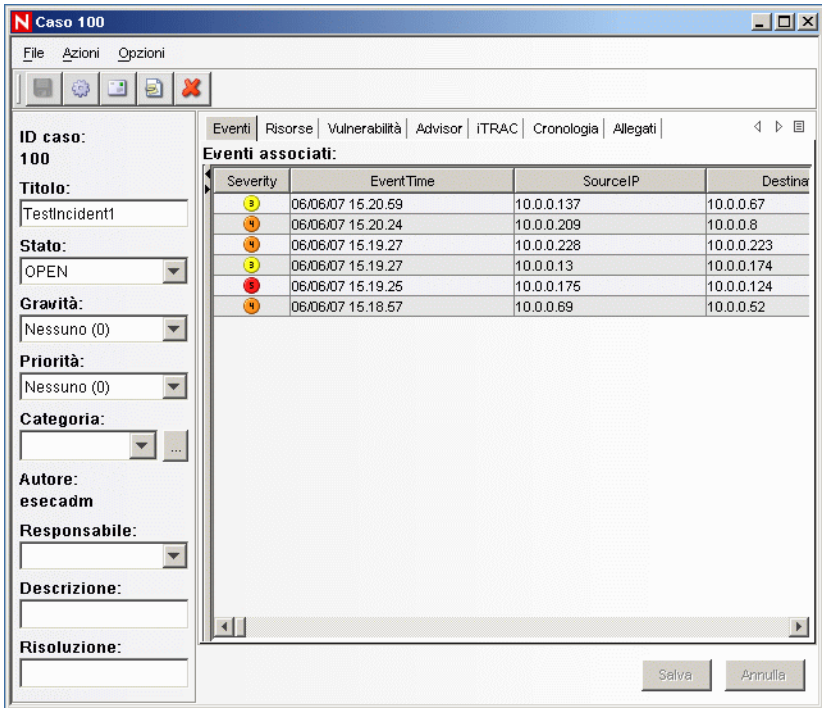


14 Assegnare il nome CasoTest1 al caso e fare clic su Crea. Viene visualizzata una notifica per confermare la creazione del caso. Fare clic su OK.

15 Passare alla scheda Caso. Viene visualizzata la finestra Gestione visualizzazione caso dove è visibile il caso appena creato.



16 Fare doppio clic sul caso per visualizzarlo.



17 Chiudere la finestra Caso, scegliendo Esci dal menu File o facendo clic su “X” nell'angolo in alto a destra della finestra.

18 Fare clic sulla scheda Analisi. Nella barra di spostamento della scheda Analisi aprire la cartella Eventi.

19 Fare clic su Interrogazioni eventi cronologia.

20 Fare clic su Analisi > Crea rapporto oppure fare clic sull'icona Crea rapporto. Viene visualizzata la finestra Interrogazione eventi. Impostare quanto segue:

- intervallo di tempo
- filtro
- livello di gravità
- dimensioni batch, ovvero il numero di eventi da visualizzare (gli eventi saranno visualizzati in ordine cronologico, da quello meno recente a quello più recente)

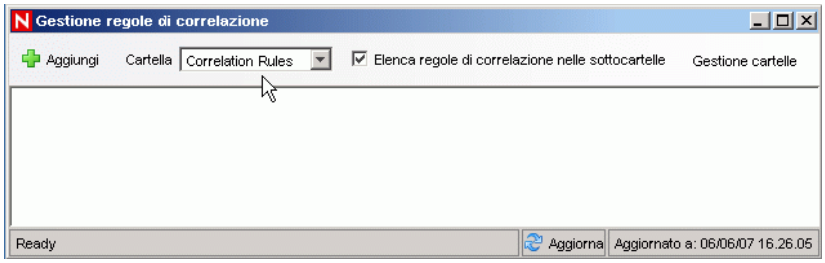
21 Fare clic sull'icona Inizia ricerca.

22 Per visualizzare il gruppo di eventi successivo, fare clic sul pulsante Altro.

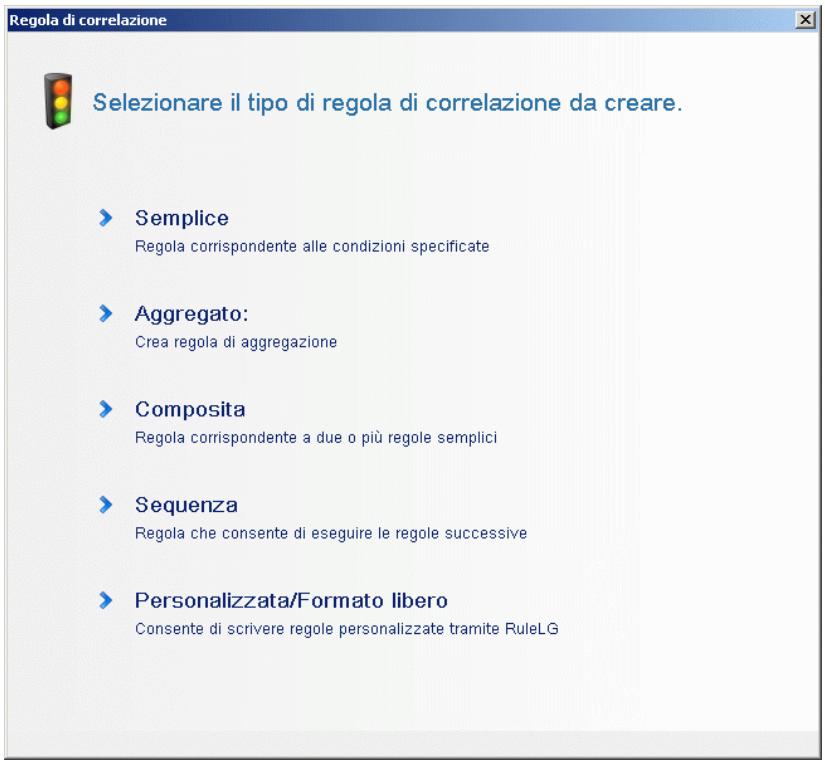
23 Riorganizzare le colonne tramite la funzione di trascinamento e rilascio, quindi ordinarle facendo clic sull'intestazione della colonna.

24 Al termine, l'interrogazione sarà aggiunta all'elenco delle interrogazioni rapide nella barra di spostamento.

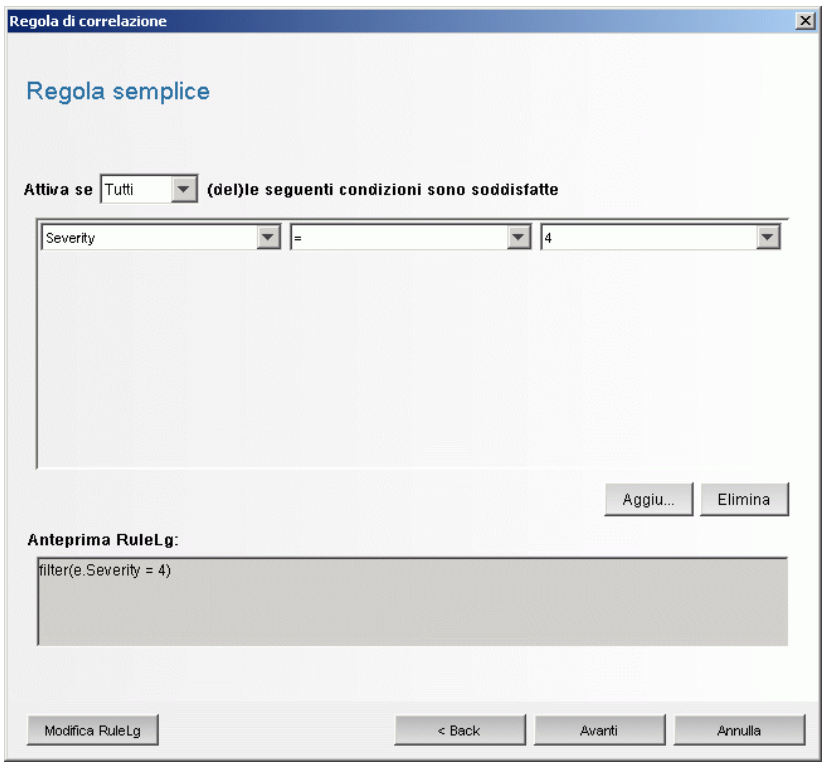
25 Passare alla scheda Correlazione. Viene visualizzata la finestra Gestione regole di correlazione.



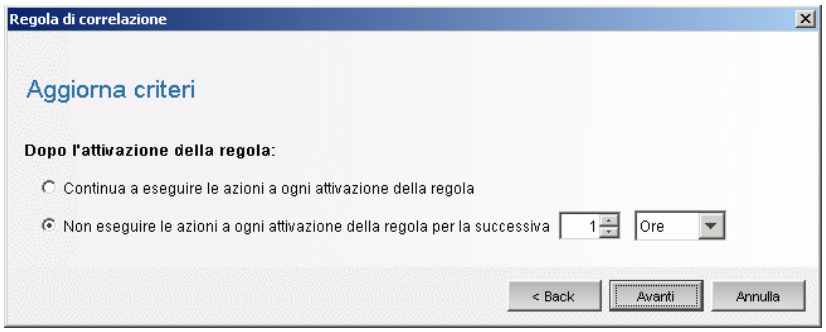
26 Fare clic su Aggiungi. Viene aperta la Creazione guidata regole di correlazione.



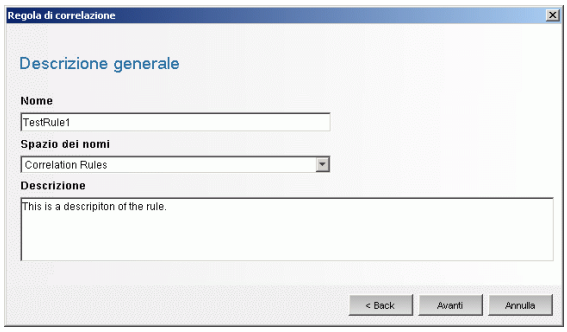
27 Fare clic su Semplice. Viene visualizzata la finestra Regola semplice.



28 Utilizzare i menu a discesa per impostare i criteri su Gravità=4. Fare clic su Avanti. Viene visualizzata la finestra Aggiorna criteri.



29 Selezionare “Non eseguire le azioni a ogni attivazione della regola per la successiva” e utilizzare il menu a discesa per impostare il periodo di tempo su 1 minuto. Fare clic su Avanti. Viene visualizzata la finestra Descrizione generale.

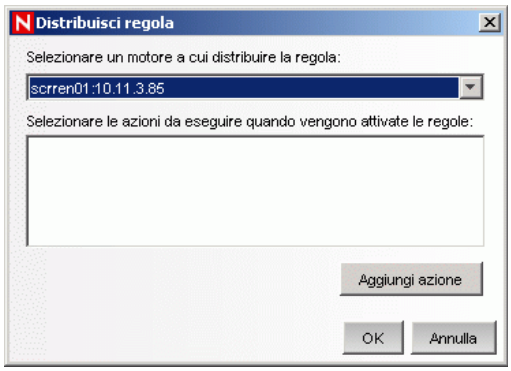


30 Assegnare il nome "Regola di correlazione" alla regola, immettere una descrizione, quindi fare clic su Avanti.

31 Selezionare “No, non creare un'altra regola” e fare clic su Avanti.

32 Aprire la finestra Gestione regole di correlazione.

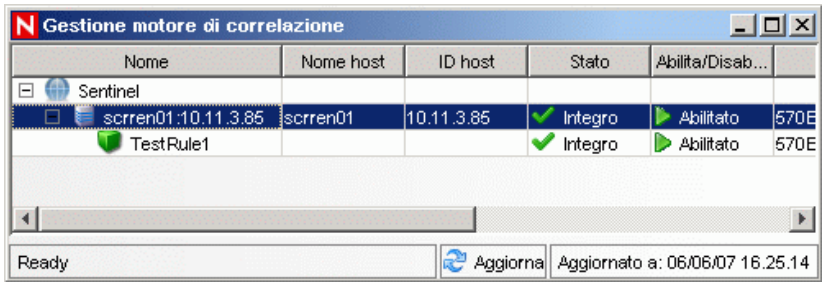
33 Evidenziare una regola e fare clic sul collegamento Distribuisci regole. Viene visualizzata la finestra Distribuisci regola.



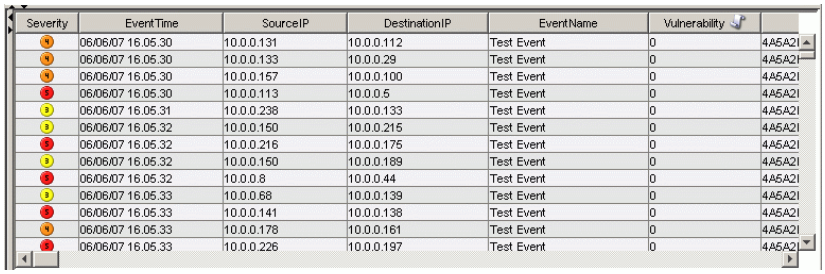
34 Nella finestra Distribuisci regola, selezionare il motore per distribuire la regola dall'elenco a discesa.

35 Selezionare un'azione “Invia e-mail” da associare alla regola e fare clic su OK. Prima di associare un'azione, è necessario crearla in Sentinel.

36 Selezionare Gestione motore di correlazione. Sotto il motore di correlazione è possibile notare che la regola è distribuita/abilitata.



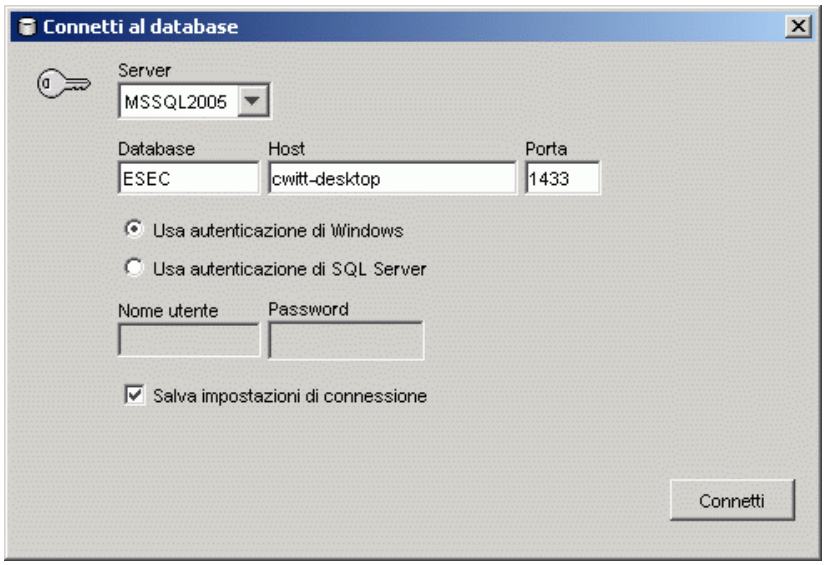
37 Passare alla scheda Active Views e verificare che sia stato generato l'evento correlato.



38 Chiudere Sentinel Control Center.

39 Fare doppio clic sull'icona di Gestione dati Sentinel sul desktop.

40 Accedere a Gestione dati Sentinel utilizzando l'utente amministrativo del database specificato durante l'installazione (per default, esecdba).



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

42 Chiudere Gestione dati Sentinel.

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

5.2 Eliminazione degli elementi del test

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

Per eliminare gli elementi del test:

1 Accedere al sistema utilizzando l'utente amministrativo di Sentinel specificato durante l'installazione (per default, esecadm).

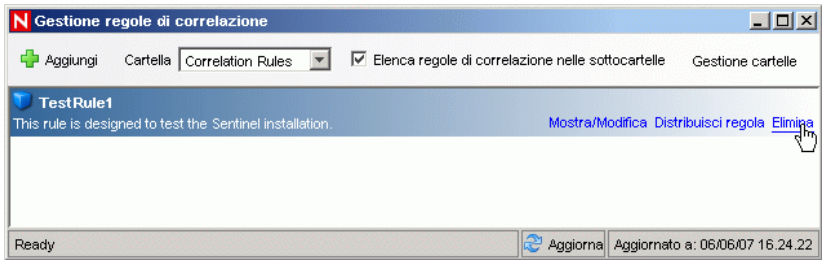
2 Passare alla scheda Correlazione.

3 Aprire Gestione motore di correlazione.

4 Fare clic col pulsante destro del mouse su RegolaTest1 in Gestione motore di correlazione e selezionare Annulla distribuzione.

5 Aprire Gestione regole di correlazione.

6 Selezionare RegolaTest1 e fare clic su Elimina.



7. Scegliere Visualizzazione in diretta dal menu Gestione origini eventi.
8. Nella gerarchia grafica delle origini di eventi, fare clic con il pulsante destro del mouse su Servizio di raccolta e selezionare Interrompi.
9. Chiudere la finestra Gestione origini eventi.
10. Passare alla scheda Caso.
11. Aprire Gestione visualizzazione caso.
12. Selezionare CasoTest1, fare clic con il pulsante destro e scegliere Elimina.

5.3 Operazioni preliminari

Per poter iniziare a lavorare con dati reali, è necessario importare e configurare servizi di raccolta adatti al proprio ambiente, configurare regole personalizzate, creare workflow iTRAC e così via. Sentinel offre pacchetti di soluzioni che consentono di iniziare a lavorare rapidamente.

Aggiunta di componenti di Sentinel

6

6.1 Aggiunta di componenti di Sentinel a un’installazione esistente

Talvolta potrebbe essere necessario installare componenti aggiuntivi di Sentinel su un computer dove è già stato installato Sentinel. Potrebbe ad esempio essere necessario installare Generatore servizi di raccolta dove è già installato Sentinel Control Center.

Il programma di installazione di Sentinel consente di eseguire facilmente questo tipo di installazione. Assicurarsi innanzitutto che i componenti aggiuntivi installati soddisfino i prerequisiti specificati in Capitolo 3, “Installazione di Sentinel 6.1”, a pagina 31. È probabile che vi sia un numero maggiore di requisiti del computer da soddisfare se si installano componenti aggiuntivi. Eseguire il programma di installazione di Sentinel sul computer di destinazione come se si eseguisse l'installazione per la prima volta. Quando viene eseguito in modalità di aggiunta di componenti, il programma di installazione si comporta in modo leggermente diverso, in particolare:

- Il programma di installazione rileva automaticamente l'installazione precedente di Sentinel e visualizza una finestra dove viene indicata l'ubicazione dell'installazione precedente e quali componenti sono già stati installati.
- Il programma di installazione non chiederà di specificare la directory di destinazione. Verrà infatti utilizzata la directory di destinazione dell'installazione precedente.
- Il programma di installazione non chiederà di selezionare un tipo di installazione semplice o personalizzata. Verrà selezionata automaticamente un'installazione personalizzata.

Nota: In un'installazione di Sentinel distribuita deve essere presente una sola istanza di Advisor e di Communication Server.

6.2 Installazione di nodi di bilanciamento del carico aggiuntivi

Talvolta potrebbe essere necessario aggiungere un nodo di elaborazione Sentinel aggiuntivo all'ambiente distribuito Sentinel per bilanciare il carico tra i computer. Se ad esempio viene utilizzata molta memoria su un computer dove viene eseguito il motore di correlazione, potrebbe essere opportuno eseguire il motore di correlazione su un altro computer (ciò potrebbe tuttavia richiedere una licenza aggiuntiva). Le regole di correlazione potrebbero quindi essere ridistribuite tra questi due computer per ridurre il carico su un singolo computer qualora tutte le regole fossero state distribuite su di esso.

A tal fine, eseguire il programma di installazione nel nuovo computer attenendosi alle istruzioni riportate in Capitolo 3, “Installazione di Sentinel 6.1”, a pagina 31. Durante la procedura del programma di installazione, selezionare solo i componenti per i quali si desidera aggiungere ulteriori nodi di bilanciamento del carico. È possibile bilanciare il carico per i seguenti componenti:

- Motore di correlazione
- Gestione servizi di raccolta
- Processo DAS_Binary

Il processo DAS_Binary è responsabile dell'inserimento degli eventi nel database. Poiché l'inserimento degli eventi nel database può provocare colli di bottiglia nel flusso degli eventi, il bilanciamento del carico del processo DAS_Binary normalmente produce un notevole incremento delle prestazioni a livello di eventi al secondo. Inoltre, i componenti del motore di correlazione e di Gestione servizi di raccolta possono essere sottoposti a bilanciamento del carico installando istanze di questi componenti su computer aggiuntivi.

6.2.1 Configurazione di più processi DAS_Binary

Le prestazioni possono essere migliorate configurando più istanze DAS_Binary in un sistema Sentinel, anche se ciò non produce un bilanciamento del carico vero e proprio. DAS_Binary è il processo che gestisce l'inserimento degli eventi nel database e configurando più processi DAS_Binary, Novell è riuscita a ottenere il tasso di eventi al secondo più elevato nel corso di prove interne. Per ulteriori informazioni sui test sulle prestazioni, visitare il sito della documentazione Novell all'indirizzo (http://www.novell.com/documentation/sentinel61).

È possibile installare più processi DAS_Binary sullo stesso computer oppure distribuirli su più computer.

Per configurare istanze del processo DAS_Binary su più computer:

1. Utilizzare il programma di installazione di Sentinel per installare il componente DAS su ognuno degli altri computer dove verrà eseguito il processo DAS_Binary. Poiché tutti i processi DAS_Binary devono connettersi allo stesso database, durante l'installazione specificare le medesime informazioni per la connessione al database specificate durante l'installazione iniziale di DAS.
2. Su tutti i computer sui quali si desidera eseguire il processo DAS_Binary, apportare le seguenti modifiche:
   - **2a** Accedere come utente esecadm (in Unix) o come Administrator (in Windows) a tutti i computer che eseguiranno istanze del processo DAS_Binary e collocare il file `configuration.xml` nella directory $ESEC_HOME/config (%ESEC_HOME%\config in Windows).
   - **2b** Aggiungere le seguenti informazioni alla sezione services (servizi) del file `configuration.xml`:

     ```
     <service name="DAS_Binary_EventStore" plugins=""
     strategyid="sentinel_client" subscriptiongroup="dasbin" />
     ```
   - **2c** Salvare il file `configuration.xml`.

3 Sui computer dove vengono eseguiti processi DAS_Binary secondari, apportare le seguenti modifiche: Un processo DAS_Binary è secondario quando non viene eseguito sul server Sentinel principale.

3a Eliminare il file `sentinelhost.id` dalla directory $ESEC_HOME/data (%ESEC_HOME%\data in Windows). In questo modo si forza l'istanza di Gestione servizi di raccolta installata su questo computer a generare un nuovo ID anziché utilizzare quello usato da Gestione servizi di raccolta installato sul server Sentinel.

3b Gli altri processi DAS vanno disabilitati. A tale scopo, nella sezione process (processo) del file `configuration.xml` situato sui computer che eseguono solo il processo DAS_Binary, impostare l'attributo min_instances come illustrato di seguito:

```
min_instances="0"
```

per le voci process (processo) seguenti:

- DAS_RT
- DAS_Aggregation
- DAS_Query
- DAS_ITRAC

4 Poiché è necessario utilizzare il servizio Sentinel secondario, modificare `sentinel.conf` nella directory ESEC_HOME/config eliminando il carattere di commento # all'inizio della riga seguente:

```
wrapper.app.parameter.1=../config/sentinel.xml
```

e aggiungendo il carattere di commento # all'inizio della riga seguente:

```
#wrapper.app.parameter.1=../config/sentinel_primary.xml
```

5 Apportare le seguenti modifiche al file `das_binary.xml` situato su uno dei computer dove verrà eseguito il processo DAS_Binary:

5a Fare una copia dell'intero componente DispatchManager e modificare l'ID del nuovo componente da DispatchManager a EventStoreDispatchManager. Dopo aver apportato questa modifica, si otterrà un componente con ID DispatchManager e un altro componente con ID EventStoreDispatchManager. Vedere l'esempio riportato sotto di come dovrebbe apparire il componente EventStoreDispatchManager.

5b Aggiornare il valore della proprietà `esecurity.communication.service` del componente EventStoreDispatchManager impostandolo su DAS_Binary_EventStore.

5c Eliminare la proprietà `handler:esecurity.event.create` dal componente DispatchManager.

5d Eliminare tutte le proprietà il cui nome inizia con "handler:*", ad eccezione di `handler:esecurity.event.create`, dal componente EventStoreDispatchManager. Il gestore `handler:esecurity.event.create` deve essere l'unico gestore definito nel componente EventStoreDispatchManager.

5e Aggiungere il seguente elemento XML al componente EventStoreService:

```
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
```

5f Salvare il file `das_binary.xml`.

