

Novell® Sentinel™

5.1.3

7 luglio 2006

Volume I - Guida all'installazione

www.novell.com

N

Novell®

Note legali

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

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

Tutti i prodotti e le informazioni tecniche forniti in base al presente contratto potrebbero essere sottoposti al controllo delle esportazioni degli Stati Uniti e alle leggi in materia di scambi commerciali di altri paesi. L'utente accetta di rispettare tutti i regolamenti relativi al controllo delle esportazioni e di procurarsi tutte le licenze o le classificazioni necessarie per esportare, riesportare o importare beni. L'utente accetta di non esportare o riesportare prodotti verso soggetti inseriti negli elenchi di esclusione di esportazione degli Stati Uniti o verso paesi soggetti a embargo o ritenuti terroristi secondo quanto specificato nelle leggi sull'esportazione degli Stati Uniti. L'utente accetta inoltre di non utilizzare i beni per impieghi finali vietati di tipo nucleare o missilistico o di armamento chimico e biologico. Per ulteriori informazioni sull'esportazione del software Novell, consultare il sito all'indirizzo www.novell.com/info/exports/. Novell non assume alcuna responsabilità per il mancato conseguimento da parte dell'utente delle necessarie autorizzazioni all'esportazione.

Copyright © 1999-2006 Novell, Inc. Tutti i diritti riservati. È vietato riprodurre, fotocopiare, memorizzare su un sistema di recupero o trasmettere la presente pubblicazione senza l'espreso consenso scritto dell'editore.

Novell, Inc. possiede i diritti di proprietà intellettuale relativa alla tecnologia incorporata nel prodotto descritto nel presente documento. In particolare, senza limitazioni, questi diritti di proprietà intellettuale possono comprendere uno o più brevetti USA elencati all'indirizzo <http://www.novell.com/company/legal/patents/> e uno o più brevetti aggiuntivi o in corso di registrazione negli Stati Uniti e in altri Paesi.

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

Documentazione in linea: Per accedere alla documentazione in linea per questo e altri prodotti Novell e per ottenere aggiornamenti, visitare il sito Novell all'indirizzo www.novell.com/documentation.

Marchi di fabbrica Novell

Per i marchi Novell, vedere l'elenco disponibile all'indirizzo (<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

In Sentinel 5 possono essere incluse le tecnologie di terze parti seguenti:

- 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/>
- ANTLR. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere <http://www.antlr.org>
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere <http://www.bouncycastle.org>.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, pacchetto di utility. Copyright © Doug Lea. Utilizzato senza classi CopyOnWriteArrayList e ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, con i materiali protetti da copyright seguenti: mars. cpp di Brian Gladman e Sean Woods. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere <http://www.eskimo.com/~weidai/License.txt>.
- Crystal Reports Developer e Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991-2003.
- edpFTPj, concesso in licenza in base alla GNU Lesser General Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere <http://www.enterprisedt.com/products/edtftpj/purchase.html>.
- Enhydra Shark, concesso in licenza in base alla Lesser General Public License disponibile all'indirizzo: <http://shark.objectweb.org/license.html>.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004.
- ILOG, Inc. Copyright © 1999-2004.
- Installshield Universal. Copyright © 1996-2005, Macrovision Corporation e/o Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt (in lingua inglese).

Java 2 Platform può inoltre includere i prodotti di terze parti seguenti:

- CoolServlets © 1999
- DES and 3xDES © 2000 by Jef Poskanzer
- Crimson © 1999-2000 The Apache Software Foundation
- Xalan J2 © 1999-2000 The Apache Software Foundation
- NSIS 1.0j © 1999-2000 Nullsoft, Inc.
- Eastman Kodak Company © 1992

- Lucinda, marchio o marchio registrato di Bigelow e Holmes
- Taligent, Inc.
- IBM, alcuni componenti disponibili all'indirizzo: <http://oss.software.ibm.com/icu4j/>