6 Copiare il file `das_binary.xml` su tutti i computer dove verrà eseguito il processo DAS_Binary. Di seguito è riportato un estratto del file `das_binary.xml` che illustra il componente EventStoreDispatchManager.

```
<obj-component id="EventStoreDispatchManager">
<class>esecurity.ccs.comp.dispatcher.CommDispatcherManager</class>
<property
name="esecurity.communication.service">DAS_Binary_EventStore</
property>
<property name="dependencies">DAS_Query</property>
<property
name="handler:esecurity.event.create">esecurity.ccs.cracker.EventC
racker@ewizard_binary_event,correlation_binary_event,database_bina
ry_event,database_tagged_event,correlation_binary_event_update</
property>
<obj-component id="DispatcherStatsService">
<class>esecurity.ccs.comp.dispatcher.stats.DispatcherStatsManager<
/class>
<property name="ReportIntervals">900,3600,14400,86400</property>
<property name="MinLogReportInterval">900</property>
<property name="MinPublishReportInterval">86400</property>
<property name="ReportByServiceName">true</property>
<property name="ReportByMethodName">true</property>
<obj-component-ref>
<name>EventPublisher</name>
<ref-id>DispatchManager</ref-id>
</obj-component-ref>
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>DispatchManager</ref-id>
</obj-component-ref>
</obj-component>
</obj-component>
```

L'estratto del file `das_binary.xml` riportato di seguito illustra il componente EventStoreService:

```
<obj-component id="EventStoreService">
<class>esecurity.ccs.comp.event.EventStoreService</class>
<property name="handler">esecurity.event.create</property>
<property name="waitBlocked">true</property>
<property name="maxThreads">6</property>
<property name="minThreads">6</property>
<property name="maxThreadsQueued">10</property>
<property name="queueSize">1000000</property>
<obj-component-ref>
<name>ThreadPool</name>
<ref-id>EventStoreThreadPool</ref-id>
</obj-component-ref>
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
<obj-component id="Persistor">
<class>esecurity.ccs.comp.event.jdbc.JDBCEventStore</class>
<property name="insert.batchsize">600</property>
```

```
<property
name="insert.strategy">esecurity.ccs.comp.event.jdbc.JDBCLoadStrat
egy</property>
<property name="insert.oci.workerCount">5</property>
<property name="insert.oci.queueWaitTime">1</property>
<property name="insert.oci.highWatermark">10000000</property>
<property name="insert.oci.lowWatermark">9000000</property>
<property name="insert.oci.optimizationFlag">on</property>
<property name="insert.pmaxWarningTime">300</property>
<property name="insert.pminWarningTime">300</property>
</obj-component>
<obj-component-ref>
<name>EventRedirect</name>
<ref-id>EventFileRedirectService</ref-id>
</obj-component-ref>
</obj-component>
```

7 Per attivare le modifiche, riavviare il servizio Sentinel su tutti i computer dove sono state apportate le modifiche.

In UNIX:

```
$ESEC_HOME/bin/sentinel.sh restart
```

In Windows:

```
Restart the "Sentinel" service using the Windows Service Manager.
```

Per configurare più istanze di DAS_Binary sullo stesso computer:

1 Accedere come utente esecadm (in Unix) o come Administrator (in Windows) al computer dove verranno eseguite più istanze del processo DAS_Binary e collocare il file `configuration.xml` nella directory $ESEC_HOME/config (%ESEC_HOME%\config in Windows).

2 Nel file `configuration.xml`, individuare la sezione del file xml dove sono definite le voci dei servizi (vedere l'esempio riportato di seguito). Fare una copia della voce del servizio DAS_Binary per ogni istanza di DAS_Binary che si desidera eseguire. Se ad esempio si desiderano eseguire due processi DAS_Binary, fare due copie della voce del servizio DAS_Binary. Eliminare l'attributo uuid in ciascuna voce del servizio (l'attributo uuid verrà automaticamente rigenerato quando si avvia Sentinel). Di seguito è riportato un esempio di voce del servizio DAS_Binary.

```
<service name="DAS_Binary" plugins="" strategyid="sentinel_client"
uuid="4DA52BE0-E7A4-1029-BB2F-00132168CBDF"/>
```

3 Nel file `configuration.xml`, creare una copia della seguente voce del servizio DAS_Binary_EventStore per ogni istanza di DAS_Binary che si desidera eseguire. Poiché questo servizio non esiste nel file `configuration.xml`, è necessario copiarlo dall'esempio riportato di seguito. Per eseguire ad esempio due processi DAS_Binary, fare due copie della seguente voce del servizio DAS_Binary_EventStore:

```
<service name="DAS_Binary_EventStore" plugins=""
strategyid="sentinel_client" subscriptiongroup="dasbin" />
```

4 Assegnare a ciascuna voce del servizio DAS_Binary e DAS_Binary_EventStore un nome univoco. I nomi dei servizi potrebbero ad esempio essere: DAS_Binary1, DAS_Binary_EventStore1, DAS_Binary2 e DAS_Binary_EventStore2.

5 Nel file `configuration.xml`, individuare la sezione dove sono definite le voci dei processi (vedere l'esempio riportato di seguito). Fare una copia della voce del processo DAS_Binary per ogni istanza di DAS_Binary che si desidera eseguire. Se ad esempio si desiderano eseguire due processi DAS_Binary, fare due copie della voce del processo DAS_Binary. Per ciascuna voce del processo DAS_Binary, modificare le sezioni della voce come descritto di seguito:

- **DAS_Binary Dsrv_name:** modificare assegnando gli stessi nomi definiti nel passaggio 4, ad esempio DAS_Binary2.
- **Nome del servizio di comunicazione DAS_Binary:** inserire il seguente testo nell'attributo di immagine della voce di processo in corrispondenza del punto indicato in grassetto dell'esempio di voce di processo riportato di seguito. Per ciascuna voce del processo DAS_Binary, sostituire la parte di testo riportata sotto riguardante DAS_Binary con il nome del servizio associato, ad esempio: DAS_Binary2.

  `-Desecurity.communication.service=DAS_Binary`
- **Nome del file `das_binary.xml` :** assegnare un qualsiasi nome univoco, ad esempio: `das_binary_2.xml`. Questi nomi verranno utilizzati in uno dei prossimi passaggi.
- **Nome del file das_binary_log_prop:** assegnare un qualsiasi nome univoco, ad esempio: `das_binary_log_2.prop`. Questi nomi verranno utilizzati in uno dei prossimi passaggi.
- **Nome della directory das_binary.cache:** assegnare un qualsiasi nome univoco, ad esempio: `das_binary2.cache`. Ciascuna istanza di DAS_Binary deve utilizzare una directory `das_binary.cache` diversa.
- **Nome del processo DAS_Binary:** modificare il valore dell'attributo nome della voce di processo in modo che corrisponda ai nomi dei servizi DAS_Binary definiti al passaggio 4, ad esempio: DAS_Binary2.

Di seguito è riportato un esempio di xml di una tipica voce di processo a cui fanno riferimento le istruzioni riportate sopra.

```
process component="DAS" depends="UNIX Communication Server,Windows
Communication Server" image="&amp;quot;$(ESEC_JAVA_HOME)/java&amp;quot; -
server -Dsrv_name=DAS_Binary -Xmx160m -Xms64m -XX:+UseParallelGC -
XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=../log/
DAS_Binary.hprof -Xss136k -Xrs -
Desecurity.communication.service=DAS_Binary -Duser.language=en  -
Djava.net.preferIPv4Stack=true -Dfile.encoding=UTF8 -
Desecurity.cache.directory=../data/das_binary.cache -
Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml -
Djava.util.logging.config.file=../config/das_binary_log.prop -
Dcom.esecurity.configurationfile=../config/configuration.xml -
Djava.security.auth.login.config=../config/auth.login -
Djava.security.krb5.conf=../config/krb5.conf -jar ../lib/
ccsbase.jar ..//config//das_binary.xml" min_instances="1"
name="DAS_Binary" post_startup_delay="20" type="container"
working_directory="$(ESEC_HOME)/data"/>
```

6 Salvare il file `configuration.xml`.

7 Individuare il file `das_binary.xml` nella directory $ESEC_HOME/config (%ESEC_HOME%\config in Windows).

8. Creare una copia del file `das_binary.xml` per ciascuna istanza del processo DAS_Binary che si desidera eseguire. Per eseguire ad esempio due istanze di DAS_Binary, creare due copie del file `das_binary.xml`.
9. Rinominare le copie del file `das_binary.xml` assegnando i nomi riportati al passaggio 5.
10. Apportare le seguenti modifiche a ciascun file `das_binary.xml`:
    - Fare una copia dell'intero componente DispatchManager e modificare l'ID del nuovo componente da DispatchManager a EventStoreDispatchManager. Dopo aver apportato questa modifica, si otterrà un componente con ID DispatchManager e un altro componente con ID EventStoreDispatchManager.
    - Aggiornare il valore della proprietà `esecurity.communication.service` del componente DispatchManager assegnando un nome univoco appropriato al processo DAS_Binary, ad esempio: DAS_Binary2.
    - Aggiornare il valore della proprietà `esecurity.communication.service` del componente EventStoreDispatchManager assegnando un nome univoco appropriato al processo DAS_Binary_EventStore, ad esempio: DAS_Binary_EventStore2.
    - Eliminare la proprietà `handler:esecurity.event.create` dal componente DispatchManager.
    - Eliminare tutte le proprietà il cui nome inizia con “handler:*”, ad eccezione di `handler:esecurity.event.create`, dal componente EventStoreDispatchManager. Il gestore `handler:esecurity.event.create` deve essere l'unico gestore definito nel componente EventStoreDispatchManager.
    - Aggiungere il seguente elemento XML al componente EventStoreService:

      ```
      <obj-component-ref>
         <name>DispatchManager</name>
         <ref-id>EventStoreDispatchManager</ref-id>
      </obj-component-ref>
      ```
11. Salvare i file `das_binary.xml`.
12. Individuare il file `das_binary_log.prop` nella directory $ESEC_HOME/config (%ESEC_HOME%\config in Windows).
13. Creare una copia del file `das_binary_log.prop` per ciascuna istanza del processo DAS_Binary che si desidera eseguire. Per eseguire ad esempio due istanze di DAS_Binary, creare due copie del file `das_binary_log.prop`.
14. Rinominare i file `das_binary_log.prop` assegnando i nomi riportati al passaggio 5.
15. Riavviare il servizio Sentinel per attivare le modifiche.

    In UNIX:

    ```
    $ESEC_HOME/bin/sentinel.sh restart
    ```

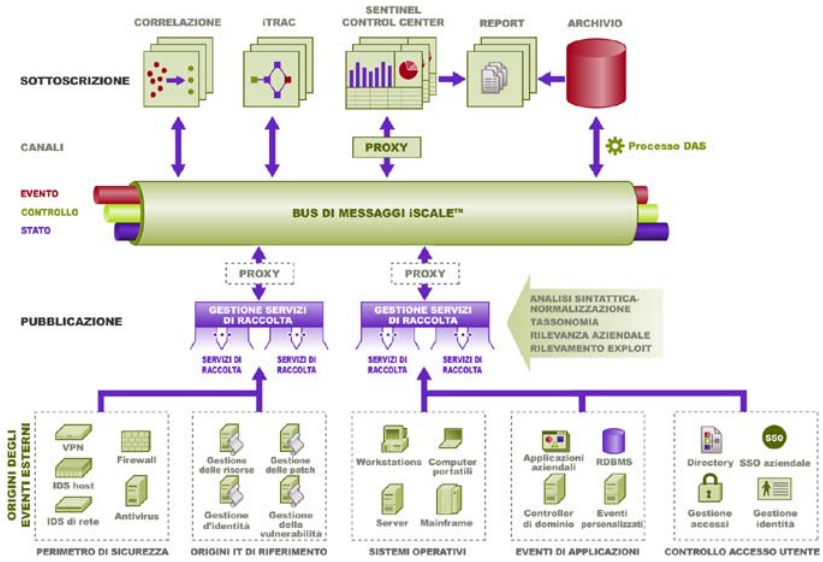
    In Windows:

    ```
    Restart the “Sentinel” service using the Windows Service Manager.
    ```

Layer di comunicazione (iSCALE) 7

Il layer di comunicazione (iSCALE) che connette tutti i componenti dell'architettura è una connessione cifrata basata su TCP/IP e incorporata a un backbone JMS (Java Messaging Service). Con Sentinel 6 è stato aggiunto un proxy SSL facoltativo per proteggere i componenti Gestione servizi di raccolta e Sentinel Control Center, se questi sono installati all'esterno del firewall.

Figura 7-1 *Architettura di Sentinel*



Quando si installa Gestione servizi di raccolta, sono disponibili due opzioni di comunicazione:

- **Eseguire la connessione direttamente al bus messaggi (default):** si tratta di un'opzione molto semplice e rapida. Gestione servizi di raccolta deve tuttavia conoscere la chiave di cifratura condivisa del bus messaggi e ciò potrebbe comportare un rischio per la sicurezza nel caso in cui Gestione servizi di raccolta sia eseguito su un computer esposto a minacce alla sicurezza (ad esempio, un computer nella zona DMZ). Questa opzione consentirà di proteggere le comunicazioni tramite la cifratura AES a 128 bit sulla base dei dati contenuti in un file denominato `.keystore`.
- **Eseguire la connessione al bus messaggi tramite il proxy:** Questa opzione consente di aggiungere un layer aggiuntivo di sicurezza configurando Gestione servizi di raccolta per la connessione tramite un server proxy SSL. In questo caso, verranno utilizzate l'autenticazione basata su certificati e la cifratura, in modo che non sia necessario memorizzare il file `.keystore` sul computer di Gestione servizi di raccolta. Questa è una soluzione efficace quando Gestione servizi di raccolta è installato in un ambiente meno sicuro.

Quando si installa Gestione servizi di raccolta, è possibile scegliere una di queste due opzioni. Per default, in Sentinel Control Center viene utilizzato il proxy.

7.1 Proxy SSL e comunicazione diretta

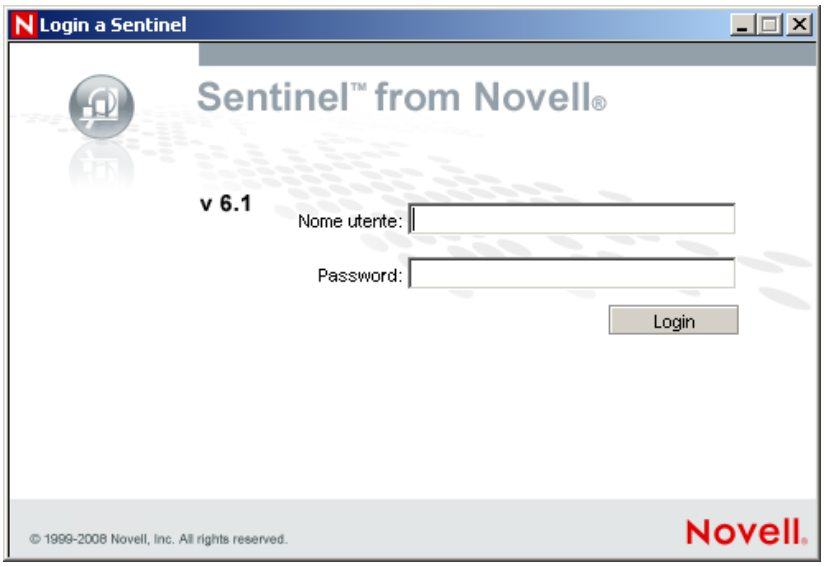
I componenti di Sentinel in grado di utilizzare il proxy SSL sono Sentinel Control Center e Gestione servizi di raccolta.

7.1.1 Sentinel Control Center

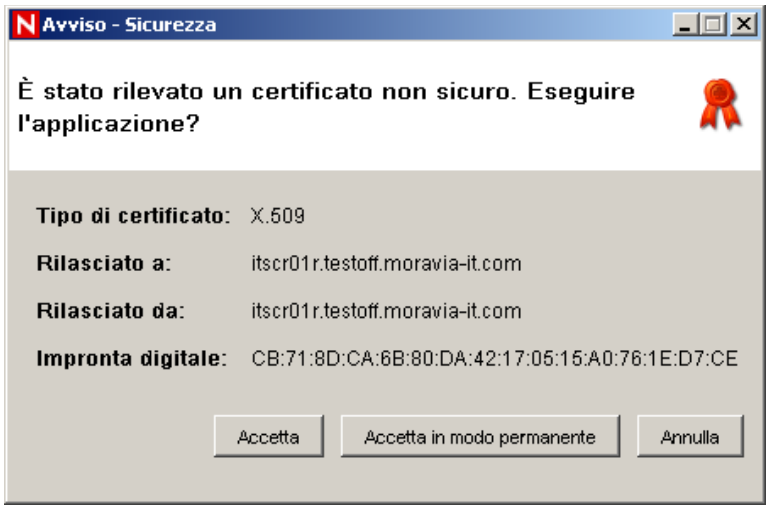
Per default, in Sentinel Control Center viene utilizzato il proxy SSL. Sentinel Control Center si connette a SSL attraverso la porta `proxied_client`. Questa porta è configurata per utilizzare solo l'autenticazione basata su certificati SSL lato server. L'autenticazione lato client utilizza il nome utente e la password dell'utente di Sentinel Control Center.

Per accedere a Sentinel Control Center per la prima volta:

1. Passare a Start > Programmi > Sentinel e selezionare Sentinel Control Center. Verrà visualizzata la finestra Login a Sentinel.



2. Immettere le credenziali utente disponibili per accedere a Sentinel Control Center.
   - Nome utente e password, se si utilizza l'autenticazione SQL Server, OPPURE
   - Dominio\nome utente e password, se si utilizza l'autenticazione Windows
3. Fare clic su Login.
4. Verrà visualizzato un messaggio di avviso (illustrato nella figura seguente) per il primo tentativo di login.



5 Se si seleziona Accetta, questo messaggio verrà visualizzato a ogni tentativo di aprire Sentinel sul sistema. Per evitarlo, è possibile selezionare Accetta in modo permanente.

Per avviare Sentinel Control Center in Linux e Solaris:

1 In veste di utente amministratore di Sentinel (esecadm), passare alla directory:
`$ESEC_HOME/bin`

2 Eseguire il comando seguente:
`control_center.sh`

3 Immettere il nome utente e la password, quindi fare clic su OK.

4 Verrà visualizzata una finestra Certificato. Fare clic su Accetta.

Gli utenti di Sentinel Control Center dovranno ripetere la procedura precedente per accettare un nuovo certificato nei seguenti casi:

- Il server di comunicazione di Sentinel viene reinstallato
- Il server di comunicazione di Sentinel viene spostato su un nuovo server.

7.1.2 Gestione servizi di raccolta

Gestione servizi di raccolta può essere installato in modalità proxy (tramite il proxy SSL) o in modalità diretta (attraverso una connessione diretta al bus messaggi).

- Per le istanze di Gestione servizi di raccolta che potrebbero essere più facilmente compromesse (ad esempio, un computer nella zona DMZ), il proxy SSL è il metodo di comunicazione più sicuro.
- Per le istanze di Gestione servizi di raccolta che si trovano in un ambiente più sicuro o dove è importante ottenere una velocità degli eventi molto elevata o per le istanze che sono installate nello stesso computer del servizio DAS (Data Access Service), è consigliata la comunicazione diretta al bus messaggi.

Gestione servizi di raccolta si connette a SSL tramite la porta`proxied_trusted_client`. Per consentire il riavvio automatico di Gestione servizi di raccolta dopo un riavvio del sistema, questa porta è configurata per utilizzare l'autenticazione basata su certificati SSL server e client. Tra il

proxy e Gestione servizi di raccolta viene stabilita una relazione di fiducia (scambio di certificati), in cui nelle future connessioni verranno utilizzati i certificati per l'autenticazione. Questa relazione di fiducia viene configurata automaticamente durante l'installazione.

La relazione di fiducia per ogni istanza di Gestione servizi di raccolta che utilizza il proxy SSL deve essere reimpostata nei seguenti casi:

- Il server di comunicazione di Sentinel viene reinstallato
- Il server di comunicazione di Sentinel viene spostato su un nuovo server

Questa procedura può essere utilizzata anche per far passare un'istanza di Gestione servizi di raccolta dalla modalità diretta alla modalità proxy.

Per reimpostare la relazione di fiducia per Gestione servizi di raccolta:

1. Accedere al server di Gestione servizi di raccolta come amministratore di Sentinel (per default, esecadm).
2. Aprire il file `configuration.xml` in $ESEC_HOME/config o %ESEC_HOME%\config in un editor di testo.
3. Modificare i servizi "Collector_Manager", "agentmanager_events" e "Sentinel" in `configuration.xml` in modo da utilizzare l'ID di strategia "proxied_trusted_client". Di seguito è riportato un estratto di un file di esempio:

   ```
   <service name="Collector_Manager" plugins=""
   strategyid="proxied_trusted_client"/>
   <service name="agentmanager_events" plugins=""
   strategyid="proxied_trusted_client"/>
   <service name="Sentinel" plugins=""
   strategyid="proxied_trusted_client"/>
   ```

4. Salvare il file e uscire.
5. Eseguire `%ESEC_HOME%\bin\register_trusted_client.bat` (o il file `.sh` in UNIX). L'output visualizzato sarà analogo al seguente:

   ```
   E:\Program Files\novell\sentinel6>bin\register_trusted_client.bat
   Please review the following server certificate:
   Type: X.509
   Issued To: foo.bar.net
   Issued By: foo.bar.net
   Fingerprint (MD5): A8:DF:BA:B2:F3:21:C9:27:28:48:13:B3:FE:F8:B4:AD
   Would you like to accept this certificate? [Y/N] (defaults to N): Y
   Please enter a Sentinel username and password that has permissions
   to register a trusted client.
   Username: esecadm
   Password:*********
   *Writing to keystore file: E:\Program
   Files\Novell\Sentinel6\config\.proxyClientKeystore
   ```

6. Riavviare il servizio Sentinel sul server host di Gestione servizi di raccolta.
7. Ripetere questi passaggi per tutte le istanze di Gestione servizi di raccolta che utilizzano la comunicazione proxy.

7.2 Modifica della chiave di cifratura per la comunicazione

L'installazione di Sentinel consente all'amministratore di generare una nuova chiave di cifratura casuale (memorizzata nel file `.keystore`) o di importare un file `.keystore` esistente. Indipendentemente dal metodo adottato, per il corretto funzionamento delle comunicazioni, è necessario che il file `.keystore` sia lo stesso su ogni computer sul quale è installato un componente di Sentinel.

Nota: Il file `.keystore` non è necessariamente sul computer del database se il database è il solo componente di Sentinel installato in questo computer. Questo file non è inoltre necessario su computer dove è installato solo Sentinel Control Center, Generatore servizi di raccolta, Gestione dati Sentinel o Gestione servizi di raccolta (con utilizzo del proxy).

La chiave di cifratura può essere modificata tramite un'utility denominata `keymgr` che genera un file contenente una chiave di cifratura casuale. Questo file deve essere copiato su ogni computer in cui è installato un componente di Sentinel Server.

Per modificare la chiave di cifratura per la comunicazione diretta:

1. Per UNIX, eseguire il login come utente amministratore di Sentinel (per default, esecadm). Per Windows, accedere come utente con diritti di amministrazione.
2. Passare a:

   In UNIX:

   `$ESEC_HOME/lib`

   In Windows:

   `%ESEC_HOME%\lib`
3. Eseguire il comando seguente:

   In UNIX:

   ```
   keymgr.sh --keyalgo AES --keysize 128 --keystore <output filename, usually .keystore>
   ```

   In Windows:

   ```
   keymgr.bat --keyalgo AES --keysize 128 --keystore <output filename, usually .keystore>
   ```
4. Copiare il file `.keystore` in ogni computer in cui è installato un componente di Sentinel Server (a meno che non venga utilizzata la comunicazione proxy). È necessario copiare il file in:

   In UNIX:

   `$ESEC_HOME/config`

   In Windows:

   `%ESEC_HOME%\config`

Nota: Se si utilizza Advisor in modalità Scaricamento diretto, è necessario aggiornare le password memorizzate nei file di configurazione di Advisor. Questa password viene cifrata tramite le informazioni contenute nel file `.keystore` e deve essere ricreata tramite il nuovo valore del file `.keystore`. Per aggiornare la password, seguire le istruzioni riportate nel Capitolo 4, "Configurazione di Advisor", a pagina 63.

7.3 Aumento della robustezza della chiave AES

Sentinel utilizza la cifratura AES per comunicazioni tramite Sonic e password di cifratura memorizzate in file config e inviate tramite Sonic. Per default, Sentinel utilizza un algoritmo di cifratura AES a 128 bit a causa di particolari restrizioni di importazione. Se queste restrizioni di importazione non sono presenti nel proprio ambiente, è possibile utilizzare un algoritmo di cifratura AES più robusto a 256 bit.

Nota: Si consiglia vivamente di consultare la sezione "Understanding the Export/Import Issues" (Problemi relativi a esportazione/importazione) del file `Readme.txt` Java prima di abilitare la cifratura a 256 bit.

Per configurare la cifratura AES a 256 bit.

1. Scaricare le norme di cifratura illimitata di Sun dal sito http://java.sun.com/javase/downloads/index_jdk5.jsp (http://java.sun.com/javase/downloads/index_jdk5.jsp). Nell'altra sezione di download, scaricare "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0".
2. Applicare questo file di norme a tutti i JRE che eseguono processi che si connettono direttamente a Sonic (DAS, motore di correlazione, Communication Server, Gestione servizi di raccolta se utilizzati in modalità di comunicazione diretta con Sonic). Per capire come vanno applicati i file di norme, consultare il file `Readme.txt` disponibile insieme alle norme scaricate.
3. Utilizzare l'utility keymgr per generare un file `.keystoreAES` a 256 bit seguendo le istruzioni fornite nella sezione Sezione 7.2, "Modifica della chiave di cifratura per la comunicazione", a pagina 95.
4. Copiare questo file `.keystore` su tutti i computer di cui al passaggio 2 e collocarlo nella directory $ESEC_HOME/config o %ESEC_HOME%\config.