Per ulteriori informazioni relative alle tecnologie di terze parti e le rispettive esclusioni di garanzia e limitazioni, vedere: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo <http://www.java.sun.com/products/javabeans/glasgow/jaf.htm> (in lingua inglese) e fare clic sul collegamento per scaricare la licenza.
- JavaMail. Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo <http://www.java.sun.com/products/javabeans/glasgow/jaf.htm> (in lingua inglese) e fare clic sul collegamento per scaricare la licenza.
- Java Ace, di Douglas C. Schmidt e il suo gruppo di ricerca presso la Washington University e Tao (con wrapper ACE) di Douglas C. Schmidt e il suo 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, visitare i siti Web agli indirizzi <http://www.cs.wustl.edu/~schmidt/ACE-copying.html> e <http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html> (in lingua inglese).
- Moduli Java Authentication e Authorization Service (JAAS), concessi in licenza in base alla Lesser General Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere <http://free.tagish.net/jaas/index.jsp>.
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo <http://www.java.sun.com/products/javabeans/glasgow/jaf.htm> (in lingua inglese) e fare clic sul collegamento per scaricare la licenza.
- 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>.
- JIDE. Copyright © 2002-2005, JIDE Software, Inc.
- jTDS è concesso in licenza in base alla Lesser GNU Public License. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere <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>.
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Parti di codice sono protette da copyright di diverse organizzazioni con tutti i diritti riservati. Copyright © 1989, 1991, 1992 di Carnegie Mellon University; Copyright © 1996, 1998-2000, the Regents of the University of California; Copyright © 2001-2003 Networks Associates Technology, Inc. ; Copyright © 2001-2003, Cambridge Broadband, Ltd. ; Copyright © 2003 Sun Microsystems, Inc. e Copyright © 2003-2004, Sparta, Inc. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo <http://net-snmp.sourceforge.net> (in lingua inglese).
- The OpenSSL Project. Copyright © 1998-2004. the Open SSL Project. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere <http://www.openssl.org>.
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, precedentemente di Macromedia.
- 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/>.
- Sonic Software Corporation. Copyright © 2003-2004. Il software SSC include software di sicurezza concesso in licenza da RSA Security, Inc.

- Tinyxml. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, vedere <http://grinninglizard.com/tinyxmldocs/index.html>.
- SecurityNexus. Copyright © 2003-2006. SecurityNexus, LLC. Tutti i diritti riservati.
- Xalan e Xerces, entrambi concessi in licenza da Apache Software Foundation Copyright © 1999-2004. Per ulteriori informazioni, esclusioni di garanzia e limitazioni, visitare il sito Web all'indirizzo <http://xml.apache.org/dist/LICENSE.txt> (in lingua inglese).
- 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 Security's Office of the Counsel at 404 Gallows Road, Vienna, VA 500. 703-852-8000.

Prefazione

La documentazione tecnica di Sentinel contiene informazioni generali sull'utilizzo e rappresenta una guida di riferimento. La presente documentazione è rivolta ai professionisti della protezione delle informazioni. Il testo contenuto nella presente documentazione è da considerarsi come documento di riferimento del sistema di gestione della protezione aziendale di Sentinel. Sul portale Web di Sentinel sono disponibili altri documenti.

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

- Volume I: Guida all'installazione di Sentinel™ 5
- Volume II: Guida dell'utente di Sentinel™ 5
- Volume III: Guida dell'utente di Sentinel™ 5 Wizard
- Volume IV: Guida di riferimento dell'utente di Sentinel™ 5
- Volume V: Guida all'integrazione con soluzioni di terze parti di Sentinel™

Volume I: Guida all'installazione di Sentinel 5

In questa guida viene descritto come installare i prodotti seguenti:

- Server Sentinel
- Console Sentinel
- Motore di correlazione di Sentinel
- Crystal Reports per Sentinel
- Generatore servizi di raccolta di Wizard
- Gestione servizi di raccolta di Wizard
- Advisor

Volume II: Guida dell'utente di Sentinel

In questa guida vengono descritti gli argomenti seguenti:

- 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 di host Wizard
- Casi
- Situazioni
- Gestione utenti
- Workflow

Volume III: Guida dell'utente di Wizard

In questa guida vengono descritti gli argomenti seguenti:

- Funzionamento di Generatore servizi di raccolta di Wizard
- Gestione servizi di raccolta di Wizard
- Servizi di raccolta
- Gestione di host Wizard
- Creazione e mantenimento di Servizi di raccolta

Volume IV: Guida di riferimento dell'utente di Sentinel

In questa guida vengono descritti gli argomenti seguenti:

- Linguaggio di script di Wizard
- Comandi di analisi sintattica di Wizard
- Funzioni dell'amministratore di Wizard
- Tag META di Wizard e Sentinel
- Autorizzazioni utente
- Motore di correlazione di Sentinel
- Opzioni della riga di comando di correlazione
- Schema database Sentinel