Nota: Se si utilizza Advisor in modalità Scaricamento diretto, è necessario aggiornare le password memorizzate nei file di configurazione di Advisor. Questa password viene cifrata tramite le informazioni contenute nel file `.keystore` e deve essere ricreata tramite il nuovo valore del file `.keystore`. Per ulteriori informazioni sull'aggiornamento delle password, vedere la sezione "Certificate Management for DAS_Proxy" della *Reference Guide*.

Crystal Reports per Windows

8

Crystal Reports Server™ (di Business Objects) è uno strumento per la generazione di rapporti utilizzato con Sentinel. In questa sezione viene illustrata l'installazione e la configurazione di Crystal Reports Server per Sentinel. Per ulteriori informazioni sulle piattaforme supportate per Crystal Reports Server in un ambiente Sentinel, vedere il Capitolo 2, “Requisiti di sistema”, a pagina 21.

In Windows, Sentinel è stato testato con Crystal Reports Server XI R2 SP3. Per ulteriori informazioni su Crystal Reports Server XI Release 2 Service Packs, visitare la pagina Web all'indirizzo https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads) ed eseguire la ricerca della versione e della piattaforma corrette.

Questo capitolo spiega come eseguire Crystal Reports Server in Windows. Per ulteriori informazioni sull'esecuzione di Crystal Reports Server in Linux/Solaris, vedere il .

Per installare Crystal Reports Server:

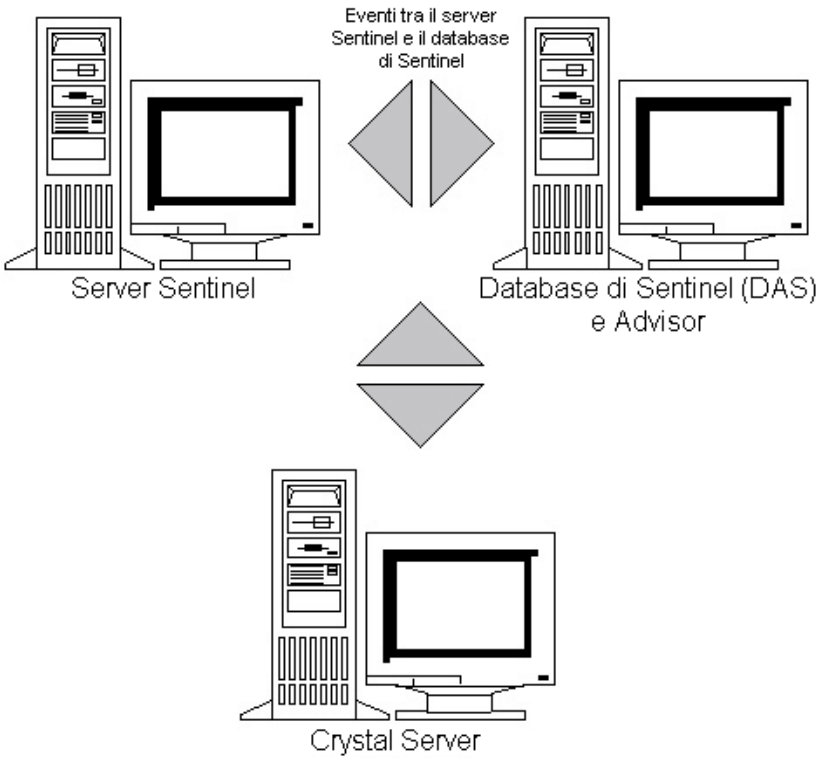
1. Installare Microsoft IIS e ASP.NET
2. Installare Microsoft SQL in base alla configurazione: come autenticazione Windows o SQL Server.
3. Per gli utenti di lingua cinese (tradizionale e semplificata) e giapponese: installare font asiatici (ad esempio, Arial Unicode MS) per visualizzare i rapporti in queste lingue.
4. Installare Crystal Reports Server
   - Configurazione di ODBC (Open Database Connectivity) per l'autenticazione SQL

     oppure
   - Installazione e configurazione del software Oracle 9i Client
5. Configurare `inetmgr`
6. Applicare la patch di Crystal Reports
7. Pubblicare (importare) rapporti di Crystal Reports
8. Impostare un conto per utente denominato
9. Verificare la connettività al server Web

10 Aumentare il limite di record per l'aggiornamento di rapporti di Crystal Reports Server (consigliato)

11 Configurare Sentinel Control Center per l'integrazione con Crystal Reports Server.

Nota: è necessario installare i componenti nell'ordine indicato sopra.



8.1 Panoramica

Il server Crystal Report richiede un database in cui memorizzare le informazioni sul sistema e i relativi utenti. Questo database è chiamato CMS (Server di gestione centrale, Central Management Server) e corrisponde a un server in cui vengono memorizzate le informazioni sul sistema Crystal Reports Server. Gli altri componenti di Crystal Reports Server possono accedere a queste informazioni.

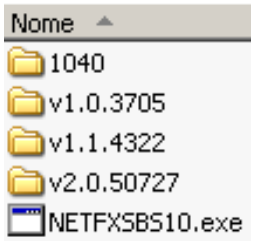
Per installare Crystal Reports Server in Windows, è necessario configurare il database CMS a un livello superiore rispetto a un database di Microsoft SQL Server locale. Sebbene il programma di installazione di Crystal Reports Server consenta di installare il database CMS a un livello superiore rispetto al database MSDE, questa configurazione non è stata testata per Sentinel e non è supportata.

8.2 Requisiti di sistema

Windows® 2003 Server SP1, una partizione NTFS con IIS (Microsoft Internet Information Server) e ASP.NET installati. Sentinel non supporta Crystal XI R2 in Windows® 2000 Server.

.NET Framework 1.1 o 2.0 (installato per default in Windows 2003). Per determinare la versione di .NET Framework installata nel computer in uso, passare a %SystemRoot%\Microsoft.NET\Framework. La cartella con il numero maggiore non deve superare il valore v.1.1.xxxx. Ad esempio:

Figura 8-1 *Versione di .NET Framework*



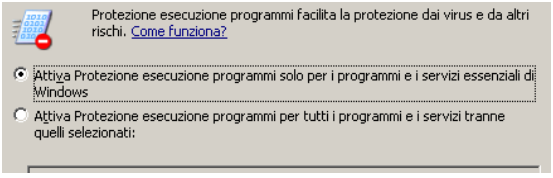
Per ulteriori informazioni sulle piattaforme supportate per Crystal Reports Server in un ambiente Sentinel, vedere Capitolo 2, “Requisiti di sistema”, a pagina 21.

8.3 Requisiti di configurazione

1. Accertarsi che il conto utilizzato per installare Crystal Reports Server disponga dei diritti di amministratore locale.
2. Impostare l'applicazione DEP (Data Execution Prevention) in modo che venga eseguita solo nei programmi e servizi Windows essenziali. Ciò consente di evitare la visualizzazione del messaggio "Error 1920. Service Crystal Report Cache Server on Windows 2003 (Errore 1920. Servizio Crystal Report Cache Server in Windows 2003)".

   Per accedere a Protezione esecuzione programmi, scegliere Pannello di controllo > Sistema> scheda Avanzate > Impostazioni prestazioni > Protezione esecuzione programmi.

   Selezionare Attiva Protezione esecuzione programmi solo per i programmi e i servizi essenziali di Windows.



3. Le istruzioni relative all'installazione e alla configurazione di Crystal Reports Server presuppongono che il server e il database di Sentinel siano stati già installati. È necessario conoscere la modalità di autenticazione selezionata per l'utente dei rapporti di Sentinel. Se si utilizza l'autenticazione di database locale, il nome dell'utente è esecrpt. Se si utilizza l'autenticazione Windows, è possibile scegliere un nome qualsiasi. La modalità di autenticazione è stata impostata in una schermata simile a quella riportata di seguito durante il processo di installazione di Sentinel.

Nota: In Windows, la password esecrpt può essere impostata esplicitamente.

4 È richiesta una risoluzione video di 1024 x 768 o superiore

5 Installare Microsoft Internet Information Server (IIS) e ASP.NET

Nota: Sentinel non supporta l'utilizzo di MSDE come database CMS di Crystal. Installare Microsoft SQL Server 2005 prima di Crystal Reports Server XI R2.

8.3.1 Installazione di Microsoft Internet Information Server (IIS) e ASP.NET

Per aggiungere questi componenti di Windows, potrebbe essere necessario utilizzare il CD di installazione di Windows 2003 Server.

Per installare IIS e ASP.NET:

1 Passare a Pannello di controllo > Installazione applicazioni.

2 Nel pannello verticale sinistro fare clic su Installazione componenti di Windows.

3 Selezionare Application Server.

4 Fare clic su Dettagli

5 Selezionare ASP.NET e Internet Information Services (IIS).

6 Fare clic su OK.

7 Fare clic su Avanti. Potrebbe essere richiesto l'inserimento del CD di installazione di Windows.

8 Fare clic su Fine.

8.4 Problemi noti

- **Installazione di Crystal Reports:** Novell fornisce due chiavi per Crystal, una per Crystal Reports Server e l'altra per Crystal Reports Developer (per modificare o creare nuovi rapporti). Accertarsi che durante l'installazione di Crystal Reports Server venga utilizzata la chiave corrispondente.
- **Disinstallazione di Crystal Reports:** qualora fosse necessario disinstallare Crystal Reports Server, è disponibile una procedura manuale di disinstallazione che elimina le chiavi di registro. Questa procedura è particolarmente utile quando l'installazione è danneggiata. Per le procedure relative alla disinstallazione manuale di Crystal Reports Server, visitare il sito Web di Business Objects all'indirizzo http://support.businessobjects.com/library/kbase/articles/c2017905.asp (http://support.businessobjects.com/library/kbase/articles/c2017905.asp).

Nota: al momento della pubblicazione di questa guida, l'URL indicato sopra risulta corretto.

8.5 Uso di Crystal Reports

Per ulteriori informazioni sull'uso di Crystal Reports Server per la generazione di rapporti in Sentinel, vedere la documentazione relativa a Crystal Reports Server (http://support.businessobjects.com/documentation/product_guides/default.asp) e la *Sentinel User Guide*.

8.6 Panoramica relativa all'installazione

8.6.1 Panoramica sull'installazione di Crystal Reports con database Microsoft SQL Server 2005

Di seguito sono elencati i passaggi principali relativi all'installazione di Crystal Reports Server con un database Sentinel Microsoft SQL Server 2005 che utilizza autenticazione Windows o autenticazione SQL. Ciascun passaggio è descritto più dettagliatamente nel resto del capitolo.

1. Installare Crystal Reports Server XI R2
   - Se durante l'installazione di Sentinel è stata selezionata l'autenticazione Windows per l'utente dei rapporti di Sentinel, vedere la Sezione 8.7.1, "Installazione di Crystal Reports Server per Microsoft SQL Server 2005 con autenticazione Windows", a pagina 102.
   - Se invece è stata selezionata l'autenticazione SQL per l'utente dei rapporti di Sentinel, vedere la Sezione 8.7.2, "Installazione di Crystal Reports Server per Microsoft SQL Server con autenticazione SQL", a pagina 107.
2. Configurare ODBC (Open Database Connectivity)
3. Mappare Crystal Reports per l'utilizzo con Sentinel
4. Applicare la patch di Crystal Reports
5. Pubblicare i rapporti
6. Impostare un conto per utente denominato

7 Creare una pagina Web Crystal (Sezione 8.9.5, “Configurazione delle autorizzazioni per i rapporti”, a pagina 120)

8 Configurare Sentinel sul server Crystal Report Server

Nota: Questi passaggi vanno eseguiti nell'ordine indicato.

8.6.2 Panoramica sull'installazione di Crystal Reports con database Oracle

Di seguito sono elencati i passaggi principali relativi all'installazione di Crystal Reports Server con un database Sentinel Oracle. Ciascun passaggio è descritto più dettagliatamente nel resto del capitolo.

Per installare correttamente Crystal Reports, eseguire la procedura seguente nell'ordine indicato.

1 Installare Oracle Client e configurare il driver nativo Oracle

2 Per gli utenti di lingua cinese (tradizionale e semplificata) e giapponese: installare font asiatici (ad esempio, Arial Unicode MS) per visualizzare i rapporti in queste lingue.

3 Installare Crystal Reports Server XI R2. Per ulteriori informazioni, vedere la Sezione 8.7.3, “Installazione di Crystal Reports Server per Oracle”, a pagina 112.

4 Mappare Crystal Reports per l'utilizzo con Sentinel

5 Importare i modelli di Crystal Reports

6 Creare una pagina Web Crystal (Sezione 8.9.5, “Configurazione delle autorizzazioni per i rapporti”, a pagina 120)

7 Configurare Sentinel sul server Crystal Report Server

Nota: Questi passaggi vanno eseguiti nell'ordine indicato.

8.7 Installazione

In questa sezione viene spiegato come installare Crystal Reports Server per:

- Sezione 8.7.1, “Installazione di Crystal Reports Server per Microsoft SQL Server 2005 con autenticazione Windows”, a pagina 102
- Sezione 8.7.2, “Installazione di Crystal Reports Server per Microsoft SQL Server con autenticazione SQL”, a pagina 107
- Sezione 8.7.3, “Installazione di Crystal Reports Server per Oracle”, a pagina 112

8.7.1 Installazione di Crystal Reports Server per Microsoft SQL Server 2005 con autenticazione Windows

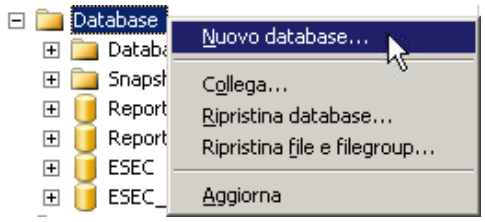
Per installare Crystal Reports Server con autenticazione Windows:

1 Installare Microsoft SQL Server 2005 in modalità mista.

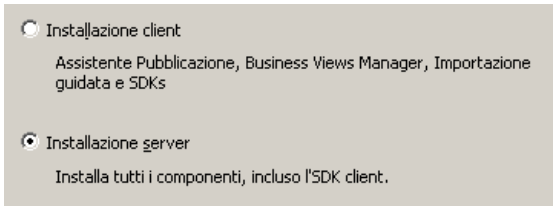
2 Avviare Microsoft SQL Server Management Studio.

3 Nel riquadro di spostamento espandere Database.

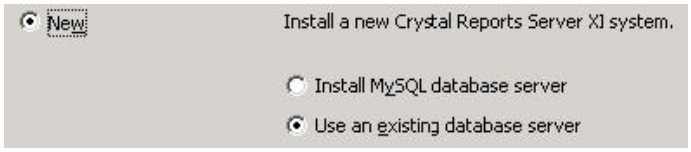
Evidenziare Database, fare clic con il pulsante destro del mouse e scegliere Nuovo database per creare il database CMS di Crystal.



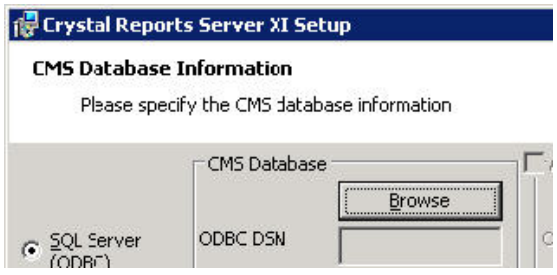
4. Nel campo Nome database, digitare BOE115 e fare clic su OK.
5. Uscire da Microsoft SQL Server Management Studio.
6. Inserire il CD di Crystal Reports XI R2 Server nell'unità CD-ROM.
7. Se sul computer in uso la funzione AutoPlay è disabilitata, eseguire `setup.exe`.
8. Selezionare la lingua per l'installazione di Crystal Reports.
9. Nella finestra Select Client or Server Installation, scegliere Perform Server Installation.



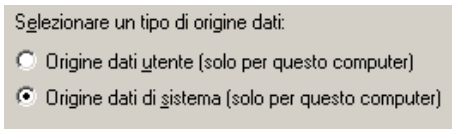
10. Immettere il codice di licenza di Crystal (fornito dal Customer Center di Novell (https://secure-www.novell.com/center/regadmin)).
11. Specificare una cartella di destinazione.
12. Per il tipo di installazione, selezionare Use an existing database server.



13. Nel riquadro CMS Database, fare clic su Browse.

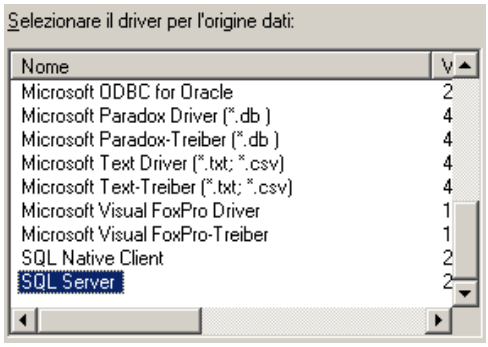


14. Fare clic sulla scheda Machine Data Source. Fare clic su New.
15. Selezionare System Data Source.

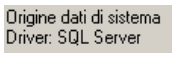


Fare clic su Next.

16 Scorrere l'elenco, selezionare SQL, quindi fare clic su Next.



17 Quando viene visualizzata una nuova origine, fare clic su Finish.

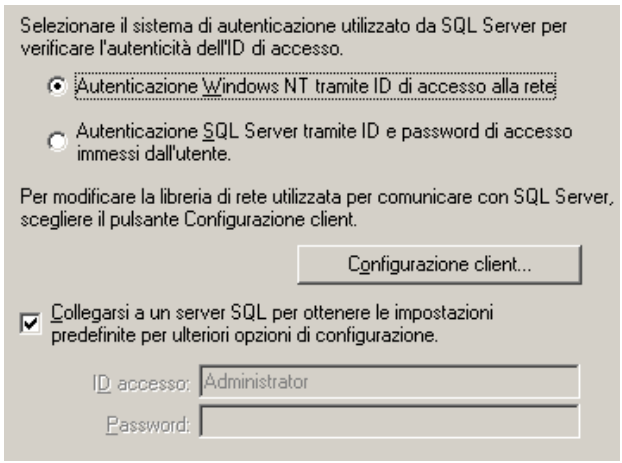


18 Nella finestra New Data Source to SQL Server, immettere:

- il nome dell'origine dati (ad esempio, BOE_XI)
- la descrizione (facoltativo)
- per il server, fare clic sulla freccia giù, quindi selezionare (local)

Fare clic su Next.

19 Se necessario, selezionare With Windows NT e fare clic su Next.



Nota: L'ID login (non attivo) è il nome di accesso Windows.

---

20 Selezionare la casella di controllo Change the default database to. Modificare il database di default impostandolo su BOE115. Fare clic su Next.

21 Nella finestra Create a New Data Source to SQL Server, fare clic su Finish.

22 Fare clic su Test Data Source e verificare l'origine dati. Dopo il test dell'origine dati, fare clic su OK.

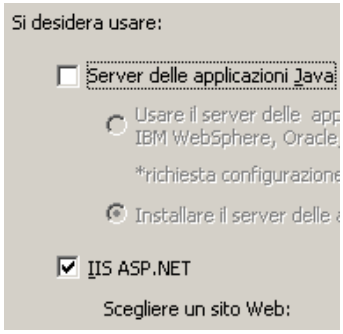
23 Nella finestra Select Data Source, evidenziare BOE115 e continuare a fare clic su OK finché non viene visualizzata la schermata SQL Server Login. Assicurarsi che la casella di controllo Usa connessione trusted sia selezionata. Fare clic su OK.

Nota: l'ID di login (non attivo) corrisponde al nome di login di Windows.

---

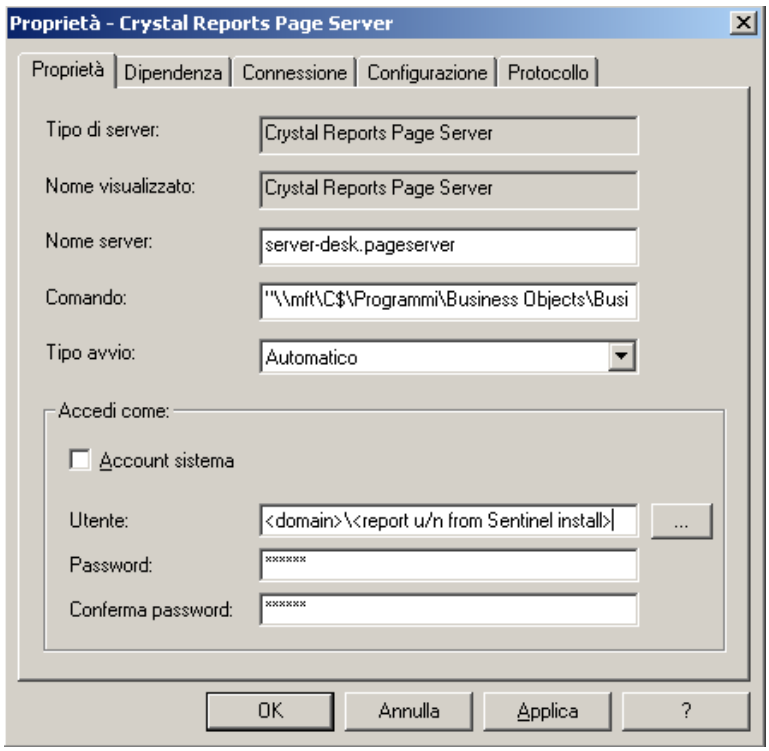
24 Nella finestra Web Component Adapter Type selezionare IIS ASP.NET.

Nota: se non si è installato IIS e ASP.NET mediante Pannello di controllo > Installazione applicazioni > Installazione componenti di Windows, IIS ASP.NET non sarà attivo.



25 Al termine dell'installazione è necessario modificare il conto di login per il page server e il job server di Crystal Reports impostandolo sul conto del dominio utente dei rapporti Sentinel.

- Fare clic su Start > Programmi > BusinessObjects > Crystal Reports Server > Central Configuration Manager.
- Fare clic con il pulsante destro del mouse su Crystal Reports Page Server quindi scegliere Stop.
- Fare clic con il pulsante destro del mouse su Crystal Reports Page Server quindi scegliere Properties.
- Deselezionare Log On As System Account, quindi specificare il nome utente e la password del conto del dominio utente di Sentinel Reports utilizzati per l'utente di Sentinel Reports durante l'installazione di Sentinel. Fare clic su OK.



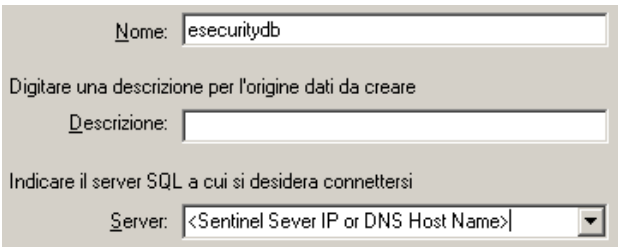
26 Evidenziare Crystal Reports Page Server e fare clic con il pulsante destro del mouse per l'avvio.

Configurazione di ODBC (Open Database Connectivity) per l'autenticazione Windows

Questa procedura consente di configurare il nome dell'origine dati ODBC in modo da consentire la connessione di Crystal Reports Server al database di Sentinel in Windows e SQL Server mediante l'autenticazione di Windows. Questi passaggi devono essere eseguiti nel computer di Crystal Reports Server.

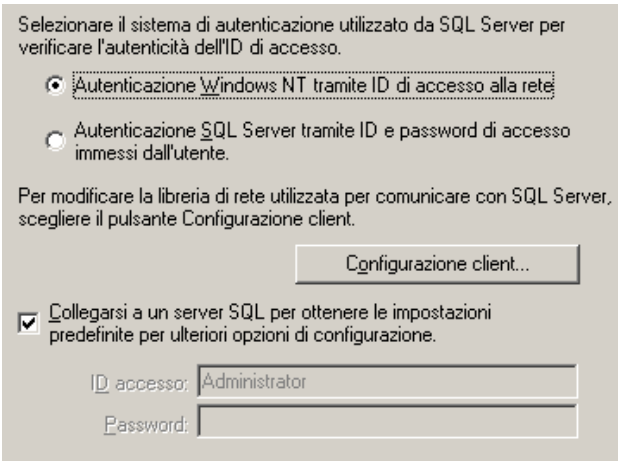
Per configurare un'origine dati ODBC per l'autenticazione di Windows:

1. In Windows passare a Pannello di controllo > Strumenti di amministrazione > Origine dati (ODBC).
2. Fare clic sulla scheda DSN di sistema e scegliere Aggiungi.
3. Selezionare SQL Server. Fare clic su Fine.
4. Viene visualizzata una finestra per l'immissione dei dati di configurazione dei driver:
   - Come nome dell'origine dati, specificare esecuritydb.
   - Nel campo facoltativo Descrizione fornire una descrizione.
   - Nel campo Server indicare il nome host o l'indirizzo IP del server Sentinel.



5 Fare clic su Avanti.

Nella finestra successiva selezionare l'autenticazione Windows.



Nota: l'ID di login (non attivo) corrisponde al nome di login di Windows.

---

6 Nella finestra successiva selezionare:

- Modificare il database di Sentinel (il nome di default è ESEC)
- Lasciare tutte le impostazioni di default

Fare clic su Avanti.

7 Fare clic su Fine.

8 Fare clic su Verifica origine dati. Viene creata una connessione. Fare clic su OK fino al completamento della procedura.

8.7.2 Installazione di Crystal Reports Server per Microsoft SQL Server con autenticazione SQL

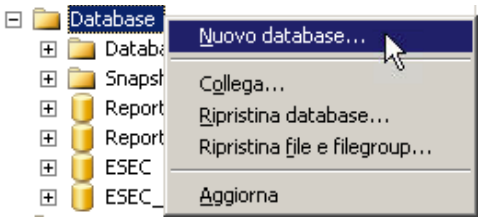
Per installare Crystal Reports Server con l'autenticazione SQL:

1 Installare Microsoft SQL Server 2005.

2 Avviare Microsoft SQL Server Management Studio.

3 Nel riquadro di spostamento espandere Database.

Evidenziare Database, fare clic con il pulsante destro del mouse e scegliere Nuovo database per creare il database CMS di Crystal.



4 Nel campo Nome database, digitare BOE115 e fare clic su OK.

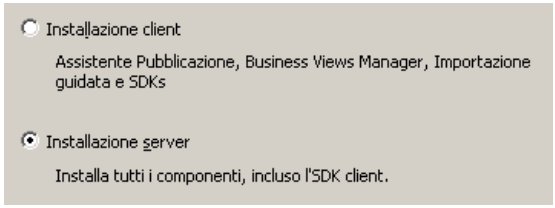
5 Chiudere Microsoft SQL Server Management Studio.

6 Inserire il CD di Crystal Reports Server XI R2 nell'unità CD-ROM.

7 Se sul computer in uso la funzione di riproduzione automatica è disabilitata, eseguire `setup.exe`.

8 Selezionare la lingua per l'installazione di Crystal Reports.

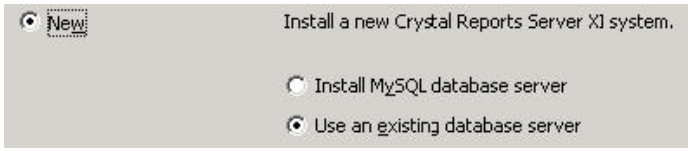
9 Nella finestra Select Client or Server Installation, scegliere Perform Server Installation.



10 Immettere il codice di licenza di Crystal (fornito dal Customer Center di Novell (https://secure-www.novell.com/center/regadmin)).

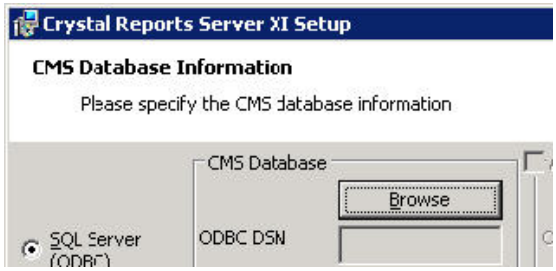
11 Specificare una cartella di destinazione.

12 Per il tipo di installazione, selezionare Use an existing database server.



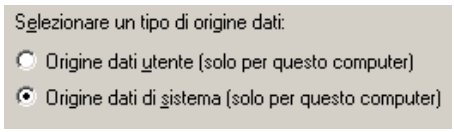
Nota: Crystal Reports Server e Microsoft SQL Server devono trovarsi nello stesso computer.

13 Nel riquadro CMS Database fare clic su Browse.



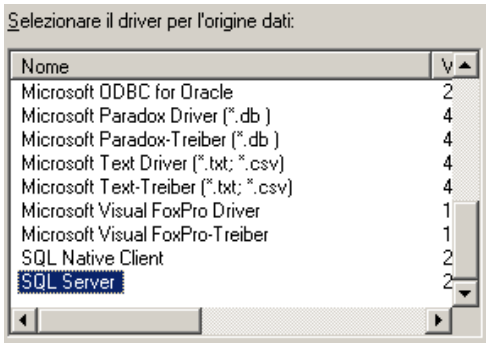
14 Fare clic sulla scheda Machine Data Source quindi scegliere New.

Selezionare System Data Source.

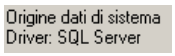


Fare clic su Next.

Scorrere l'elenco, selezionare SQL, quindi fare clic su Next.



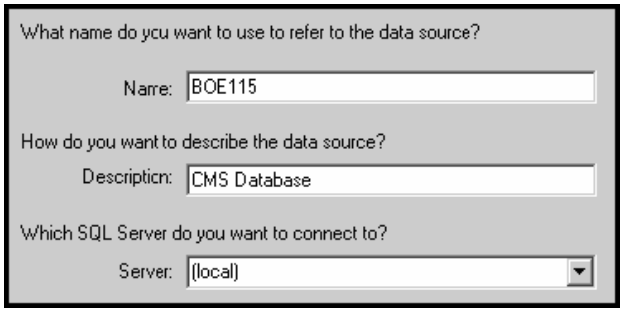
Quando viene visualizzata una nuova origine, fare clic su Finish.



15 Fare clic con il pulsante destro del mouse su Database quindi scegliere Create New Database (BOE115).

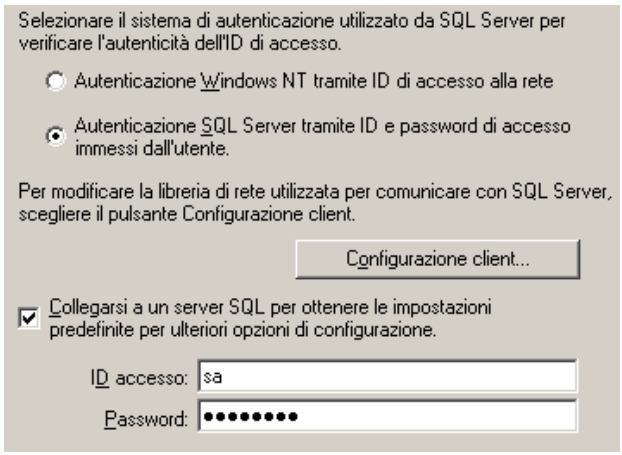
16 Nella finestra New Data Source to SQL Server specificare:

- Il nome dell'origine dati in uso, ad esempio BOE115.
- la descrizione (facoltativo).
- per il server, fare clic sulla freccia giù, quindi selezionare (local)



Fare clic su Next.

17 Selezionare With SQL Server authentication, specificare sa come login e la relativa password. Fare clic su Avanti.

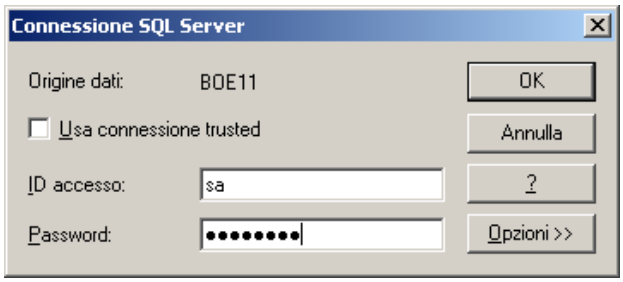


Selezionare la casella di controllo Change the default database to. Modificare il database di default impostandolo su BOE115. Fare clic su Next.

18 Nella finestra Create a New Data Source to SQL Server fare clic su Finish.

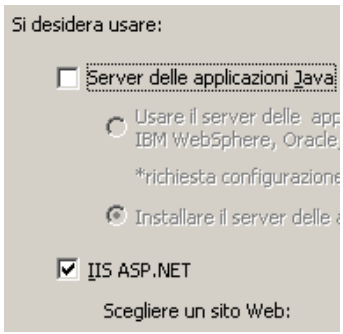
19 Fare clic su Verifica origine dati. Fare clic su OK.

Nella finestra Select Data Source evidenziare BOE115 e continuare a fare clic su OK finché non viene visualizzata la schermata Connessione SQL Server. Assicurarsi che la casella di controllo Usa connessione trusted NON sia selezionata. Fare clic su OK. Fare clic su Avanti.



20 Nella finestra Web Component Adapter Type selezionare IIS ASP.NET.

Nota: se non si è installato IIS e ASP.NET mediante Pannello di controllo > Installazione applicazioni > Installazione componenti di Windows, IIS ASP.NET non sarà attivo.

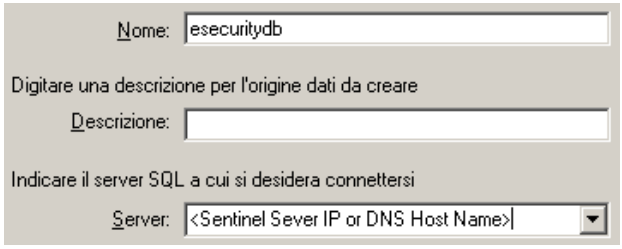


Configurazione di ODBC (Open Database Connectivity) per l'autenticazione di SQL

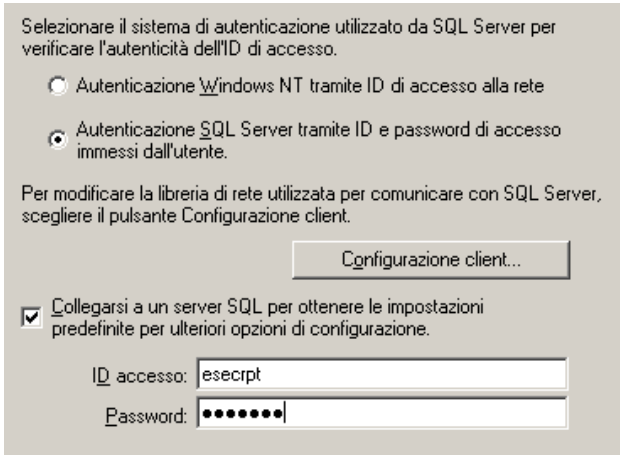
Con questa procedura è possibile configurare il nome dell'origine dati ODBC in modo da consentire la connessione di Crystal Reports Server al database di Sentinel in Windows e SQL Server mediante l'autenticazione di SQL. Questi passaggi devono essere eseguiti nel computer di Crystal Reports Server.

Per configurare un'origine dati ODBC per Windows:

1. In Windows passare a Pannello di controllo > Strumenti di amministrazione > Origine dati (ODBC).
2. Fare clic sulla scheda DSN di sistema e scegliere Aggiungi.
3. Selezionare SQL Server. Fare clic su Fine.
4. Viene visualizzata una finestra per l'immissione dei dati di configurazione dei driver:
   - Come nome dell'origine dati, specificare esecuritydb.
   - Nel campo facoltativo Descrizione fornire una descrizione.
   - Nel campo Server indicare il nome host o l'indirizzo IP del server Sentinel



   Fare clic su Avanti.
5. Nella finestra successiva selezionare l'autenticazione SQL. Immettere esecrpt nei campi ID accesso e Password. Fare clic su Avanti.



6. Nella finestra successiva selezionare:
   - Modificare il database di Sentinel (il nome di default è ESEC)
   - Lasciare tutte le impostazioni di default

Fare clic su Avanti, quindi su Fine.

7 Fare clic su Verifica origine dati. Al termine della verifica, fare clic su OK. Fare clic su OK fino al completamento della procedura.

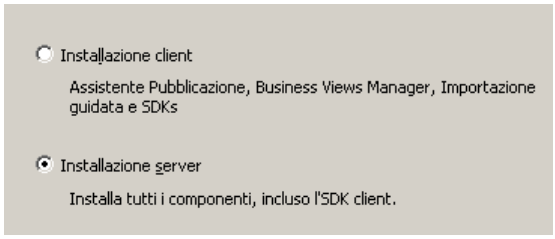
8.7.3 Installazione di Crystal Reports Server per Oracle

Per installare Crystal Reports Server XI R2 per Oracle:

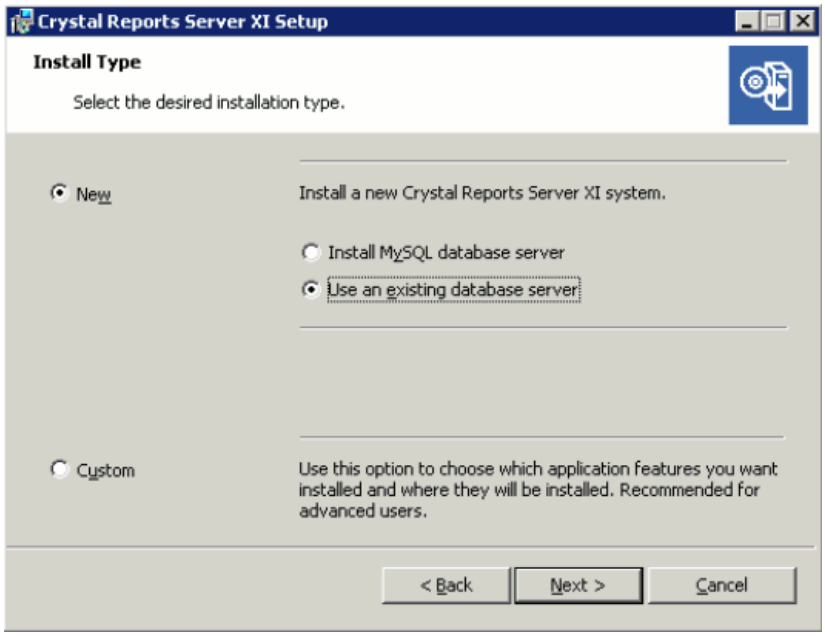
1 Inserire il CD di Crystal Reports Server XI R2 nell'unità CD-ROM.

2 Selezionare la lingua di configurazione dei rapporti di Crystal Reports.

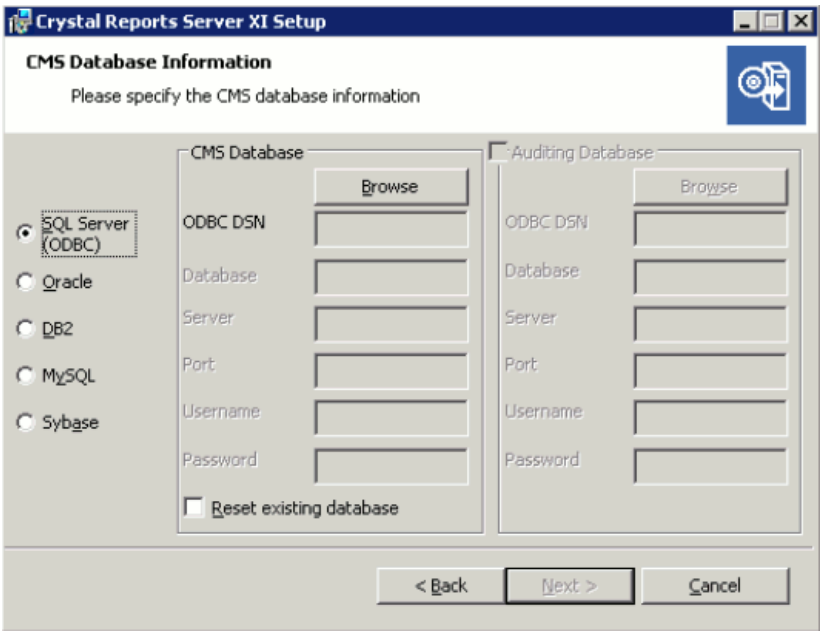
3 Nella finestra Select Client or Server Installation, scegliere Perform Server Installation.



4 Selezionare Use an existing database server.



Viene visualizzata la finestra CMS Database Information:



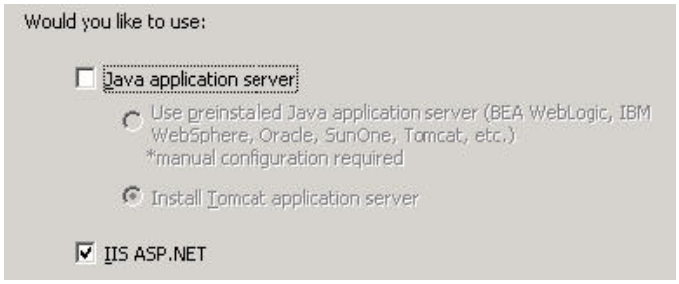
Selezionare il tipo SQL Server (ODBC) e fare clic su Browse per selezionare un DSN. Dopo aver selezionato un DSN, viene richiesto il nome utente e la password. Fornire le informazioni richieste e fare clic su Next.

Nota: Crystal Reports Server e Microsoft SQL Server 2005 devono trovarsi nello stesso computer.

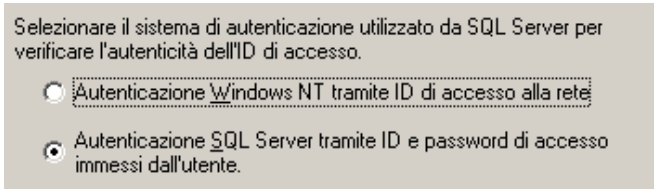
---

5 Selezionare IIS ASP.NET.

Nota: se non si è installato IIS e ASP.NET mediante Pannello di controllo > Installazione applicazioni > Installazione componenti di Windows, IIS ASP.NET non sarà attivo. L'installazione di IIS and ASP.NET è necessaria per poter eseguire la presente installazione.



6 Verrà richiesto di specificare la modalità di autenticazione. Selezionare l'autenticazione di SQL Server.



Crystal Reports Server supporta l'accesso diretto a un database di Sentinel in Oracle grazie al file di conversione crdb_oracle.dll. Questo file comunica con il driver del database Oracle , il quale interagisce direttamente con i client e i database Oracle recuperando i dati necessari per il rapporto.

Nota: per consentire a Crystal Reports Server di utilizzare i database Oracle, è necessario che nel sistema sia installato il software client Oracle e che l'ubicazione del client Oracle sia indicata nella variabile di ambiente PATH.

Installazione e configurazione del software Oracle Client

Quando si installa il client Oracle:

- Accettare l'ubicazione di installazione di default.
- Non selezionare Perform Typical Configuration
- Non selezionare Directory Service
- Selezionare Local
- TNS Service Name: ESEC
- User (facoltativo): esecrpt

Al termine dell'installazione, creare una configurazione locale dei nomi dei servizi di rete.

La seguente procedura è relativa al driver nativo di Oracle 9, ma dovrebbe essere valida anche per Oracle 10.

Per creare la configurazione dei nomi dei servizi di rete (configurazione del driver nativo di Oracle 9):

1. Selezionare Oracle-OraHome92 > Configuration and Migration Tools > Net Manager.
2. Nel riquadro di navigazione espandere Local ed evidenziare Service Naming.
3. Fare clic sul segno più a sinistra per aggiungere un nome di servizio.
4. Nella finestra Service Name specificare il nome del servizio di rete.
   - Immettere ESECURITYDB.

   Fare clic su Avanti.
5. Nella finestra Select Protocols selezionare il protocollo di defaul:
   - TCP/IP (protocollo Internet)

   Fare clic su Avanti.
6. Per il nome host e il numero di porta:
   - Immettere il nome host o l'indirizzo IP del computer in cui si trova il database di Sentinel.
   - Selezionare la porta Oracle (di default 1521 durante l'installazione)

   Fare clic su Avanti.
7. Per identificare il database o il servizio di Sentinel:
   - Selezionare (Oracle8i o versioni successive), quindi specificare il nome del servizio (nome dell'istanza Oracle).
   - Per il tipo di connessione selezionare Database Default.

   Fare clic su Avanti.

8 Nella finestra Test fare clic su Test. Fare clic su Avanti. Il test potrebbe non riuscire perché utilizza un ID DB e una password.

9 Se il test non riesce, eseguire le operazioni seguenti:

- Nella finestra Connection Test fare clic su Change Login.
- Immettere l'ID di Oracle Sentinel, ovvero esecrpt, e la password. Fare clic su Test.

Se il test non riesce:

- Eseguire il ping del Sentinel.
- Verificare che il nome host del server Sentinel sia incluso nel file degli host di Crystal Reports Server. Il file degli host si trova in %SystemRoot%\system32\drivers\etc\.

10 Fare clic su Close, quindi su Finish.

8.8 Configurazione per tutte le autenticazioni e configurazioni

Per consentire l'interazione tra Crystal Reports Server e Sentinel Control Center, è necessario eseguire le procedure seguenti.

8.8.1 Configurazione di inetmgr

Per configurare inetmgr:

1 Copiare il file `web.config` da:

`C:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content`

in c:\Inetpub\wwwroot.

2 Avviare Gestione servizio Intenrnet facendo clic su Start > Esegui. Immettere inetmgr e fare clic su OK.

3 Espandere (computer locale) > Siti Web > Sito Web predefinito > businessobjects.

4 In businessobjects fare clic con il pulsante destro del mouse quindi scegliere Proprietà.

5 Nella scheda Virtual Directory fare clic su Configuration.

6 Vengono visualizzate le mappature seguenti. In caso contrario, aggiungerle. Se si desidera aggiungere una mappatura, non fare clic sui nodi 'businessobjects' o 'crystalreportsviewer11'.

Estensione	Eseguibile
.csp	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cwr	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cri	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.wis	...\BusinessObjects Enterprise 11.5

Fare clic su OK per chiudere la finestra.

7 Riavviare IIS. A questo scopo, espandere (computer locale) > Siti Web > Sito Web predefinito, evidenziare Sito Web predefinito e fare clic con il pulsante destro del mouse, quindi scegliere Arresta.

8 Espandere (computer locale) > Siti Web > Sito Web predefinito, evidenziare Sito Web predefinito e fare clic con il pulsante destro del mouse, quindi scegliere Start.

8.9 Pubblicazione di modelli di Crystal Reports

Molti modelli di rapporti sono creati da Novell per l'uso nelle schede Analisi e Advisor di Sentinel Control Center. È possibile scaricare i rapporti più recenti dalle pagine Web di Sentinel 6 al seguente indirizzo URL:

http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html)

Il set principale dei rapporti di Sentinel viene distribuito nel Sentinel Core Solution Pack.

Sono disponibili quattro modi per aggiungere i rapporti al sistema:

- Mediante il download di un pacchetto di soluzioni dall'apposita scheda e l'utilizzo di Solution Manager per installare uno o più controlli che includono rapporti
- Mediante il download di un pacchetto di raccolta dall'apposita scheda e l'utilizzo di Solution Manager per installare uno o più controlli che includono rapporti
- Mediante l'aggiunta di uno o più modelli di rapporti (file RPT) utilizzando la pubblicazione guidata Crystal
- Mediante l'aggiunta di uno o più modelli di rapporti (file RPT) utilizzando la console di gestione centrale di Crystal Reports.

Importante: Per eseguire uno qualsiasi dei primi 10 rapporti, è necessario che l'aggregazione sia abilitata e che Event in `DAS_Binary.xml` sia impostato come attivo. Questa configurazione è già impostata nel l'installazione di default di Sentinel. Per informazioni su come abilitare l'aggregazione, consultare la sezione “Report Data Configuration” di “Admin” nella *Sentinel User Guide*.

8.9.1 Pubblicazione di modelli di rapporti con Solution Manager

Se il server Web e il server Crystal Reports sono stati configurati in modo corretto·seguendo le istruzioni di installazione riportate in questo capitolo, è possibile pubblicare i rapporti inclusi in un pacchetto soluzioni o raccolta direttamente nel server Crystal Reports mediante Solution Manager. Per ulteriori informazioni, vedere “Solution Packs” nella *Sentinel User Guide*.

8.9.2 Pubblicazione di modelli di rapporti - Pubblicazione guidata di Crystal

I rapporti di Sentinel vengono ora distribuiti utilizzando i pacchetti di soluzione, ma questo metodo può essere utilizzato per pubblicare modelli di rapporti di altre origini.

Per pubblicare i modelli di rapporti di Crystal Reports:

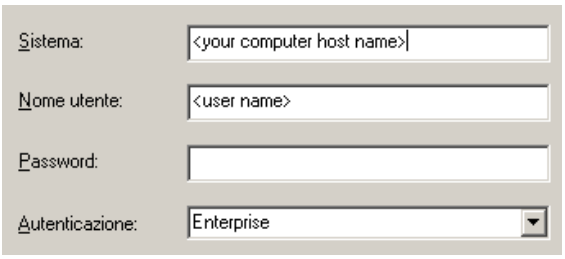
Nota: se si desidera pubblicare di nuovo i modelli di rapporti, eliminare quelli importati in precedenza.

1. Fare clic su Start > Programmi > BusinessObjects > Crystal Reports Server > Pubblici Miliardi.

   Fare clic su Avanti.

2. Login. In System è necessario specificare il nome host del computer in cui è installato Crystal, mentre in Authentication è necessario immettere Enterprise. In User Name è possibile immettere Administrator. Per motivi di sicurezza, si raccomanda di creare un nuovo nome utente anziché utilizzare Administrator. Immettere la password, quindi fare clic su Next.

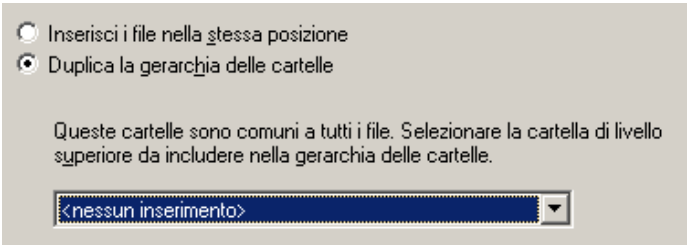
   Nota: La pubblicazione di rapporti da parte dell'utente Administrator (Amministratore) consente a tutti gli utenti di accedere ai rapporti.