Volume V: Guida all'integrazione con soluzioni di terze parti di Sentinel

- Remedy
- HP OpenView Operations
- HP Service Desk

Sommario

1 Introduzione	1-1
Convenzioni utilizzate.....	1-1
Note e avvertenze.....	1-1
Comandi	1-1
Panoramica di Sentinel 5	1-1
Moduli del prodotto Sentinel.....	1-3
Sentinel Control Center	1-3
Sentinel Wizard.....	1-3
Sentinel Advisor.....	1-4
Configurazione standard	1-4
Piattaforme supportate per il server Sentinel in Linux.....	1-5
Piattaforme supportate per il server Sentinel in Solaris.....	1-7
Piattaforme supportate per il server Sentinel in Windows	1-9
Altri riferimenti Novell	1-10
Come contattare Novell.....	1-10
2 Procedure consigliate	2-1
Procedure consigliate per l'installazione	2-1
Configurazione semplice autonoma (utilizzo demo)	2-2
Installazione di prova: Configurazione autonoma	2-3
Produzione: Configurazione distribuita	2-4
Norme di supporto delle patch	2-5
Indicazioni sull'hardware.....	2-5
Configurazione dell'array di dischi.....	2-6
Esempio di una configurazione di dispositivi di memorizzazione per un'installazione MS SQL.....	2-6
Esempio di una configurazione di memorizzazione per Oracle	2-8
Configurazione di rete.....	2-8
Installazione del server Oracle e MS SQL	2-8
Patch del database Sentinel	2-9
Impostazioni consigliate per il kernel UNIX.....	2-9
Configurazione di parametri durante la creazione di un'istanza personale del database	2-10
Installazione di Sentinel	2-11
Aumentare al massimo la generazione di rapporti di eventi per Crystal	2-13
Rapporti forniti da Sentinel	2-14
Suggerimenti per lo sviluppo di report Crystal personalizzati	2-14
Procedure consigliate per la manutenzione	2-14
Analisi del database per Oracle.....	2-14
Controllo dello stato del database per Oracle.....	2-16
Archiviazione automatica di dati e aggiunta di partizioni (solo Windows)	2-17
Motore di correlazione	2-21
Log delle transazioni.....	2-23
Ubicazioni dei file di log di Sentinel.....	2-23
3 Installazione di Sentinel 5 per Oracle in Solaris	3-1
Operazioni preliminari all'installazione di Sentinel 5 per Oracle in Solaris	3-1
Per ottenere un codice di licenza.....	3-2
Database di Sentinel.....	3-2
Server Sentinel	3-3

Sentinel Control Center e Wizard	3-4
Advisor	3-4
verifica del layout di Solaris (Requisiti patch per il sistema operativo).....	3-4
Operazioni preliminari all'installazione di Oracle in Solaris	3-4
Installazione di Sentinel 5 per Oracle in Solaris	3-6
Installazione semplice in Solaris	3-6
Installazione personalizzata in Solaris	3-9
Operazioni successive all'installazione di Sentinel 5 per Oracle	3-19
Aggiornamento di e-mail Sentinel per l'autenticazione SMTP	3-19
Database di Sentinel.....	3-20
Servizio di raccolta.....	3-20
Aggiornamento del codice di licenza	3-21
Creazione di un'istanza Oracle per il database di Sentinel	3-21
Impostazione della strategia di inserimento eventi OCI (Oracle Call Interface).....	3-23
Altre opzioni per l'inserimento di eventi OCI	3-24
Suggerimenti per il debug di OCI.....	3-24

4 Installazione di Sentinel 5 per Oracle in Linux 4-1

Operazioni preliminari all'installazione di Sentinel 5 per Oracle in Linux.....	4-1
Per ottenere un codice di licenza	4-2
Database di Sentinel.....	4-3
Server Sentinel	4-4
Sentinel Control Center e Wizard	4-4
Advisor.....	4-4
Operazioni preliminari all'installazione di Oracle in Linux	4-4
Installazione di Sentinel 5 per Oracle in Linux.....	4-11
Installazione semplice in Linux	4-12
Installazione personalizzata in Linux	4-15
Installazione di Sentinel Control Center e Generatore servizi di raccolta in Windows	4-25
Operazioni successive all'installazione di Sentinel 5 per Oracle	4-26
Aggiornamento di e-mail Sentinel per l'autenticazione SMTP	4-26
Database di Sentinel.....	4-27
Servizio di raccolta.....	4-27
Aggiornamento del codice di licenza	4-28
Creazione di un'istanza Oracle per il database di Sentinel	4-28
Impostazione della strategia di inserimento eventi OCI (Oracle Call Interface).....	4-30
Altre opzioni per l'inserimento di eventi OCI	4-31
Suggerimenti per il debug di OCI.....	4-31