3. Fare clic su Aggiungi cartella. [Facoltativo] Selezionare Include Subfolders (Includi sottocartelle).
4. Passare all'ubicazione del modello di rapporto. Fare clic su OK. Fare clic su Avanti.
5. Nella finestra Specify Location (Specifica ubicazione), fare clic su New Folder (Nuova cartella) nell'angolo in alto a destra, quindi creare una cartella chiamata SentinelReports (se non esiste già). Fare clic su Avanti.

6. Seleziona:
   - Il pulsante di scelta 'Duplicate the folder hierarchy' (Duplica gerarchia cartelle).

     Fare clic sulla freccia giù e selezionare <include none>.



Fare clic su Avanti.

7 Nella finestra Confirm Location (Conferma percorso) fare clic su Next (Avanti).

8 Nella finestra Specify Categories (Specifica categorie), immettere un nome di categoria (ad esempio sentinel), evidenziare il nome, quindi fare clic sul pulsante +.

Nota: Dopo aver fatto clic su Next sotto la categoria verrà visualizzato solo il primo rapporto.

Fare clic su Avanti.

9 Nella finestra Specify Schedule (Specifica pianificazione), fare clic sul pulsante di scelta 'Let users update the object' (Oggetto aggiornato dagli utenti) (dovrebbe essere l'impostazione di default). Fare clic su Avanti.

10 Nella finestra Specify Repository Refresh (Specifica aggiornamento archivio), fare clic su Enable All (Attiva tutti) per abilitare l'aggiornamento degli archivi. Fare clic su Avanti.

11 Nella finestra Specify Keep Saved Data (Specifica mantieni dati salvati), fare clic su Enable All (Attiva tutti) per conservare i dati salvati durante la pubblicazione dei rapporti. Fare clic su Avanti.

12 Nella finestra Change Defaults Values (Modifica valori predefiniti), fare clic sul pulsante di scelta 'Publish reports without modifying properties' (Pubblica rapporti senza modificare le proprietà) (dovrebbe essere l'opzione di default). Fare clic su Avanti.

13 Fare clic su Next (Avanti) per aggiungere gli oggetti.

14 Quando viene visualizzato l'elenco delle pubblicazioni, fare clic su Finish.

Una volta pubblicati i modelli Sentinel per Crystal Reports in Crystal Reports Server, è necessario che siano ubicati all'interno della directory SentinelReports per poter essere visualizzati in Sentinel Control Center.

8.9.3 Pubblicazione di modelli di rapporti – Central Management Console (Console di gestione centrale)

I rapporti di Sentinel vengono ora distribuiti utilizzando i pacchetti di soluzione, ma questo metodo può essere utilizzato per pubblicare i modelli di rapporti di altre origini.

Per importare i modelli di rapporti di Crystal Reports:

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

```
http://<hostname_or_IP_of_web_server>/businessobjects/
enterprise115/WebTools/adminlaunch
```

2 Fare clic su Central Management Console

3 Eseguire il login al server Crystal Reports.

4 Nel riquadro Organize (Organizza) fare clic su Folders (Cartelle).

5 Nell'angolo superiore destro fare clic su New Folder.

6 Creare una cartella denominata SentinelReports, se non esiste già. Fare clic su OK.

Nota: È necessario assegnare alla cartella esattamente il nome SentinelReports.

7 Fare clic su SentinelReports.

8 Fare clic sulla scheda Subfolders (Sottocartelle) e creare delle sottocartelle, se necessario. Se si aggiungono i rapporti principali di Sentinel manualmente, creare le seguenti sottocartelle:

- Advisor_Vulnerability
- rinnovi/previsioni
- Incident Management
- Eventi interni
- Security Events
- Top 10

9 Fare clic su Home > Objects > New Object.

10 Sul lato sinistro della pagina evidenziare Report.

11 Fare clic su Sfoglia e individuare l'ubicazione dei modelli di rapporti da aggiungere. Fare clic su una cartella e selezionare un rapporto.

12 Evidenziare SentinelReports, quindi fare clic su Show Subfolders (Mostra sottocartelle).

13 Selezionare la cartella appropriata per il rapporto e fare clic su 'Show Subfolders' (Mostra sottocartelle).

14 Fare clic su Invia.

15 Per aggiungere gli altri rapporti, ripetere i passaggi da 9 a 17 fino a quando sono stati aggiunti tutti i rapporti.

8.9.4 Impostazione di un conto utente denominato

Il codice di licenza fornito con Crystal Reports Server è un codice di conto Named User. Il conto Guest deve essere modificato da Concurrent User a Named User.

Per impostare il conto Guest come Named User:

1 Fare clic su Start > Programmi > BusinessObjects > Crystal Reports Server > .NET Administration Launchpad.

2 Fare clic su Central Management Console.

3 Il nome del sistema dovrebbe essere il nome del computer host. Il tipo di autenticazione dovrebbe essere Enterprise. In caso contrario, selezionare Enterprise.

4 Specificare Administrator come User Name. Immettere la password (vuota per default). Fare clic su Log On. Nel riquadro Organize fare clic su Users.

5 Fare clic su Guest (Ospite).

6 Modificare il tipo di connessione da Concurrent User a Named User.

Importante: Per poter generare un numero di rapporti illimitato, è necessario utilizzare il conto di licenza Named User.

7 Fare clic su Aggiorna.

8 Eseguire il logoff o chiudere la finestra oppure passare alla sezione Configuring .NET Administration Launchpad.

8.9.5 Configurazione delle autorizzazioni per i rapporti

Questa procedura indica come utilizzare .NET Administration Launchpad per configurare le autorizzazioni per i rapporti per consentirne la visualizzazione e la modifica su richiesta.

Per configurare le autorizzazioni per i rapporti:

1 Avviare .NET Administration Launchpad facendo clic su Start > Programmi > BusinessObjects > Crystal Reports Server > .NET Administration Launchpad.

Nota: se all'avvio di .NET Administration Launchpad viene visualizzato l'errore "HTTP 404 - File or Directory not found", vedere http://support.microsoft.com/kb/315122 (http://support.microsoft.com/kb/315122) per la risoluzione del problema.

---

2 Fare clic su Central Management Console.

Il nome del sistema dovrebbe essere il nome del computer host. Il tipo di autenticazione dovrebbe essere Enterprise. In caso contrario, selezionare Enterprise.

3 Specificare Administrator come User Name. Immettere la password (vuota per default). Fare clic su Log On. Nel riquadro Organize fare clic su Folders.

4 Fare clic su SentinelReports.

5 Seleziona tutti.

6 Fare clic sulla scheda Rights (Diritti).

7 Per Everyone, selezionare View on Demand dal menu a discesa a destra nella sezione Access Level.

8 Fare clic su Aggiorna.

9 Eseguire il logoff e chiudere la finestra.

Test della connessione del server Web al database di Sentinel

Per eseguire il test della connessione del server Web al database:

1 Avviare .NET Administration Launchpad facendo clic su Start > Programmi > BusinessObjects > Crystal Reports Server > .NET Administration Launchpad.

2 Fare clic su Central Management Console.

3 Specificare Administrator come User Name. Immettere la password (vuota per default). Fare clic su Log On (Esegui login).

4 Scegliere Folders > SentinelReports > Internal Events.

5 Selezionare Column Display Details.

6 Fare clic su Preview.

7 In base al sistema in uso eseguire il login come esecrpt o come utente di Sentinel Reports.

8 Nel menu a discesa del campo di ordinamento selezionare Tag.

9 Fare clic su OK. Viene visualizzato un rapporto.

Test della connettività al server Web

Per eseguire il test della connettività al server Web:

1. Passare a un computer diverso ma che sia nella stessa rete del server Web.
2. Specificare
   `http://<DNS name or IP address of your web server>/businessobjects/enterprise115/WebTools/adminlaunch/default.aspx`

Dovrebbe essere visualizzata una pagina Web di Crystal BusinessObjects.

8.9.6 Disabilitazione dei primi 10 rapporti di Sentinel

Per default in Sentinel sono abilitati i primi 10 rapporti. Se non si prevede di utilizzare questi rapporti, è possibile ridurre l'utilizzo di CPU e di spazio di archiviazione del database disabilitando i primi 10 rapporti di Sentinel:

- Disattivare l'aggregazione.
- Disabilitare EventFileRedirectService.

Per disattivare l'aggregazione:

1. Avviare Sentinel Control Center.
2. Login.
3. Fare clic sulla scheda Admin e aprire l'opzione Rapporto dati.
4. Disabilitare i riepiloghi seguenti:
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   Fare clic su ciascun pulsante Attivo nella colonna Stato finché diventa Inattivo.

Nome riepilogo	Ora	Attributi		Origine	Stato
EventDestSum...	1 ora	CUST_ID.RS	...	TransformedEv...	Attivo
EventSevDestT...	1 ora	CUST_ID.DE	...	TransformedEv...	Inattivo
EventSevDestE...	1 ora	CUST_ID.DE	...	TransformedEv...	Inattivo
EventSevDestP...	1 ora	SEV.DEST_F	...	TransformedEv...	Inattivo
EventSevSumm...	1 ora	CUST_ID.SE	...	TransformedEv...	Attivo
EventSrcSumm...	1 ora	CUST_ID.RS	...	TransformedEv...	Attivo

Per disabilitare EventFileRedirectService:

1. Nel computer DAS, mediante l'editor di testo, aprire:

   Per UNIX:

   `$ESEC_HOME/config/das_binary.xml`

   In Windows:

   `%ESEC_HOME%\config\das_binary.xml`
2. Per EventFileRedirectService cambiare lo stato in off.

```
<property name="status">off</property>
```

3 Riavviare il componente DAS eseguendo le operazioni seguenti:

In Windows:

```
Use Service Manager to stop and then start the "sentinel" service
```

8.9.7 Configurazione di Sentinel Control Center per l'integrazione con Crystal Reports Server

Sentinel Control Center può essere configurato per l'integrazione con Crystal Reports Server per consentire la visualizzazione dei rapporti di Crystal Reports da Sentinel Control Center.

Per abilitare l'integrazione di Sentinel Control Center con Crystal Reports Server, attenersi alle seguenti istruzioni.

Nota: è possibile eseguire questa configurazione solo dopo aver installato Crystal Reports Server e aver pubblicato sul server i rapporti di Crystal Reports.

Per configurare Sentinel per l'integrazione con Crystal Reports Server:

1 Eseguire il login a Sentinel Control Center come utente con privilegi per la scheda Amministratore.

2 Nella scheda Amministratore, selezionare Crystal Report Configuration (Configurazione Crystal Report).

3 Nel campo URL analisi specificare quanto segue:

```
http://<hostname_or_IP_of_web_server>/
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

Nota: <hostname_or_IP_of_web_server> deve essere sostituito con l'indirizzo IP o il nome host del server Crystal Reports.

Nota: Questo URL non funzionerà correttamente se APS (Automated Process Scheduler) è impostato sull'indirizzo IP. È necessario immettere il nome del server Crystal Reports.

---

4 Fare clic sul pulsante Aggiorna accanto al campo URL analisi.

5 Se è installato Advisor, nel campo URL Advisor specificare:

```
http://<hostname_or_IP_of_web_server>/
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

Nota: <hostname_or_IP_of_web_server> deve essere sostituito con l'indirizzo IP o il nome host del server Crystal Reports.

Nota: Questo URL non funzionerà correttamente se APS è impostato sull'indirizzo IP. È necessario immettere il nome del server Crystal Reports.

---

6 Fare clic sul pulsante Aggiorna accanto al campo URL di Advisor.

7 Fare clic su Salva.

8 Eseguire il logout e quindi il login in Sentinel Control Center. Gli alberi di Crystal Reports nelle schede Analisi e Advisor (se Advisor è installato) ora dovrebbero essere visualizzati nella barra di spostamento.

8.10 Configurazioni a prestazioni elevate per Crystal

8.10.1 Aumento del limite di record di aggiornamento dei rapporti di Crystal Reports Server

A seconda del numero di eventi su cui viene eseguita l'interrogazione in Crystal, è possibile che venga visualizzato un errore relativo al tempo massimo di elaborazione o al limite massimo di record. Per impostare il server per l'elaborazione di un numero superiore o illimitato di record sarà necessario riconfigurare Crystal Page Server. Questa operazione può essere eseguita utilizzando Central Configuration Manager o la pagina Web di Crystal.

Per riconfigurare Crystal Page Server tramite Central Configuration Manager:

1. Fare clic su Start > Tutti i programmi > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.
2. Fare clic con il pulsante destro del mouse su Crystal Reports Page Server quindi scegliere Stop.
3. Fare clic con il pulsante destro del mouse su Crystal Reports Page Server quindi scegliere Properties.
4. Nel campo Comando della scheda Proprietà, alla fine della riga di comando aggiungere:

   ```
   maxDBResultRecords <value greater than 20000 or 0 to disable the default limit>
   ```
5. Riavviare Crystal Page Server.

Per riconfigurare Crystal Page Server mediante la console di gestione centrale:

1. Fare clic su Start > Tutti i programmi > BusinessObjects 11 > Crystal Reports Server > .Net Administration Launchpad. In alternativa, avviare un browser Web e immettere il seguente URL:

   http://<nome DNS o indirizzo IP del server Web>/businessobjects/enterprise11/WebTools/adminlaunch/default.aspx
2. Fare clic su Central Management Console.
3. Il nome del sistema dovrebbe essere il nome del computer host. Il tipo di autenticazione dovrebbe essere Enterprise. In caso contrario, selezionare Enterprise.
4. Immettere nome utente e password e fare clic su Log On. Fare clic su Server.
5. Fare clic su <nome server>.pageserver.
6. In Database Records to Read When Previewing Or Refreshing a report (Record del database da leggere durante la visualizzazione in anteprima o l'aggiornamento di un report), selezionare Unlimited records (Senza limite di record). Fare clic su Applica.
7. Verrà visualizzato un prompt per il riavvio del page server. Fare clic su OK.

È possibile che vengano richiesti un nome di login e una password per accedere al manager dei servizi del sistema operativo.

8.10.2 Creazione di rapporti con il servizio Aggregazione

Per migliorare le prestazioni, i primi 10 rapporti inclusi in Sentinel Core Solution Pack eseguono le interrogazioni sulle tabelle di riepilogo anziché sulla tabella eventi. Le tabelle di riepilogo contengono i conteggi in un intervallo di tempo delle combinazioni di campi nei dati dell'evento. Ciò fornisce un dataset molto più ridotto per alcuni tipi di interrogazione rendendo molto più rapide le interrogazioni e l'esecuzione dei rapporti.

Il servizio Aggregazione è responsabile dell'inserimento nelle tabelle di riepilogo dei riepiloghi di tutti gli eventi presenti nella tabella eventi. Il servizio Aggregazione genererà dati di riepilogo solo per i riepiloghi attivi. Per i primi 10 rapporti sono necessari i seguenti riepiloghi che sono abilitati per default:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

I riepiloghi possono essere attivati o disattivati mediante la finestra Configurazione dati rapporti nella scheda Amministratore di Sentinel Control Center.

Il servizio Aggregazione dipende inoltre dal componente `EventFileRedirectService` del file binario DAS per il feed dei dati di evento che verranno riepilogati. Di conseguenza, per il funzionamento corretto del servizio Aggregazione è necessario abilitare questo componente. Il componente viene abilitato o disabilitato modificando l'attributo "status" del componente `EventFileRedirectService` nel file `das_binary.xml` su "on" o "off". Per default questo componente è impostato su "on".

Nota: Per informazioni su EventFileRedirectService e i tre riepiloghi di aggregazione, vedere “Report Data Configuration” in Admin della *Sentinel User Guide*.

Nota: I rapporti con interrogazioni su un intervallo di date esteso possono richiedere tempi lunghi di esecuzione. È possibile pianificarli anziché eseguirli interattivamente. Per informazioni sulla pianificazione dei rapporti di Crystal Reports, consultare la documentazione di Crystal BusinessObjects Enterprise™ 11 (http://support.businessobjects.com/documentation/product_guides/default.asp).

8.10.3 Sviluppo di rapporti

Per creare o modificare i rapporti di Crystal Reports è possibile utilizzare Crystal Reports Developer. Per sviluppare rapporti personalizzati, si consiglia quanto segue:

- Se i rapporti possono utilizzare tabelle aggregate predefinite, selezionare la tabella aggregata che comporta l'elaborazione della minore quantità di dati.
- Provare a inserire quasi tutti i dati da elaborare nel motore del database.
- Per diminuire il sovraccarico dei processi di elaborazione in Crystal Server, ridurre al minimo la quantità di dati da recuperare sul server di Crystal.
- Scrivere sempre i rapporti utilizzando le viste di database fornite da Novell anziché le tabelle di base.

Crystal Reports per Linux

9

Crystal Reports Server™ (di Business Objects) è lo strumento per la generazione di rapporti utilizzato in Sentinel. In questa sezione viene illustrata l'installazione e la configurazione di Crystal Reports Server per Sentinel. Per ulteriori informazioni sulle piattaforme supportate per Crystal Reports Server in un ambiente Sentinel, consultare il Capitolo 2, “Requisiti di sistema”, a pagina 21.

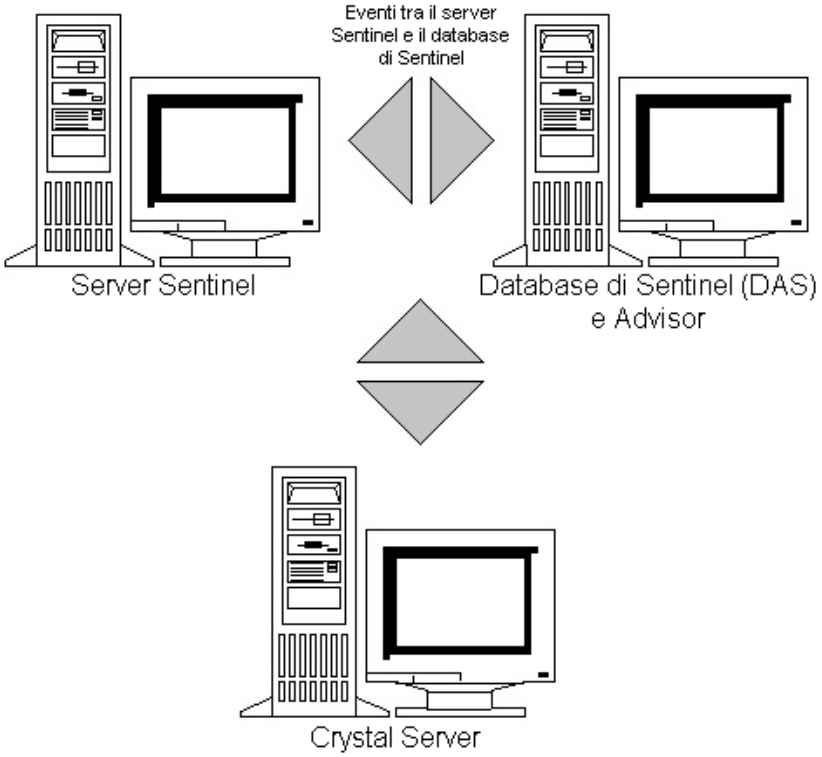
In Linux Sentinel è stato testato con Crystal Reports Server XI R2 SP2. Per ulteriori informazioni su Crystal Reports Server XI Release 2 Service Packs o per eseguire il download dei service pack, visitare la pagina Web all'indirizzo https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads) ed eseguire la ricerca della versione e della piattaforma corrette.

In questa sezione viene illustrata l'esecuzione di Crystal Reports Server in Linux. Per ulteriori informazioni su Crystal Reports Server in Windows, consultare il Capitolo 8, “Crystal Reports per Windows”, a pagina 97.

Importante: È necessario eseguire l'installazione nell'ordine indicato di seguito.

Per installare Crystal Reports Server:

1. Preinstallare e installare Crystal Reports Server™ XI R2.
2. Eseguire le patch di Crystal Reports Server.
3. Pubblicare (importare) i rapporti di Crystal Reports.
4. Impostare un conto "Named User".
5. Eseguire il test della connettività al server Web.
6. Abilitazione dei primi 10 rapporti (facoltativo)
7. Aumentare il limite di record di aggiornamento dei rapporti di Crystal Reports Server (consigliato).
8. Configurare Sentinel Control Center per l'integrazione con Crystal Reports Server.



9.1 Panoramica

Il server Crystal Report richiede un database in cui memorizzare le informazioni sul sistema e i relativi utenti. Questo database è chiamato CMS (Server di gestione centrale, Central Management Server) e corrisponde a un server in cui vengono memorizzate le informazioni sul sistema Crystal Reports Server. Gli altri componenti di Crystal Reports Server possono accedere a queste informazioni.

9.2 Documentazione sull'installazione

9.2.1 Preinstallazione di Crystal Reports Server™ XI R2

Per preinstallare Crystal Reports Server:

1. Se il database di Sentinel non si trova nello stesso computer di Crystal Reports Server, sarà necessario installare il software Oracle Client nel computer di Crystal Reports Server. Questa operazione aggiuntiva non è necessaria se il database di Sentinel si trova nello stesso computer di Crystal Reports Server perché in questo caso il software Oracle necessario è già stato installato durante l'installazione del database di Oracle.
2. Eseguire il login al computer di Crystal Reports Server come utente root.
3. Creare il gruppo bobje

   ```
   groupadd bobje
   ```

4. Creare l'utente di Crystal (la home directory in questo esempio è /export/home/crystal, modificarla se necessario; la parte del percorso /export/home deve essere già esistente).

   ```
   useradd –g bobje –s /bin/bash –d /export/home/crystal –m crystal
   ```

5. Creare la directory per il software Crystal:

   ```
   mkdir –p /opt/crystal_xir2
   ```

6. Modificare la proprietà della directory del software Crystal (in modo ricorsivo) in crystal/bobje:

   ```
   chown -R crystal:bobje /opt/crystal_xir2
   ```

7. È necessario concedere le autorizzazioni all'utente di Crystal nella directory $ORACLE_HOME utilizzando un Elenco di controllo dell'accesso (ACL). Supponendo che l'utente di Crystal sia "crystal" e $ORACLE_HOME sia `/opt/oracle/product/10.2/db_1`, il comando da eseguire sarà:

   ```
   setfacl -m u:crystal:rx -R  /opt/oracle/product/10.2/db_1
   ```

   Per verificare la corretta impostazione dell'ACL, eseguire il comando seguente e verificare che l'output contenga "crystal":

   ```
   getfacl  /opt/oracle/product/10.2/db_1
   ```

8. Passare all'utente crystal:

   ```
   su - crystal
   ```

9. È necessario che nell'ambiente dell'utente crystal sia impostata la variabile di ambiente ORACLE_HOME. A tal fine, modificare lo script di login dell'utente crystal per impostare la variabile di ambiente ORACLE_HOME alla base del software Oracle. Se ad esempio la shell dell'utente crystal è bash e il software Oracle è installato nella directory `/opt/oracle/product/10.2/db_1`, aprire il file `~crystal/.bash_profile` (`.profile` in SLES) e aggiungere la riga seguente alla fine del file:

   ```
   export ORACLE_HOME=/opt/oracle/product/10.2/db_1
   ```

10. La variabile di ambiente LD_LIBRARY_PATH nell'ambiente dell'utente crystal deve contenere il percorso per le librerie software Oracle. A tal fine, modificare lo script di login dell'utente crystal per impostare la variabile di ambiente LD_LIBRARY_PATH perché includa le librerie del software Oracle. Se ad esempio la shell dell'utente crystal è bash, aprire il file `~crystal/.bash_profile` e aggiungere la riga seguente alla fine del file (sotto la riga in cui è impostata la variabile di ambiente ORACLE_HOME):

    ```
    export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
    ```

11. La variabile di ambiente PATH nell'ambiente dell'utente crystal deve contenere il percorso per i file eseguibili del software Oracle. A tal fine, modificare lo script dell'utente crystal per impostare la variabile di ambiente PATH perché includa i file eseguibili del software Oracle. Se ad esempio la shell dell'utente crystal è bash, aprire il file `~crystal/.bash_profile` e aggiungere la riga seguente alla file del file.

    ```
    export PATH=$PATH:$ORACLE_HOME/bin
    ```

12. È necessario aggiungere una voce al file Oracle `tnsnames.ora` con il nome del servizio esecuritydb che fa riferimento al database di Sentinel. A tal fine, nel computer di Crystal Reports Server eseguire le operazioni seguenti:

    12a Eseguire il login come utente Oracle.

    12b Passare alla directory $ORACLE_HOME/network/admin

    12c Eseguire il backup del file `tnsnames.ora`.

    12d Aprire il file `tnsnames.ora` per la modifica.

12e Se il database di Sentinel si trova nello stesso computer di Crystal Reports Server, sarà già presente una voce nel file `tnsnames.ora` per il database di Sentinel. Se ad esempio il database di Sentinel è denominato ESEC, esisterà una voce simile alla seguente:

```
ESEC =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

12f Se il database di Sentinel non si trova nello stesso computer di Crystal Reports Server, aprire il file `tnsnames.ora` nel computer del database di Sentinel per individuare la voce indicata sopra.

12g Fare una copia della voce e incollarla alla fine del file `tnsnames.ora` nel computer di Crystal Reports Server. La parte della voce relativa al nome del servizio deve essere rinominata in `esecuritydb`. Quando ad esempio questa voce viene copiata e rinominata in modo corretto sarà simile alla seguente:

```
esecuritydb =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

12h Verificare che la parte HOST della voce sia corretta (verificare cioè che non sia impostata su localhost se Crystal Reports Server e il database di Sentinel si trovano su computer diversi).

12i Salvare le modifiche apportate al file `tnsnames.ora`.

12j Eseguire il comando seguente per verificare che il nome del servizio `esecuritydb` sia configurato correttamente:

```
tnsping esecuritydb
```

12k Dopo l'esecuzione del comando, un messaggio indicherà che la connessione è stata stabilita.

9.2.2 Installazione di Crystal Reports Server XIR2

Il programma di installazione di Crystal Reports Server è costituito da due file `.iso`. Durante l'installazione verrà richiesto il percorso del secondo disco.

Per installare Crystal Reports Server:

1. Eseguire il login come utente crystal.
2. Passare alla directory disk1 del programma di installazione di Crystal.
3. Esecuzione:

   ```
   ./install.sh
   ```

4. Selezionare Language: English.
5. Selezionare New Installation.
6. Leggere e accettare il contratto di licenza.
7. Immettere il codice del prodotto.
8. Indicare la directory di installazione:
   `/opt/crystal_xir2`
9. Selezionare User install.
10. Selezionare New Install.
11. Selezionare Install MySQL se non si prevede di installare il database CMS di Crystal in un database esistente.
12. Specificare le informazioni di configurazione per MySQL:
    - **12a** Utilizzare la porta di default 3306
    - **12b** Admin password (Password amministratore)
13. Specificare ulteriori informazioni di configurazione per MySQL:
    - **13a** Default DB Name: BOE115
    - **13b** User ID: mysqladm
    - **13c** Password
14. Specificare ulteriori informazioni di configurazione per MySQL:
    - **14a** Local Name Server: <nome host computer locale>
    - **14b** Default CMS Port Number: 6400
15. Selezionare Install Tomcat.
16. Specificare le informazioni di configurazione di Tomcat:
    - **16a** Default Receive HTTP requests port: 8080
    - **16b** Default Redirect jsp requests port: 8443
    - **16c** Default Shutdown Hook port: 8005
17. Premere Invio per confermare la directory di default.
18. Premere Invio per avviare l'installazione.
19. Si noti il collegamento al server CMS che sarà simile al seguente:
    http://<nome host>:8080/businessobjects/enterprise115/adminlaunch/launchpad.html

9.3 Pubblicazione di modelli di Crystal Reports

Nota: prima di eseguire questa operazione si consiglia di leggere attentamente le note sulla versione di Sentinel Reports che potrebbero contenere file e script aggiornati o procedure aggiuntive.

Molti modelli di rapporti sono creati da Novell per l'uso nelle schede Analisi e Advisor di Sentinel Control Center. È possibile scaricare i rapporti più recenti dalle pagine Web di Sentinel 6 al seguente indirizzo URL:

http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html)

Il set principale dei rapporti di Sentinel viene distribuito nel Sentinel Core Solution Pack.

Sono disponibili quattro modi per aggiungere i rapporti·al sistema:

- Mediante il download di un pacchetto di soluzioni dall'apposita scheda e l'utilizzo di Solution Manager per installare uno o più controlli che includono rapporti
- Mediante il download di un pacchetto di raccolta dall'apposita scheda e l'utilizzo di Solution Manager per installare uno o più controlli che includono rapporti
- Mediante l'aggiunta di uno o più modelli di rapporti (file RPT) utilizzando la pubblicazione guidata Crystal
- Mediante l'aggiunta di uno o più modelli di rapporti (file RPT) utilizzando la console di gestione centrale di Crystal Reports.

Importante: Per eseguire uno qualsiasi dei primi 10 rapporti, è necessario che l'aggregazione sia abilitata e che EventFileRedirectService in `DAS_Binary.xml` sia impostato come attivo. Per informazioni su come abilitare l'aggregazione, consultare la sezione “Report Data Configuration” di “Admin” nella *Sentinel User Guide*.

9.3.1 Pubblicazione di modelli di rapporti con Solution Manager

Se il server Web e il server Crystal Reports sono stati configurati in modo corretto·seguendo le istruzioni di installazione riportate in questo capitolo, è possibile pubblicare i rapporti inclusi in un pacchetto soluzioni o raccolta direttamente nel server Crystal Reports mediante Solution Manager. Per ulteriori informazioni, vedere “Solution Packs” nella *Sentinel User Guide*.

9.3.2 Pubblicazione di modelli di rapporti - Crystal Publishing Wizard (Pubblicazione guidata Crystal)

I rapporti di Sentinel vengono ora distribuiti utilizzando i pacchetti di soluzione, ma questo metodo può essere utilizzato per pubblicare i modelli di rapporti di altre origini.

Nota: per eseguire Crystal Publishing Wizard (Pubblicazione guidata Crystal) è necessaria una piattaforma Windows.

Per importare i modelli di Crystal Reports:

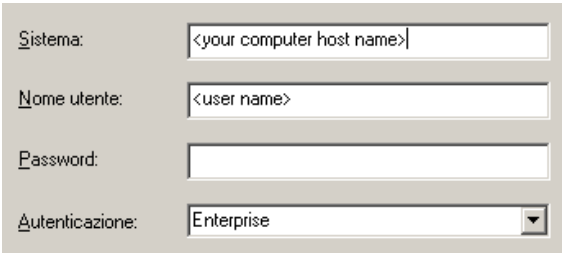
Nota: se si importano (pubblicano) di nuovo i modelli di rapporto, eliminare quelli importati in precedenza.

---

1. Fare clic su Start > Tutti i programmi > BusinessObjects 115 > Crystal Reports Server > Publishing Wizard (Pubblicazione guidata).
2. Fare clic su Avanti.

   Login. System (Sistema) dovrebbe essere il nome del computer host e Authentication (Autenticazione) dovrebbe essere Enterprise. In User Name è possibile immettere Administrator. Per motivi di sicurezza, è opportuno utilizzare un utente diverso da Administrator. Immettere la password, quindi fare clic su Next.

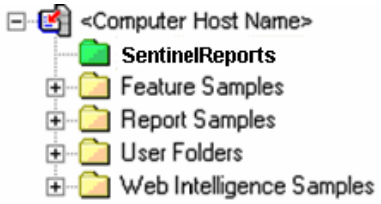
Nota: La pubblicazione di rapporti da parte dell'utente Administrator (Amministratore) consente a tutti gli utenti di accedere ai rapporti.



3 Fare clic su Aggiungi cartella. [Facoltativo] Fare clic su Include Subfolders (Includi sottocartelle).

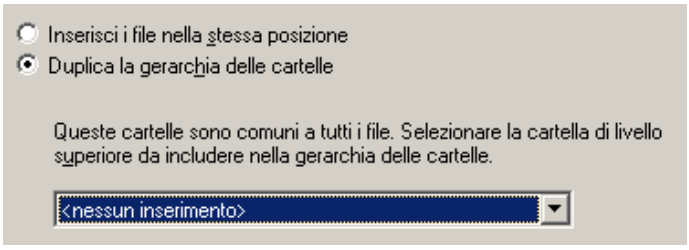
4 Passare all'ubicazione del modello di rapporto. Fare clic su OK. Fare clic su Avanti.

5 Nella finestra Specify Location (Specifica ubicazione), fare clic su New Folder (Nuova cartella) nell'angolo in alto a destra, quindi creare una cartella chiamata SentinelReports (se non esiste già). Fare clic su Avanti.



6 Seleziona:

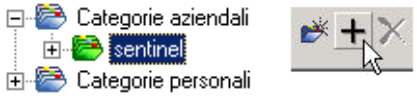
- Il pulsante di scelta 'Duplicate the folder hierarchy' (Duplica gerarchia cartelle).
- Fare clic sulla freccia giù e selezionare <include none>.



Fare clic su Avanti.

7 Nella finestra Confirm Location (Conferma percorso) fare clic su Next (Avanti).

8 Nella finestra Specify Categories (Specifica categorie), immettere un nome di categoria (ad esempio sentinel), evidenziare il nome, quindi fare clic sul pulsante +.



Nota: Dopo aver fatto clic su Next sotto la categoria verrà visualizzato solo il primo rapporto.

Fare clic su Avanti.

9. Nella finestra Specify Schedule (Specifica pianificazione), fare clic sul pulsante di scelta 'Let users update the object' (Oggetto aggiornato dagli utenti) (dovrebbe essere l'impostazione di default). Fare clic su Avanti.
10. Nella finestra Specify Repository Refresh (Specifica aggiornamento archivio), fare clic su Enable All (Attiva tutti) per abilitare l'aggiornamento degli archivi. Fare clic su Avanti.
11. Nella finestra Specify Keep Saved Data (Specifica mantieni dati salvati), fare clic su Enable All (Attiva tutti) per conservare i dati salvati durante la pubblicazione dei rapporti. Fare clic su Avanti.
12. Nella finestra Change Defaults Values (Modifica valori predefiniti), fare clic sul pulsante di scelta 'Publish reports without modifying properties' (Pubblica rapporti senza modificare le proprietà) (dovrebbe essere l'opzione di default). Fare clic su Avanti.
13. Fare clic su Next (Avanti) per aggiungere gli oggetti.
14. Fare clic su Avanti. Fare clic su Fine.

Una volta pubblicati i modelli Sentinel per Crystal Reports in Crystal Reports Server, è necessario che siano ubicati all'interno della directory SentinelReports per poter essere visualizzati in Sentinel Control Center.

9.3.3 Pubblicazione di modelli di rapporti – Central Management Console (Console di gestione centrale)

I rapporti di Sentinel vengono ora distribuiti utilizzando i pacchetti di soluzione, ma questo metodo può essere utilizzato per pubblicare i modelli di rapporti di altre origini.

Per importare i modelli di Crystal Reports:

1. Avviare un browser Web e digitare l'URL seguente:
   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise115/adminlaunch
   ```
2. Fare clic su Central Management Console
3. Eseguire il login al server Crystal Reports.
4. Nel riquadro Organize (Organizza) fare clic su Folders (Cartelle).
5. Nell'angolo superiore destro fare clic su New Folder.
6. Creare una cartella denominata SentinelReports, se non esiste già. Fare clic su OK.

   Nota: È necessario assegnare alla cartella esattamente il nome SentinelReports.
7. Fare clic su SentinelReports.
8. Fare clic sulla scheda Subfolders (Sottocartelle) e creare delle sottocartelle, se necessario. Se si aggiungono i rapporti principali di Sentinel manualmente, creare le seguenti sottocartelle:
   - Advisor_Vulnerability
   - rinnovi/previsioni

- Incident Management
- Eventi interni
- Security Events
- Top 10

9 Fare clic su Home > Objects > New Object.

10 Sul lato sinistro della pagina evidenziare Report.

11 Fare clic su Sfoglia e individuare l'ubicazione dei modelli di rapporti da aggiungere. Fare clic su una cartella e selezionare un rapporto.

12 Evidenziare SentinelReports, quindi fare clic su Show Subfolders (Mostra sottocartelle).

13 Selezionare la cartella appropriata per il rapporto e fare clic su 'Show Subfolders' (Mostra sottocartelle).

14 Fare clic su Invia.

15 Per aggiungere gli altri rapporti, ripetere i passaggi da 9 a 17 fino a quando sono stati aggiunti tutti i rapporti.

9.4 Uso del server Web di Crystal XI R2

In Linux Crystal Reports Server XI installa un server Web che consente di eseguire task di amministrazione oltre alla pubblicazione e visualizzazione di rapporti.

È possibile accedere al portale di amministrazione tramite il browser Web all'URL seguente:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

È possibile accedere al portale non di amministrazione (di uso generale) tramite il browser Web all'URL seguente:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115
```

9.4.1 Esecuzione del test della connettività al server Web

Per eseguire il test della connettività al server Web:

1 Passare a un computer diverso ma che sia nella stessa rete del server Web.

2 Immettere

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

Dovrebbe essere visualizzata una pagina Web di Crystal BusinessObjects.

9.4.2 Impostazione di un conto "Named User"

Il codice di licenza fornito con Crystal Reports Server è un codice di conto Named User. Il conto Guest deve essere modificato da Concurrent User a Named User.

Per impostare il conto Guest come Named User:

1. Avviare un browser Web e digitare l'URL seguente:
   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise115/adminlaunch
   ```
2. Fare clic su Central Management Console.
3. Il nome del sistema dovrebbe essere il nome del computer host. Il tipo di autenticazione dovrebbe essere Enterprise. In caso contrario, selezionare Enterprise.
4. Nel riquadro Organize fare clic su Users > Guest.
5. Modificare il tipo di connessione da Concurrent User a Named User, quindi scegliere Update.

   Eseguire il logoff e chiudere la finestra.

9.4.3 Configurazione delle autorizzazioni per i rapporti

Questa procedura indica come utilizzare .NET Administration Launchpad per configurare le autorizzazioni per i rapporti per consentirne la visualizzazione e la modifica su richiesta.

Per configurare le autorizzazioni per i rapporti:

1. Avviare un browser Web e digitare l'URL seguente:
   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise115/adminlaunch
   ```
2. Fare clic su Central Management Console.

   Il nome del sistema dovrebbe essere il nome del computer host. Il tipo di autenticazione dovrebbe essere Enterprise. In caso contrario, selezionare Enterprise.
3. Immettere nome utente e password e fare clic su Log On.
4. Nel riquadro Organize fare clic su Folders.
5. Fare clic su SentinelReports, quindi scegliere Select All.
6. Fare clic sulla scheda Rights (Diritti).
7. Per Everyone, selezionare View on Demand (Visualizza su richiesta) nel menu a discesa a destra.
8. Fare clic su Update, eseguire il logoff e chiudere la finestra.

9.5 Aumento del limite di record di aggiornamento dei rapporti di Crystal Reports Server

Se Crystal tenta di elaborare un numero molto elevato di eventi, potrebbe verificarsi un errore relativo al tempo massimo di elaborazione o al limite massimo di record. Per impostare il server per l'elaborazione di un numero superiore o illimitato di record sarà necessario riconfigurare Crystal Page Server.

Per riconfigurare Crystal Page Server:

1. Avviare un browser Web e digitare l'URL seguente:
   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise115/adminlaunch
   ```
2. Fare clic su Central Management Console.
3. Il nome del sistema dovrebbe essere il nome del computer host. Il tipo di autenticazione dovrebbe essere Enterprise. In caso contrario, selezionare Enterprise.
4. Immettere nome utente e password e fare clic su Log On.
5. Fare clic su Servers, quindi su <nome server>.pageserver.
6. In Database Records to Read When Previewing Or Refreshing a report fare clic su Unlimited records, quindi scegliere Apply.
7. Verrà visualizzato un prompt per il riavvio del page server. Fare clic su OK.
8. È possibile che vengano richiesti un nome di login e una password per accedere al manager dei servizi del sistema operativo.

9.6 Configurazione di Sentinel Control Center per l'integrazione con Crystal Reports Server

Sentinel Control Center può essere configurato per l'integrazione con Crystal Reports Server per consentire la visualizzazione dei rapporti di Crystal Reports da Sentinel Control Center.

Per abilitare l'integrazione di Sentinel Control Center con Crystal Reports Server, attenersi alle seguenti istruzioni.

Nota: È possibile eseguire questa configurazione solo dopo aver installato Crystal Reports Server e aver pubblicato sul server i rapporti di Crystal Reports. Per ulteriori informazioni sulle piattaforme supportate per Crystal Reports Server in un ambiente Sentinel, vedere Capitolo 2, “Requisiti di sistema”, a pagina 21.

Per configurare Sentinel per l'integrazione con Crystal Reports Server:

1. Eseguire il login a Sentinel Control Center come utente con privilegi per la scheda Amministratore.
2. Nella scheda Amministratore, selezionare Crystal Report Configuration (Configurazione Crystal Report).
3. Nel campo URL analisi specificare quanto segue:
   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   esec-script/
   GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
   ```

   Nota: <hostname_or_IP_of_web_server> deve essere sostituito con l'indirizzo IP o il nome host del server Crystal Reports.

Nota: Questo URL non funzionerà correttamente se APS è impostato sull'indirizzo IP. Deve corrispondere al nome host.

Nota: <web_server_port_default_8080> deve essere sostituito con la porta sulla quale è in ascolto il server Web di Crystal Reports.

4 Fare clic sul pulsante Aggiorna accanto al campo URL analisi.

5 Se è installato Advisor, nel campo URL Advisor specificare:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
esec-script/
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

Nota: <hostname_or_IP_of_web_server> deve essere sostituito con l'indirizzo IP o il nome host del server Crystal Reports.

Nota: Questo URL non funzionerà correttamente se APS è impostato sull'indirizzo IP. Deve corrispondere al nome host.

Nota: <web_server_port_default_8080> deve essere sostituito con la porta sulla quale è in ascolto il server Web di Crystal Reports.

6 Fare clic sul pulsante Aggiorna accanto al campo URL di Advisor;

Fare clic su Salva.

7 Eseguire il logout e quindi il login in Sentinel Control Center.

Gli alberi di Crystal Reports nelle schede Analisi e Advisor (se Advisor è installato) ora dovrebbero essere visualizzati nella barra di spostamento.

9.7 Utility e soluzione dei problemi

9.7.1 Avvio di MySQL

Per verificare che MySQL sia in esecuzione:

1 Eseguire il login come utente crystal.

2 cd /opt/crystal_xir2/bobje

3 `./mysqlstartup.sh`

9.7.2 Avvio di Tomcat

Per verificare che Tomcat sia in esecuzione:

1 Eseguire il login come utente crystal

2 cd /opt/crystal_xir2/bobje

3 `./tomcatstartup.sh`

9.7.3 Avvio dei server Crystal Reports

Per verificare che i server Crystal Reports siano in esecuzione:

1. Eseguire il login come utente crystal
2. cd /opt/crystal_xir2/bobje
3. `./startservers`

9.7.4 Errore del nome host Crystal

Per risolvere un errore del nome host:

1. Se viene visualizzato l'errore seguente:

   ```
   Warning: ORB::BOA_init: hostname lookup returned `localhost'
   (127.0.0.1)
   Use the -OAhost option to select some other hostname
   ```

   Verificare che l'indirizzo IP e il nome host siano presenti nel file /etc/hosts. Ad esempio,

   ```
   10.0.0.1   linuxCE02
   ```

9.7.5 Impossibile connettersi a CMS

Se il sistema indica l'impossibilità di connettersi a CMS, provare a eseguire i comandi seguenti.

Per risolvere i problemi di connessione del CMS:

1. Se il comando netstat –an | grep 6400 non restituisce alcun risultato, eseguire le seguenti procedure:
   - Immettere di nuovo le informazioni per la connessione MySQL:
     1. Eseguire il login come utente crystal
     2. cd /opt/crystal_xir2/bobje
     3. `./cmsdbsetup.sh`
     4. Quando viene visualizzato `[<nome host>.cms]` premere Invio.
     5. Immettere tutte le informazioni del database MySQL specificate durante l'installazione. Per ulteriori informazioni, consultare le istruzioni di installazione nel Capitolo 3, “Installazione di Sentinel 6.1”, a pagina 31.
     6. Al termine, chiudere `cmsdbsetup.sh`
     7. `./stopservers`
     8. `./startservers`
   - Inizializzare di nuovo il database MySQL:
     1. Eseguire il login come utente crystal
     2. cd /opt/crystal_xir2/bobje
     3. `./cmsdbsetup.sh`
     4. Quando viene visualizzato `[<nome host>.cms]` premere Invio.
     5. Selezionare reinitialize e seguire le istruzioni.

6. Al termine, chiudere `cmsdbsetup.sh`
7. `./stopservers`
8. `./startservers`

1 Verificare che tutti i server CCM siano abilitati:

1a Eseguire il login come utente crystal

1b cd /opt/crystal_xir2/bobje

1c `./ccm.sh` -enable all

9.8 Configurazioni a prestazioni elevate per Crystal

A seconda del numero di eventi su cui viene eseguita l'interrogazione in Crystal, è possibile che venga visualizzato un errore relativo al tempo massimo di elaborazione o al limite massimo di record. Per impostare il server per l'elaborazione di un numero superiore o illimitato di record sarà necessario riconfigurare Crystal Page Server. Questa operazione può essere eseguita utilizzando Central Configuration Manager o la pagina Web di Crystal.

Per riconfigurare Crystal Page Server tramite Central Configuration Manager:

1 Fare clic su Start > Tutti i programmi > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.

2 Fare clic con il pulsante destro del mouse su Crystal Reports Page Server quindi scegliere Stop.

3 Fare clic con il pulsante destro del mouse su Crystal Reports Page Server quindi scegliere Properties.

4 Nel campo Comando della scheda Proprietà, alla fine della riga di comando aggiungere:

```
maxDBResultRecords <value greater than 20000 or 0 to disable the default limit>
```

5 Riavviare Crystal Page Server.

Per riconfigurare Crystal Page Server mediante la console di gestione centrale:

1 Fare clic su Start > Tutti i programmi > BusinessObjects 11 > Crystal Reports Server > .Net Administration Launchpad. In alternativa, avviare un browser Web e immettere il seguente URL:

http:// nome DNS o indirizzo IP del server Web /businessobjects/enterprise /WebTools/ adminlaunch/default.aspx

2 Fare clic su Central Management Console.

3 Il nome del sistema dovrebbe essere il nome del computer host. Il tipo di autenticazione dovrebbe essere Enterprise. In caso contrario, selezionare Enterprise.

4 Immettere nome utente e password e fare clic su Log On. Fare clic su Server.

5 Fare clic su <nome server>.pageserver.

6 In Database Records to Read When previewing or Refreshing a report fare clic su Unlimited records. Fare clic su Applica.

7 Verrà visualizzato un prompt per il riavvio del page server. Fare clic su OK.

È possibile che vengano richiesti un nome di login e una password per accedere al manager dei servizi del sistema operativo.

9.8.1 Rapporti mediante il servizio di aggregazione

Per migliorare le prestazioni, i primi 10 rapporti inclusi in Sentinel Core Solution Pack eseguono le interrogazioni sulle tabelle di riepilogo anziché sulla tabella eventi. Le tabelle di riepilogo contengono i conteggi in un intervallo di tempo delle combinazioni di campi nei dati dell'evento. Ciò fornisce un dataset molto più ridotto per alcuni tipi di interrogazione rendendo molto più rapide le interrogazioni e l'esecuzione dei rapporti.

Il servizio Aggregazione è responsabile dell'inserimento nelle tabelle di riepilogo dei riepiloghi di tutti gli eventi presenti nella tabella eventi. Il servizio Aggregazione genererà dati di riepilogo solo per i riepiloghi attivi. Per i primi 10 rapporti sono necessari i seguenti riepiloghi che sono abilitati per default:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

I riepiloghi possono essere attivati o disattivati mediante la finestra Configurazione dati rapporti nella scheda Amministratore di Sentinel Control Center.

Il servizio Aggregazione dipende inoltre dal componente `EventFileRedirectService` del file binario DAS per il feed dei dati di evento che verranno riepilogati. Di conseguenza, per il funzionamento corretto del servizio Aggregazione è necessario abilitare questo componente. Il componente viene abilitato o disabilitato modificando l'attributo "status" del componente `EventFileRedirectService` nel file `das_binary.xml` su "on" o "off". Per default questo componente è impostato su "on".

Nota: Per informazioni su EventFileRedirectService e i tre riepiloghi di aggregazione, vedere “Report Data Configuration” in Admin della *Sentinel User Guide*.

Nota: I rapporti con interrogazioni su un intervallo di date esteso possono richiedere tempi lunghi di esecuzione. È possibile pianificarli anziché eseguirli interattivamente. Per informazioni sulla pianificazione dei rapporti in Crystal Reports, vedere la documentazione su Crystal Reports Server XI R2 (http://support.businessobjects.com/documentation/product_guides/default.asp).

9.8.2 Sviluppo di rapporti

Per creare o modificare i rapporti di Crystal Reports è possibile utilizzare Crystal Reports Developer. Per sviluppare rapporti personalizzati, si consiglia quanto segue:

- Se i rapporti possono utilizzare tabelle aggregate predefinite, selezionare la tabella aggregata che comporta l'elaborazione della minore quantità di dati.
- Provare a inserire quasi tutti i dati da elaborare nel motore del database.
- Per diminuire il sovraccarico dei processi di elaborazione in Crystal Server, ridurre al minimo la quantità di dati da recuperare sul server di Crystal.
- Scrivere sempre i rapporti utilizzando le viste di database fornite da Novell anziché le tabelle di base.

Disinstallazione di Sentinel 10

Per rimuovere un'installazione di Sentinel, sono disponibili i programmi di disinstallazione per Linux, Solaris e Windows. Vengono mantenuti numerosi file, tra i quali i file di log, che tuttavia è possibile eliminare manualmente, se si desidera. Prima di eseguire una nuova installazione, si raccomanda di eseguire tutte le procedure seguenti per essere certi di eliminare tutti i file e le impostazioni di sistema dell'installazione precedente.

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

10.1 Disinstallazione di Sentinel

10.1.1 Disinstallazione per Solaris e Linux

Per utilizzare il programma di disinstallazione di Sentinel per Solaris e Linux:

1. Eseguire il login come utente radice.
2. Arrestare il server Sentinel.
3. Accedere ad:
   `$ESEC_HOME/_uninst`
4. Immettere:

   Per la modalità GUI:

   `./uninstall.bin`

   O

   Per la modalità basata su testo ("console seriale"):

   `./uninstall.bin -console`
5. Selezionare una lingua e fare clic su OK.
6. Viene visualizzata l'installazione guidata InstallShield di Sentinel. 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.

9 Se si è scelto di disinstallare il componente Database, viene richiesto di selezionare una delle seguenti opzioni:

- **Elimina l'intera istanza del database:** rimuove l'istanza del database e libera lo spazio su disco utilizzato dal database.
- **Elimina solo oggetti di database:** rimuove il contenuto del database tranne che per l'utente esecdba. Nell'istanza del database sarà possibile inserire i dati in seguito utilizzando il programma di installazione di Sentinel. Questa opzione non consente di liberare spazio su disco.

10 Se è stata selezionata l'opzione Elimina solo oggetti di database, verrà richiesto di fornire la password esecdba. Fare clic su Avanti.

11 Verrà visualizzato un riepilogo delle funzionalità selezionate per la disinstallazione. Fare clic su Disinstalla.

12 Fare clic su Fine.

10.1.2 Disinstallazione per Windows

Per utilizzare il programma di disinstallazione di Sentinel per Windows:

1 Eseguire il login come Amministratore.

2 Arrestare il server Sentinel.

3 Selezionare Start > Tutti i programmi (Win XP) o Programmi (WIN 2000) > Sentinel > Disinistalla Sentinel. È inoltre possibile scegliere Start > Esegui e digitare %Esec_home%_uninst, quindi fare doppio clic su `uninstall.exe`.

4 Selezionare una lingua e fare clic su OK.

5 Viene visualizzata l'installazione guidata InstallShield di Sentinel 6.1. 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.

8 Se si è scelto di disinstallare il componente Database, viene richiesto di selezionare una delle seguenti opzioni:

- **Elimina l'intera istanza del database:** rimuove il database e libera lo spazio su disco utilizzato dal database.
- **Elimina solo oggetti di database:** rimuove il contenuto del database tranne che per l'utente esecdba. Nel database sarà possibile inserire i dati in seguito utilizzando il programma di installazione di Sentinel. Questa opzione non consente di liberare spazio su disco.

9 Se si è scelto di disinstallare il componente Database, viene richiesto di selezionare una delle seguenti opzioni:

- **Autenticazione di Windows:** Per utilizzare l'Autenticazione Windows, è necessario aver eseguito il login in Windows come amministratore di sistema di un'istanza di MS SQL Server.
- **Autenticazione di SQL:** Immettere il nome utente sa (o equivalente) e la relativa password.

Fare clic su Avanti.

10 Verrà visualizzato un riepilogo delle funzionalità selezionate per la disinstallazione. Fare clic su Disinstalla.

11 Scegliere di riavviare il sistema e fare clic su Fine.

10.2 Operazioni successive alla disinstallazione

10.2.1 Impostazioni di Sentinel

Dopo aver disinstallato Sentinel, 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 Solaris e in Linux, la disinstallazione di Sentinel Server non eliminerà l'utente amministratore di Sentinel dal sistema operativo. Se si desidera eliminare questo utente, sarà necessario procedere manualmente.

Eliminazione delle impostazioni di sistema di Sentinel in Linux

Per eseguire la pulitura manuale di Sentinel in Linux:

1 Eseguire il login come utente radice.

2 Assicurarsi di interrompere tutti i processi di Sentinel.

3 Rimuovere il contenuto di /opt/novell/sentinel6 (o della directory in cui è stato installato il software di Sentinel).

4 Rimuovere i file di avvio di Sentinel Service:

In SLES:

```
chkconfig --del sentinel
```

In RedHat:

```
rm /etc/rc.d/rc0.d/K02sentinel
rm /etc/rc.d/rc3.d/S98sentinel
rm /etc/rc.d/rc5.d/S98sentinel
```

5 Rimuovere i seguenti file, se esistenti, nella directory `/etc/rc.d/rc0.d`:

- K01wizard
- K01esdee
- K01esyslogserver

6 Rimuovere i seguenti file, se esistenti, nella directory `/etc/rc.d/rc3.d`:

- S99wizard
- S99esyslogserver
- S99esdee

7 Rimuovere i seguenti file, se esistenti, nella directory `/etc/rc.d/rc5.d`:

- S99wizard

- S99esyslogserver
- S99esdee

8 Rimuovere i seguenti file, se esistenti, nella directory `/etc/init.d`:

- sentinel
- wizard
- esdee
- esyslogserver

9 Assicurarsi che nessun utente abbia effettuato il login come utente amministratore di Sentinel (esecadm per default), quindi rimuovere l'utente (e la home directory) e il gruppo esec.

- Eseguire: `userdel -r esecadm`
- Eseguire: `groupdel esec`

10 Rimuovere la directory /root/InstallShield.

11 Rimuovere il file /root/vpd.properties

12 Rimuovere la sezione di InstallShield `/etc/profile and /etc/.login`

13 Rimuovere il database Oracle di Sentinel. Per ulteriori informazioni, vedere “Rimuovere il database Sentinel Oracle su Linux e Solaris.” a pagina 145.

14 Riavviare il sistema operativo.

Eliminazione delle impostazioni di sistema di Sentinel in Solaris

Per eseguire la pulitura manuale di Sentinel in Solaris:

1 Eseguire il login come utente radice.

2 Assicurarsi che non siano in esecuzione processi di Sentinel.

3 Rimuovere il contenuto di `/opt/novell/sentinel6` (o della directory in cui è stato installato il software di Sentinel).

4 Rimuovere i seguenti file, se esistenti, nella directory `/etc/rc0.d`:

- K01wizard
- K02sentinel
- K01esdee
- K01esyslogserver

5 Rimuovere i seguenti file, se esistenti, nella directory `/etc/rc3.d` :

- S98sentinel
- S99wizard
- S99esyslogserver
- S99esdee

6 Rimuovere i seguenti file, se esistenti, nella directory `/etc/init.d` :

- sentinel
- wizard

- esdee
- esyslogserver

7 Rimuovere i seguenti file, se esistenti, nella directory `/usr/local/bin`:

- `stop_wizard.sh`
- `restart_wizard.sh`
- `start_wizard.sh`

8 Assicurarsi che nessun utente abbia effettuato il login come utente amministratore di Sentinel, quindi rimuovere l'utente (e la home directory) e il gruppo esec.

- Eseguire: `userdel -r esecadm`
- Eseguire: `groupdel esec`

9 Rimuovere la sezione di Installshield `/etc/profile and /etc/.login`

10 Rimuovere l'eventuale directory /InstallShield.

11 Eliminare i riferimenti di InstallShield in `/var/sadm/pkg.` Se sono presenti i seguenti file, rimuoverli dalla directory `/var/sadm/pkg` :

- Tutti i file che iniziano con IS (IS* nella riga di comando)
- Tutti i file che iniziano con ES (ES* nella riga di comando)
- Tutti i file che iniziano con MISCwp (MISCwp* nella riga di comando)

12 Rimuovere il database Sentinel Oracle. Per ulteriori informazioni, vedere "Rimuovere il database Sentinel Oracle su Linux e Solaris." a pagina 145.

13 Riavviare il sistema operativo.

Rimuovere il database Sentinel Oracle su Linux e Solaris.

Per eseguire manualmente la pulitura del database Sentinel Oracle su Linux e Solaris, attenersi alla seguente procedura:

Nota: prima di rimuovere il database, accertarsi che non venga utilizzato da altre applicazioni.

---

1 Eseguire il login come oracle.

2 Interrompere Oracle Listener:

- Eseguire: `lsnrctl stop`

3 Arrestare il database di Sentinel

- Impostare la variabile di ambiente ORACLE_SID sul nome dell'istanza del database Sentinel in uso (ESEC per default).
- Eseguire: `sqlplus "/ as sysdba"`
- Al prompt sqlplus, eseguire: `shutdown immediate`

4 Rimuovere la voce corrispondente al database Sentinel nel file oratab, la cui posizione è:

Su Linux:

`/etc/oratab`

In Solaris:

`/var/opt/oracle/oratab`

5 Rimuovere il file init<nome_istanza>.ora (per default initESEC.ora) dalla directory $ORACLE_HOME/dbs.

6 Rimuovere le voci dal database di Sentinel dai file seguenti nella directory $ORACLE_HOME/network/admin:

- tnsnames.ora
- listener.ora

7 Eliminare i file di dati del database dall'ubicazione in cui si è scelto di installarli.

8 Eliminare i file di archivio del database dall'ubicazione in cui si è scelto di crearli.

Rimuovere le impostazioni di sistema Sentinel su Windows con il server MS SQL.

Per eseguire la pulitura manuale di Sentinel su Windows:

1 Eliminare la cartella %CommonProgramFiles%\InstallShield\Universal e tutto il relativo contenuto.

2 Eliminare la cartella %ESEC_HOME% % (per default: C:\Programmi\Novell\Sentinel6).

3 Fare clic con il pulsante destro del mouse su Risorse del computer, Proprietà, quindi scegliere la scheda Avanzate.

4 Fare clic sul pulsante Variabili d'ambiente.

5 Se presenti, eliminare le seguenti variabili:

- ESEC_HOME
- ESEC_VERSION
- ESEC_JAVA_HOME
- ESEC_CONF_FILE
- WORKBENCH_HOME

6 Rimuovere dalla variabile d'ambiente PATH eventuali voci che fanno riferimento all'installazione di Sentinel.

Avviso: non rimuovere percorsi né altri elementi, ad eccezione della precedente installazione di Sentinel, per evitare problemi di cattivo funzionamento del sistema.

---

7 Eliminare tutti i collegamenti a Sentinel nel desktop.

8 Eliminare dal menu Start la cartella di collegamento Start >Programmi > Sentinel.

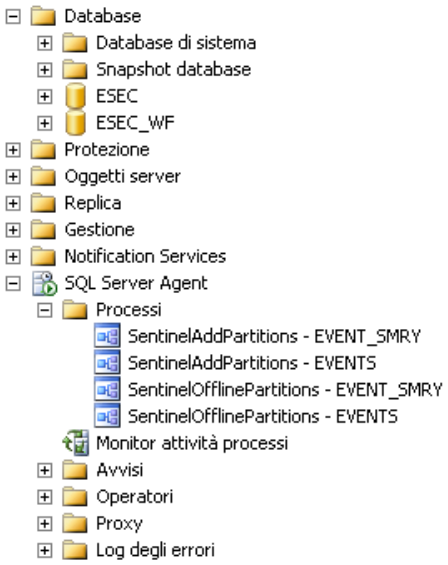
9 Riavviare il sistema operativo.

Per eseguire la pulitura manuale del database Sentinel Microsoft SQL Server su Windows:

Nota: prima di rimuovere il database, accertarsi che non venga utilizzato da altre applicazioni.

---

1 Aprire Microsoft SQL Server Management Studio ed eseguire la connessione all'istanza SQL Server in cui è stato installato il database Sentinel in uso.



2. Espandere l'albero SQL Server Agent > Processi e rimuovere i processi di Sentinel.
3. Espandere l'albero dei database e individuare il database Sentinel in uso. Dovrebbero essere presenti un database Sentinel (denominato ESEC per default) e un database iTRAC (ESEC_WF per default). Fare clic su ciascun nome con il pulsante destro del mouse e selezionare Cancella.
4. Quando richiesto, selezionare Sì per eliminare il database.
5. Espandere l'albero Sicurezza > Login e rimuovere gli eventuali utenti del database di Sentinel.
   - esecdba
   - esecapp
   - esecadm
   - esecrpt
6. Eliminare i file archivio del database dall'ubicazione selezionata per la creazione.

Questionario preliminare all’installazione

A

Rispondendo alle seguenti domande si facilita la propria pianificazione dell'installazione o si consente ai consulenti di preparare l'installazione del sistema Sentinel.

Domande preliminari all’installazione

1. Per quale scopo o intenzione si utilizza Novell Sentinel?
   - **1a** Conformità
   - **1b** Gestione degli eventi di sicurezza
   - **1c** Altro_____
2. Quali componenti hardware sono stati allocati per l’installazione di Sentinel? Corrisponde alle specifiche hardware riportate nella guida all'installazione di Sentinel per la configurazione in uso?
3. L'hardware Sentinel e i requisiti di sistema descritti nella guida all'installazione di Sentinel sono stati convalidati per la configurazione in uso?
   - Livelli patch sistema operativo
   - Service Pack
   - Hot fix e così via.
4. Il computer DAS soddisfa i requisiti obbligatori di sistema operativo e hardware?
5. In quale architettura di rete per i dispositivi di origine, in relazione al segmento di sicurezza, deve trovarsi l’hardware di Sentinel e dei servizi di raccolta?

Nota: questa informazione è importante per comprendere la gerarchia dalla raccolta dati dei servizi di raccolta e per identificare tutti i firewall che è necessario attraversare per consentire le comunicazioni tra i servizi di raccolta e Sentinel, Sentinel e il database o Crystal Server e il database.

Fornire di seguito le informazioni richieste (testo e/o disegni) o il collegamento alle informazioni.

6 Quali rapporti si desidera escludere dal sistema? Questa informazione serve a garantire che Collectors raccolga i dati corretti da trasferire al database di Sentinel.

6a _____

6b _____

6c _____

6d _____

6e _____

6f _____

7 Da quali dispositivi di origine si desidera raccogliere dati (IDS, HIDS, Router, Firewall e così via), con che frequenza eventi (EPS, eventi al secondo) e con quali versioni, metodi di connessione, piattaforme e patch?

Dispositivo (produttore/ modello)	Frequenza evento (EPS)	Versione	Metodo di connessione	Piattaforma	Patch

È possibile specificare un esempio dei dati che si desidera vengano raccolti e analizzati dai Servizi di raccolta Sentinel? È possibile configurare Sentinel in modo che fornisca l'output desiderato sulla base delle informazioni riportate nella presente guida.

8 Quale modello o quali standard di sicurezza sono utilizzati in azienda?

- In che modo vengono gestiti i conti locali rispetto all'autenticazione di dominio?
  - Per Windows con autenticazione di dominio è necessario specificare impostazioni di conti di dominio appropriate che consentano di installare Sentinel.
  - Questa procedura non può essere applicata alle installazioni Solaris. Sentinel non supporta NIS.

9 Specificare il periodo di memorizzazione dei dati in termini di giorni?

10 In base alle informazioni sulla memorizzazione ed EPS quali dimensioni disco verranno utilizzate? Per le dimensioni stimate utilizzare da 500 a 800 byte per evento.

11 Quali schemi evento si desidera identificare nei dati?

12 I dati disponibili al momento mediante le origini evento utilizzate supportano gli schemi evento che si desidera rilevare oppure sarà necessario applicare un servizio di mappatura per arricchire l'evento?

13. Qualora sia necessario il servizio di mappatura, qual è l'origine dei dati di arricchimento e quale chiave verrà utilizzata per eseguire la mappatura? Come verranno mantenute aggiornate le mappe?
14. Se viene rilevata una violazione di sicurezza o conformità, quali processi verranno utilizzati per risolverla?

Installazione di Oracle

B

B.1 Installazione di Oracle

Importante: Dichiarazione di non responsabilità: le istruzioni riportate di seguito non devono essere considerate sostitutive della documentazione Oracle. Si tratta solo di un esempio di uno scenario di impostazione. Questa documentazione presume che la home directory degli utenti di Oracle sia //home/oracle e che Oracle venga installato in /opt/oracle. La configurazione esatta in uso potrebbe variare. Per ulteriori informazioni consultare documentazione del sistema operativo e di Oracle.

Per ulteriori informazioni sulle installazioni Oracle e per il preciso livello di patch certificato o supportato per Sentinel, vedere la sezione Capitolo 2, “Requisiti di sistema”, a pagina 21.

B.1.1 Installazione di Oracle 10g su SLES 10

Per installare Oracle in SUSE Linux Enterprise Server 10:

1. Attenersi alle istruzioni di installazione disponibili nel manuale di installazione di SLES 10. Installare SLES 10 con il filesystem ext3 e i pacchetti di default insieme a Oracle Server Base e a Strumenti e Compilatore C/C++.
2. Eseguire il login come utente radice.
3. Installare il Service Pack SLES 10. Verificare le informazioni sul service pack immettendo:

   ```
   SPident
   ```

   oppure

   ```
   cat /etc/SuSE-release
   ```

   Al momento della compilazione della presente documentazione, il service pack SLES 10 non è ancora stato rilasciato. Per la verifica, utilizzare SPident o cat/etc/SUSE-release.

   Il risultato dovrebbe essere:

   ```
   CONCLUSION: System is up-to-date!
     Found     SLES-10-x86_64-current
   ```
4. L'account dell'utente oracle è disabilitato. Abilitarlo modificando la shell dell'utente Oracle da /bin/false a /bin/bash mediante l'amministrazione degli utenti di YaST o modificando il file /etc/passwd.
5. Impostare una nuova password per l'utente Oracle mediante YaST o digitando:

   ```
   /usr/bin/passwd oracle
   ```
6. Se necessario, modificare l'ambiente Oracle di default impostato da orarun:
   - Cambiare la home directory di Oracle modificando la variabile ORACLE_HOME nel file `/etc/profile.d/oracle.sh`.
   - Il valore di default ORACLE_SID impostato dall'installazione di orarun è "orcl". Modificarlo in ESEC nel file `/etc/profile.d/oracle.sh`.

7 Per impostare i parametri del kernel, eseguire

```
/usr/sbin/rcoracle start
```

8 Passare all'utente Oracle:

```
su - oracle
```

9 Passare alla directory del database ed eseguire `/runinstaller` (Oracle Universal Installer). Si verificherà un errore come indicato di seguito:

10 Risolvere l'errore effettuando una delle operazioni seguenti:

- Modificare il file `database/install/oraparam.ini` per aggiungere il supporto per SUSE Linux 10. Dopo la modifica, la riga "[Certified Versions]" del file oraparam.ini risulterà analoga alla seguente:

  ```
  [Certified Versions]
  Linux=redhat=3,SuSE-9,SuSE-10,redhat-4,UnitedLinux-1.0.asianux-1,asianux-2
  ```

- Eseguire l'installazione con l'opzione -ignoreSysPrereqs

  ```
  that is ./runInstaller –ignoreSysPrereqs
  ```

11 Accettare la directory di inventario di default oppure sfogliare e selezionare una nuova directory. Fare clic su Avanti.

12 Tra i tipi di installazione selezionare Enterprise Edition. Fare clic su Avanti.

13 Per il controllo dei requisiti di configurazione della rete, selezionare User Verified. Fare clic su Avanti.

14 Tra le opzioni di configurazione selezionare solo Install Database Software. Fare clic su Avanti.

15 Verrà visualizzato il riepilogo dell'installazione. Esaminarlo e fare clic su Install.

16 Eseguire gli script specificati come radice. Al termine, scegliere OK.

17 Una volta completata l'installazione, fare clic su Exit.

B.1.2 Installazione di Oracle 10g in Red Hat Linux 4

Per installare Oracle su Red Hat Linux:

1 Eseguire il login come utente radice.

2 Eseguire il seguente comando per verificare che i pacchetti richiesti (elencati di seguito) siano installati sul server in uso.

```
rpm –q make
```

Elenco di pacchetti:

```
compat –db
compat-gcc-32
compat-gcc-32-c++
compat-oracle-rhel4
compat-libcwait
compat-libgcc-296
compat-libstdc++-296
compat-libstdc++-33
gcc
gcc-c++
gnome-libs
gnome-libs-devel
```

```
libaio-devel
libaio
make
openmotif21
xorg-x11-deprecated-libs-devel
xorg-x11-deprecated-libs
```

3 Creare un gruppo UNIX e un conto utente UNIX per il proprietario del database Oracle.

Aggiungere un gruppo dba (come utente radice):

```
groupadd oinstall
groupadd dba
```

4 Aggiungere l'utente Oracle come root:

```
useradd –g oinstall –G dba –d /opt/oracle/product/<10.2.0.3>/db_1 –
m oracle
passwd oracle
```

5 Creare una directory per ORACLE_HOME e ORACLE_BASE:

```
mkdir –p /opt/oracle/product/<10.2.0.3>
```

6 Modificare la proprietà della directory ORACLE_BASE e passare a un livello inferiore di oracle/oinstall:

```
chown -R oracle:oinstall /opt/oracle
```

7 Passare all'utente Oracle:

```
su - oracle
```

8 Aprire il file `.bash_profile` (nella home directory dell'utente oracle) per apportare modifiche, quindi aggiungere il testo seguente alla fine del file:

Nota: Questo gruppo di variabili di ambiente deve essere utilizzato solo per l'utente. Non utilizzarlo nell'ambiente del sistema o dell'utente amministratore di Sentinel.

```
# User specific environment and startup programs
ORACLE_BASE=/opt/oracle; export ORACLE_BASE
ORACLE_HOME=$ORACLE_BASE/product/10.2.0/db_1; export ORACLE_HOME
ORACLE_TERM=xterm; export ORACLE_TERM
PATH=$ORACLE_HOME/bin:$PATH; export PATH
ORACLE_SID=oracle; export ORACLE_SID
LD_LIBRARY_PATH=$ORACLE_HOME/lib; export LD_LIBRARY_PATH
CLASSPATH=$ORACLE_HOME/JRE:$ORACLE_HOME/jlib:$ORACLE_HOME/rdbms/
jlib
CLASSPATH=$CLASSPATH:$ORACLE_HOME/network/jlib; export CLASSPATH
LD_ASSUME_KERNEl=2.4.19; export LD_ASSUME_KERNEL
TMP=/tmp; export TMP
TMPDIR=$TMP;export TMPDIR
PATH=$PATH:$HOME/bin
export PATH

unset USERNAME
```

9 Salvare `.bash_profile`, quindi uscire.

10 Eseguire di nuovo il login come utente oracle per caricare le modifiche apportate alle variabili d'ambiente nell'ultimo passaggio:

```
exit
su - oracle
```

11 Verificare che l'esecuzione di `.bash_profile` sia corretta mediante il seguente comando:

```
set | more
```

12 Eseguire il login come utente Oracle. Se si utilizza l'emulazione X, impostare la variabile d'ambiente DISPLAY:

```
DISPLAY=<machine-name>:0.0; export DISPLAY
```

13 Per installare Oracle 10.2.0.1 dal disco 1, eseguire lo script:

```
./runInstaller
```

14 Durante l'esecuzione del programma di installazione, lasciare tutti i prompt con i valori di default a meno che non sia specificato diversamente di seguito.

- Nella schermata iniziale, scegliere Next.
- Nella finestra File locations, selezionare OUIHome dall'elenco a discesa per Destination Name. Fare clic su Avanti.
- In base alla versione in uso, nella schermata Select Product to Install scegliere Oracle 10g Database 10.2.0.1. Fare clic su Next.
- Nella finestra Installation types, selezionare Enterprise Edition. Fare clic su Avanti.
- Nella finestra Database Configuration, selezionare General Purpose. Fare clic su Avanti.
- Nella finestra di riepilogo, esaminare il riepilogo dell'installazione e fare clic su Install.
- Nella finestra di completamento dell'installazione fare clic su Exit.

15 Per applicare la patch Oracle 10.2.0.3, passare al disco 1 della distribuzione della patch Oracle 10.2.0.3 ed eseguire lo script:

```
./runInstaller
```

16 Seguire le istruzioni visualizzate nelle finestre dell'installazione. Nella finestra di riepilogo, esaminare il riepilogo dell'installazione e fare clic su Install. Nella finestra di completamento dell'installazione, fare clic su Exit.

B.1.3 Installazione di Oracle 10g in Solaris

Nota: Per ulteriori informazioni sulle procedure relative alla definizione delle impostazioni del parametro del kernel in Solaris 10, vedere Sezione 3.4.1, “Impostazione dei valori del kernel”, a pagina 39.

Per installare Oracle 10g in Solaris 10:

1 Eseguire il login come utente radice.

2 Avviare l'installazione

```
#  su - oracle
# < Installation directory or CD mount>/ .runInstaller
```

3 Nella finestra introduttiva:

- Selezionare l'installazione di base.
- Deselezionare l'opzione Create Starter Database.
- Specificare la posizione della directory Oracle Home.
- Il gruppo UNIX DBA corrisponde generalmente a dba. Fare clic su Avanti.

4 Nella finestra dei prerequisiti specifici del prodotto:

- Accertarsi che tutte le verifiche di sistema abbiano avuto esito positivo. Fare clic su Avanti.

5 Nella finestra di riepilogo:

- Esaminare il riepilogo dell'installazione e fare clic su Install.
- Nella finestra di completamento dell'installazione fare clic su Exit.

B.2 Creazione di istanza Oracle manuale (facoltativo)

Per motivi di semplicità, Novell consiglia di utilizzare il programma di installazione di Sentinel per creare l'istanza Oracle durante l'installazione dei componenti del database di Sentinel. La presente procedura viene fornita per i casi in cui la creazione dell'istanza Oracle da parte del DBA rientri nei criteri aziendali. Gli spazi delle tabelle devono essere denominati esattamente come specificato.

Nell'istanza Oracle, sarà necessario configurare:

- Parametri
- Spazi delle tabelle

Per creare un'istanza Oracle:

1 Eseguire il login come utente Oracle.

2 Utilizzando l'interfaccia grafica utente di Oracle Database Assistant, creare gli elementi seguenti:

Nota: i valori possono essere diversi a seconda della configurazione e dei requisiti del sistema. Rivolgersi al proprio amministratore di database.

Tabella B-1 *Parametri consigliati per la configurazione minima di Solaris/Linux*

Parametri consigliati per la configurazione minima di Solaris/Linux	
Parametri	**Dimensioni (byte o specificato diversamente)**
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 MB
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAR
hash_join_enabled	TRUE

Parametri consigliati per la configurazione minima di Solaris/Linux	
Parametri	**Dimensioni (byte o specificato diversamente)**
optimizer_index_caching	50
optimizer_index_cost_adj	55

Tabella B-2 *Dimensioni minime consigliate per lo spazio delle tabelle in Solaris/Linux*

Dimensioni minime consigliate per lo spazio delle tabelle in Solaris/Linux		
Spazio delle tabelle	**Dimensioni esempio**	**Note**
REDO	3x100M	Valore minimo. Questo valore minimo deve essere aumentato se la frequenza degli eventi è elevata.
SYSTEM	500 M	Valore minimo (estensione automatica abilitata)
TEMP	1 G	Valore minimo (estensione automatica abilitata)
UNDO	1 G	Valore minimo (estensione automatica abilitata)
ESENTD	5 G	Valore minimo Per dati di evento (estensione automatica abilitata)
ESENTD2	500 M	Valore minimo Dati per configurazione, risorse, vulnerabilità e associazioni (estensione automatica abilitata)
ESENTWFD	250 M	Per dati di iTrac (estensione automatica abilitata)
ESENTWFX	250 M	Per l'indice di iTrac (estensione automatica abilitata)
ESENTX	3 G	Valore minimo Per indice di evento (estensione automatica abilitata)
ESENTX2	500 M	Valore minimo Indice per configurazione, risorse, vulnerabilità e associazioni (estensione automatica abilitata)
SENT_ADVISORD	15 G	Valore minimo se Advisor viene acquistato. Per dati di Advisor (estensione automatica abilitata).
SENT_ADVISORX	15 G	Valore minimo se Advisor viene acquistato. Per indice di Advisor (estensione automatica abilitata)
SENT_AUDITD	250 M	Valore minimo Per i dati di revisione·di Sentinel (estensione automatica abilitata)

Dimensioni minime consigliate per lo spazio delle tabelle in Solaris/Linux		
Spazio delle tabelle	**Dimensioni esempio**	**Note**
SENT_AUDITX	250 M	Valore minimo
		Per l'indice di revisione di Sentinel (estensione automatica abilitata)
SENT_LOBS	100 M	Valore minimo nell'installazione di base
		Per oggetti di database di grandi dimensioni (estensione automatica abilitata)
	2 G	Valore minimo nell'installazione se è abilitata l'integrazione con il sistema di gestione delle identità
		Per oggetti di database di grandi dimensioni (estensione automatica abilitata)
SENT_SMRYD	3 G	Valore minimo
		Per aggregazione, dati di riepilogo (estensione automatica abilitata)
SENT_SMRYX	2 G	Valore minimo
		Per aggregazione, indice di riepilogo (estensione automatica abilitata)
SYSAUX	100 M	Valore minimo
		Per la revisione di Oracle 10g (non specifico di Sentinel)
		Richiesto solo per Oracle 10g

3. Eseguire lo script `createEsecdba.sh` ubicato nella directory sentinel\dbsetup\bin del CD di installazione di Sentinel. Questo script creerà l'utente esecdba, necessario per l'aggiunta di oggetti di database mediante il programma di installazione di Sentinel.
4. Eseguire il backup del database.

Per ulteriori informazioni sull'installazione del database in un database esistente, vedere la sezione Capitolo 3, “Installazione di Sentinel 6.1”, a pagina 31.

Sentinel con Oracle Real Application Clusters

C

Sentinel 6 è certificato per l'esecuzione su un database Oracle con Real Application Clusters (RAC). La versione di database Oracle supportata è Oracle 10g Release 2 (64 bit) con Real Application Clusters (RAC).

Oltre alle procedure di installazione standard per Sentinel, è necessario eseguire alcuni passaggi aggiuntivi per installare e configurare Sentinel per l'utilizzo di Oracle RAC:

- Configurare il database Oracle RAC
- Installare lo schema di database di Sentinel in Oracle RAC
- Configurare i file delle proprietà di connessione per componenti DAS
- Configurare la connessione per Gestione dati Sentinel
- Configurare la connessione per il server Crystal Enterprise

I passaggi sono riportati nel presente documento.

Nota: prima di installare il software Sentinel 6.0, accertarsi che il cluster di Oracle in uso sia attivo e in esecuzione mediante gli strumenti di Oracle RAC.

C.1 Configurazione del database Oracle RAC

Per configurare il database Oracle RAC:

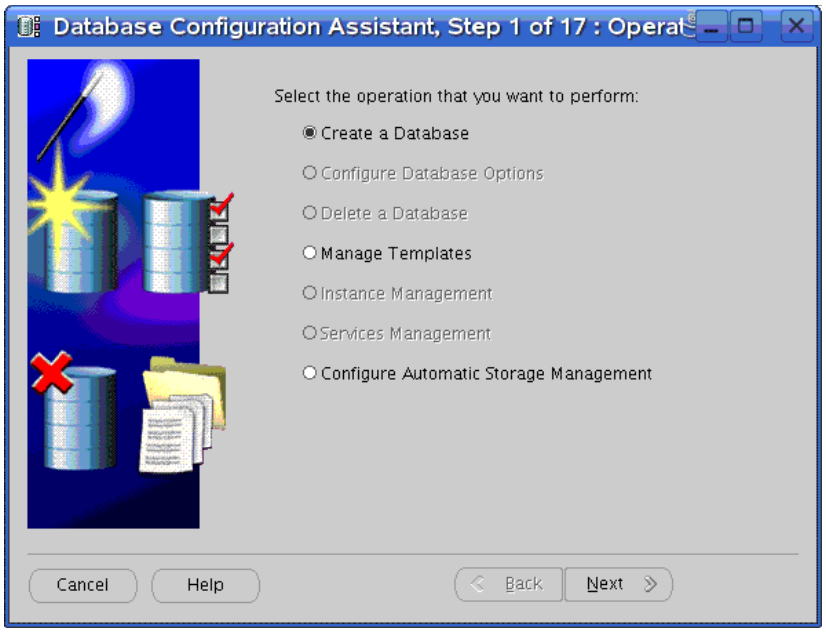
- Creare il database Oracle RAC utilizzando l'utility di configurazione guidata del database di Oracle.
- Creare in Sentinel gli spazi delle tabelle necessari per contenere i dati.
- Creare lo schema proprietario Sentinel ESECDBA
- Installare il database di Sentinel
- Installare gli altri componenti Sentinel
- Configurare il file delle proprietà di connessione

C.1.1 Creazione del database RAC

La procedura consente di creare un database RAC Oracle vuoto, pronto per l'installazione dei componenti Sentinel, mediante Oracle Database Configuration Assistant (DBCA).

Per creare un database RAC:

1. In Database Configuration Assistant, selezionare il database Oracle Real Application Clusters. Fare clic su Avanti.
2. Tra le opzioni presenti nella schermata, scegliere Create a database. Fare clic su Avanti.

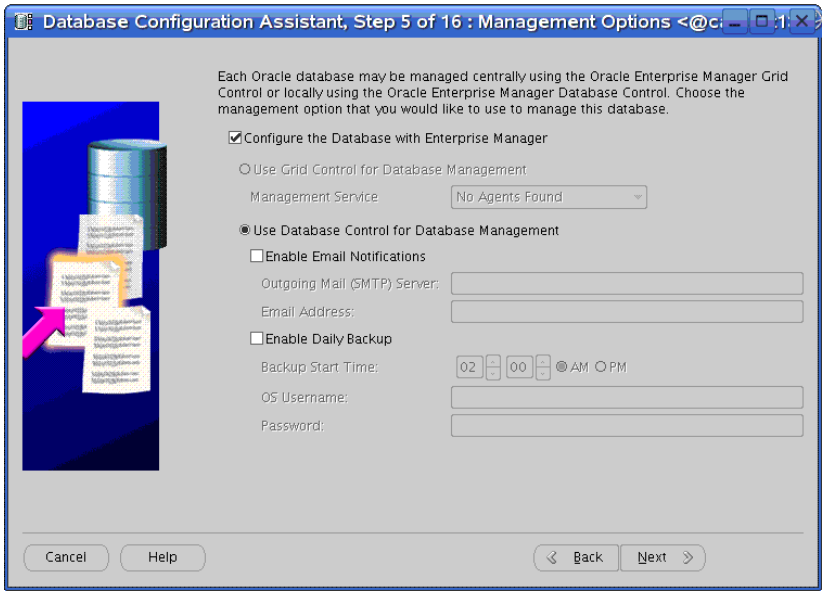


3 Fare clic su Select All per selezionare tutti i nodi per la creazione di database in cluster. Fare clic su Avanti.

4 Selezionare un modello dall'elenco proposto. Per default, è selezionato il modello General Purpose. Fare clic su Avanti.

5 Specificare il nome del database e il prefisso SID (ID di sistema di Oracle). Fare clic su Avanti.

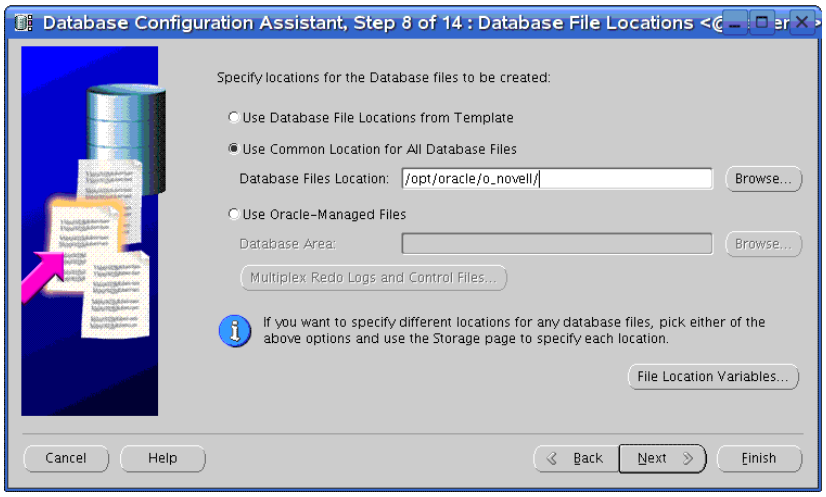
6 Per default, l'opzione di gestione selezionata per il database è Configure the Database with Enterprise Manager. Fare clic su Avanti.



7 È possibile utilizzare le stesse password o password diverse per tutti i conti utente. Selezionare le opzioni e immettere le password. Fare clic su Avanti.

8 Selezionare uno dei tre meccanismi di memorizzazione del sistema, ovvero Cluster File System / Automatic Storage Management / Raw Devices. Se si sceglie Raw Devices, specificare il percorso del file di mappatura corrispondente. Fare clic su Avanti.

9 Specificare la directory in cui posizionare i file di database nel sistema Storage. Fare clic su Fine.



10 Mantenere la selezione di default nelle finestre delle opzioni di Recovery e Sample Schemas, quindi scegliere Next.

11 È possibile creare un servizio database in questo punto oppure in seguito, utilizzando DBCA.

12 Nella finestra di memorizzazione del database, mantenere la selezione di default. Fare clic su Avanti.

13 Selezionare Create database dalle opzioni di creazione del database. Fare clic su Fine.

C.1.2 Creazione di spazi delle tabelle Sentinel

Avviso: L'installazione di Sentinel verrà completata soltanto se si sono creati tutti gli spazi delle tabelle riportati di seguito.

Nota: è possibile utilizzare un'interrogazione Oracle Enterprise Manager o SQL per verificare l'esistenza di tali spazi delle tabelle.

Tabella C-1 *Dimensioni minime consigliate per lo spazio delle tabelle*

Parametri minimi per le dimensioni dello spazio delle tabelle in		
Spazio delle tabelle	**Dimensioni esempio**	**Note**
Parametri minimi per le dimensioni dello spazio delle tabelle in		
REDO	3 x 100 M	Corrisponde al valore minimo. È necessario aumentare questo valore se la frequenza degli eventi è elevata.
SYSTEM	500 M	Valore minimo (estensione automatica abilitata)

Parametri minimi per le dimensioni dello spazio delle tabelle in		
Spazio delle tabelle	**Dimensioni esempio**	**Note**
TEMP	1 G	Valore minimo (estensione automatica abilitata)
UNDO	1 G	Valore minimo (estensione automatica abilitata)
ESENTD	5 G	Valore minimo
		Per dati di evento (estensione automatica abilitata)
ESENTD2	500 M	Valore minimo
		Dati per configurazione, risorse, vulnerabilità e associazioni (estensione automatica abilitata)
ESENTWFD	250 M	Per dati di iTrac (estensione automatica abilitata)
ESENTWFX	250 M	Per l'indice di iTrac (estensione automatica abilitata)
ESENTX	3 G	Valore minimo
		Per indice di evento (estensione automatica abilitata)
ESENTX2	500 M	Valore minimo
		Indice per configurazione, risorse, vulnerabilità e associazioni (estensione automatica abilitata)
SENT_ADVISORD	15 G	Valore minimo se Advisor viene acquistato.
		Per dati di Advisor (estensione automatica abilitata)
SENT_ADVISORX	15 G	Valore minimo se Advisor viene acquistato.
		Per indice di Advisor (estensione automatica abilitata)
SENT_AUDITD	250 M	Valore minimo
		Per i dati di revisione di Sentinel (estensione automatica abilitata)
SENT_AUDITX	250 M	Valore minimo
		Per l'indice di revisione di Sentinel (estensione automatica abilitata)
SENT_LOBS	100 M	Valore minimo nell'installazione di base
		Per oggetti di database di grandi dimensioni (estensione automatica abilitata)
	2 G	Valore minimo nell'installazione se è abilitata l'integrazione con il sistema di gestione delle identità
		Per oggetti di database di grandi dimensioni (estensione automatica abilitata)
SENT_LOBS	100 M	Valore minimo
		Per oggetti di database di grandi dimensioni (estensione automatica abilitata)

Parametri minimi per le dimensioni dello spazio delle tabelle in		
Spazio delle tabelle	**Dimensioni esempio**	**Note**
SENT_SMRYD	3 G	Valore minimo
		Per aggregazione, dati di riepilogo (estensione automatica abilitata)
SENT_SMRYX	2 G	Valore minimo
		Per aggregazione, indice di riepilogo (estensione automatica abilitata)
SYSAUX	100 M	Valore minimo
		Per la revisione di Oracle 10g (non specifico di Sentinel)

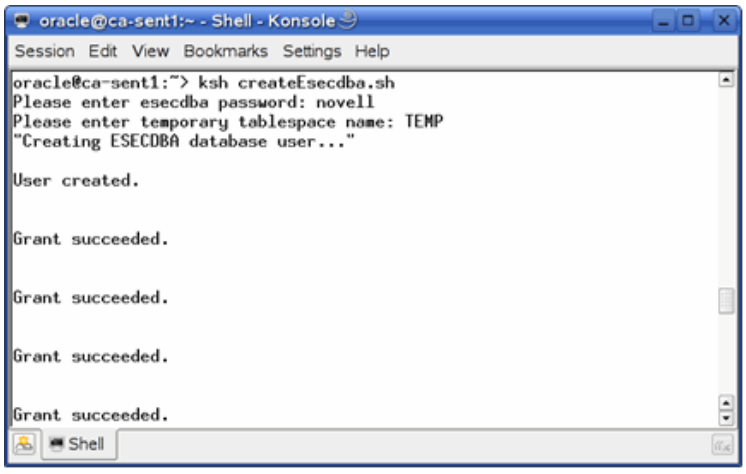
C.1.3 Creazione di ESECDBA

ESECDBA è il nome del proprietario dello schema Sentinel. La maggior parte degli oggetti creati dal programma di installazione di Sentinel sono proprietà di questo utente.

Per creare ESECDBA:

1. Individuare lo script Sentinel `createEsecdba.sh` nel disco di installazione di Sentinel, in disk1/sentinel/dbsetup/bin.
2. Eseguire lo script da qualsiasi computer su cui è installato il client Oracle. Potrebbe essere necessario modificare lo script per impostare correttamente le variabili d'ambiente di Oracle e la stringa “CONNECT AS” (per default, lo script esegue la connessione come “sysdba”).

   Avviso: Eseguire questo script soltanto una volta.



C.2 Installazione del database di Sentinel

Una volta configurato il database, è necessario installare il database di Sentinel. Tale procedura eseguirà l'installazione in un singolo nodo di cluster come nel caso di un'istanza non RAC di Oracle.

È possibile eseguire il programma di installazione di Sentinel da qualsiasi computer su cui sia installato un client Oracle, a condizione che le variabili d'ambiente Oracle corrette per l'utente “Oracle” (ORACLE_HOME, ORACLE_BASE) siano installate nel sistema. Se tale computer sarà anche il server Sentinel, è possibile installare i componenti contemporaneamente (vedere le sezioni precedenti per i prompt relativi ai componenti di base).

Per installare il database di Sentinel:

1. Eseguire il login al server di installazione come utente root.
2. Inserire ed eseguire il CD di installazione di Sentinel oppure il set di file.
3. Passare al CD e fare doppio clic su:

   Per la modalità GUI:

   ```
   ./setup.sh
   ```

   Per la modalità testuale ("headless"):

   ```
   ./setup.sh -console
   ```
4. Selezionare la lingua e fare clic su OK.
5. Dopo aver letto la schermata introduttiva, fare clic su Avanti.
6. Leggere e accettare le condizioni del Contratto di licenza per l'utente finale, quindi fare clic su Avanti.
7. Accettare la directory di installazione di default o fare clic su Sfoglia per specificare un altro percorso di installazione. Fare clic su Avanti.
8. Per il tipo di installazione, selezionare Personalizzata (default). Fare clic su Avanti.
9. Nella finestra di selezione della funzione, deselezionare le eventuali opzioni non necessarie e selezionare database. Fare clic su Avanti.
10. Selezionare la piattaforma del server di database di destinazione.
    - Dall'elenco a discesa, selezionare Oracle 10g.
    - Selezionare Aggiungi oggetti di database a un database vuoto esistente.

    Fare clic su Avanti.
11. Immettere le informazioni sull'autenticazione per la creazione:
    - Utente database dell'applicazione Sentinel
    - Utente amministratore di Sentinel

    Fare clic su Avanti.
12. Verrà visualizzato il riepilogo dei parametri del database specificati. Fare clic su Avanti.
13. Verrà visualizzato il riepilogo dell'installazione. Fare clic su Installa
14. Una volta completata l'installazione, fare clic su Fine.
15. Installare il resto del sistema Sentinel (raccolta servizi, DAS, server di comunicazione e altri componenti Sentinel) utilizzando le informazioni in Capitolo 3, “Installazione di Sentinel 6.1”, a pagina 31.

C.3 Configurazione del file delle proprietà di connessione

È necessario creare manualmente un file delle proprietà di connessione al database con le informazioni relative alla connessione al database RAC. Il file delle proprietà di connessione al database deve essere creato nello stesso computer in cui sono installati i DAS (Data Access Services). Alcune informazioni necessarie sono reperibili nel file $ORACLE_HOME/db/network/admin/tnsnames.ora nei nodi del cluster.

Per configurare RACconnect.properties:

1. Accedere al computer in cui sono installati i componenti DAS (Data Access Service) di Sentinel.
2. Cambiare la directory in $ESEC_HOME/config.
3. Creare il file RACconnect.properties. Di seguito viene riportato un esempio di configurazione per un servizio denominato OLTP con tre nodi:

```
driver=esecurity.base.db.driver.OracleProxyDriver
dburl=jdbc:esecurity:oracleproxy:@
realdriver=oracle.jdbc.driver.OracleDriver
realdburl=jdbc:oracle:thin:@
fatalvendorstates=28,600,1012,1014,1033,1034,1035,1089,1090,1092,1
094,2396,3106,3111,3113,3114
advancedconnectionstring=(DESCRIPTION=
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent1.novell.com) (PORT=1521))
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent2.novell.com) (PORT=1521))
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent3.novell.com) (PORT=1521))
(LOAD_BALANCE=yes)
(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=OLTP)
(FAILOVER_MODE=(TYPE=SELECT)(METHOD=BASIC)(RETRIES=180)
(DELAY=5))))
```

Nota: l'intera stringa “advancedconnectionstring” deve essere su un'unica riga.

4. Modificare il file `configuration.xml` in $ESEC_HOME e aggiungere gli argomenti seguenti ai componenti di processo elencati di seguito:

```
-Desecurity.connect.config.file=../config/RACconnect.properties
```

Tra i componenti di processo che richiedono questo cambiamento sono inclusi:

- DAS_Aggregation
- DAS_Binary
- DAS_iTRAC
- DAS_Query
- DAS_RT

Ad esempio:

```
<process component="DAS" depends="UNIX Communication
Server,Windows Communication Server" image=""$(ESEC_JAVA_HOME)/
java" -server -Dsrv_name=DAS_Query
-Xmx256m -Xms85m -XX:+UseParallelGC -Xss136k -Xrs
-Duser.language=en -Dfile.encoding=UTF8
-Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml,
```

```
/xml/WorkflowMetaData.xml
-Djava.util.logging.config.file=../config/das_query_log.prop
-Djava.security.auth.login.config=../config/auth.login
-Djava.security.krb5.conf=../config/krb5.conf
-Desecurity.execution.config.file=../config/execution.properties -
Dcom.esecurity.configurationfile=../config/configuration.xml
-Desecurity.connect.config.file=../config/RACconnect.properties
-jar ../lib/ccsbase.jar ..//config//das_query.xml"
min_instances="1" name="DAS_Query" post_startup_delay="20"
type="container" working_directory="$(ESEC_HOME)/data" />
```

5 Riavviare i servizi Sentinel in modo da rendere effettive le modifiche apportate alla connessione al database.

C.4 Configurazione della connessione per Gestione dati Sentinel

Per effettuare il login in Gestione dati Sentinel è necessario utilizzare il valore advancedconnectionstring del file RACconnect.properties.

Per effettuare il login a Gestione dati Sentinel:

1 Avviare Gestione dati Sentinel da $ESEC_HOME/bin/sdm.

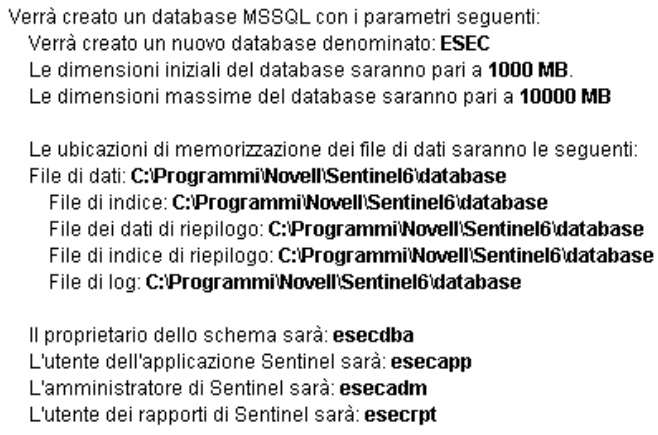
2 Immettere nome utente e password per l'amministratore del database di Sentinel (esecdba per default).

3 Copiare il valore advancedconnectionstring dal file RACconnect.properties.

4 Incollare il valore advancedconnectionstring nel campo Stringa di connessione.

5 Fare clic su Salva impostazioni di connessione.

6 Fare clic su Connetti.



C.5 Configurazione della connessione per Crystal

Per far sì che il server Crystal Enterprise utilizzi il database Oracle RAC, è necessario modificare il file tnsnames.ora. Prima di eseguire le operazioni di questo passaggio, è necessario seguire le fasi dell'installazione standard del server Crystal Enterprise.

Per modificare il file tnsnames.ora:

1. Effettuare il login nel server in cui è installato Crystal Enterprise e individuare il file tnsnames.ora.
2. Modificare il servizio ESECURITYDB perché visualizza le informazioni relative a tutti i nodi. L'indirizzo IP deve essere l'indirizzo IP virtuale. Di seguito è riportato un file di esempio per un sistema a tre nodi:

```
ESECURITYDB =
 (DESCRIPTION =
   (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.1)(PORT = 1521))
   (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.2)(PORT = 1521))
   (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.3)(PORT = 1521))
   (LOAD_BALANCE = yes)
   (CONNECT_DATA =
     (SERVER = DEDICATED)
     (SERVICE_NAME = REPORT.novell.com)
     (FAILOVER_MODE =
       (TYPE = SELECT)
       (METHOD = BASIC)
       (RETRIES = 180)
       (DELAY = 5)
     )
   )
)
```