5 Installazione di Sentinel 5 per MS SQL 5-1

Operazioni preliminari all'installazione di Sentinel 5 MSSQL	5-1
Per ottenere un codice di licenza	5-2
Database di Sentinel.....	5-2
Server Sentinel	5-3
Sentinel Control Center e Wizard	5-4
Advisor.....	5-4
Installazione di Sentinel 5 per MS SQL	5-4
Installazione semplice.....	5-5
Installazione personalizzata.....	5-7
Operazioni successive all'installazione di Sentinel 5 per MS SQL	5-18
Aggiornamento di e-mail Sentinel per l'autenticazione SMTP	5-18
Database di Sentinel.....	5-19
Servizio di raccolta.....	5-19
Aggiornamento del codice di licenza	5-20
Istruzioni di configurazione per l'utilizzo dell'autenticazione di Windows di SQL Server con il driver JDBV DataDirect	5-20

Server di database SQL Server	5-20
Controller di dominio	5-21
Computer client	5-22
Impostazione della strategia di inserimento eventi ADO (Active Data Objects)	5-22
Prerequisiti per la strategia di caricamento ADO	5-23
Impostazione della strategia di inserimento degli eventi di caricamento ADO	5-23
Suggerimenti per il debug di ADO	5-23

6 Migrazione di dati e patch per Oracle in Solaris 6-1

Migrazione di dati e upgrade da v4.2 a v5.1.3	6-1
Server Sentinel	6-2
Gestione servizi di raccolta	6-3
Server Crystal Reporting	6-3
Server di database	6-3
Operazioni preliminari alla migrazione – Esportazione delle regole di correlazione	6-4
Operazioni preliminari alla migrazione – Backup degli script e delle configurazioni delle porte dei servizi di raccolta.	6-4
Operazioni preliminari alla migrazione – Disinstallazione della versione v4.2	6-5
Operazioni preliminari alla migrazione – Installazione del database di Sentinel 5	6-6
Migrazione	6-12
Operazioni successive alla migrazione – Installazione di Sentinel 5	6-14
Operazioni successive alla migrazione – Riconfigurazione degli script e delle configurazioni delle porte dei servizi di raccolta.	6-16
Operazioni successive alla migrazione – Configurazione di Sentinel 5 per Crystal Reporting	6-16
Patch da v5.x.x a v5.1.3	6-17
Aggiornamento del connettore syslog	6-17
Ulteriore aggiornamento da v5.0.x a v5.1.3	6-18
Aggiornamento delle autorizzazioni di gestione degli utenti per v5.0.x a v5.1.3	6-18
Aggiornamento delle opzioni di configurazione menu da v5.0.x a v5.1.3	6-19
Aggiornamento dell'opzione di visualizzazione server da v5.0.x a v5.1.3	6-19
Server Crystal Reporting	6-20
Aggiornamento di e-mail Sentinel per l'autenticazione SMTP	6-20

7 Migrazione di dati e patch per MS SQL 7-1

Migrazione di dati e upgrade da v4.2 a v5.1.3	7-1
Server Sentinel	7-2
Gestione servizi di raccolta	7-2
Server Crystal Reporting	7-3
Server di database	7-3
Operazioni preliminari alla migrazione – Esportazione delle regole di correlazione	7-4
Operazioni preliminari alla migrazione – Backup degli script e delle configurazioni delle porte dei servizi di raccolta.	7-4
Operazioni preliminari alla migrazione – Disinstallazione della versione v4.2	7-4
Operazioni preliminari alla migrazione – Installazione del database di Sentinel 5	7-5
Migrazione	7-11
Operazioni successive alla migrazione – Installazione di Sentinel 5	7-13
Operazioni successive alla migrazione – Riconfigurazione degli script e delle configurazioni delle porte dei servizi di raccolta.	7-16
Operazioni successive alla migrazione – Configurazione di Sentinel 5 per Crystal Reporting	7-16
Patch da v5.x.x a v5.1.3	7-16
Applicazione di patch a Sentinel da v5.x.x a v5.1.3 quando l'amministratore del database di Sentinel (esecdba) esegue il login con autenticazione di SQL Server	7-17
Applicazione di patch a Sentinel da v5.x.x a v5.1.3 quando l'amministratore del database di Sentinel (esecdba) esegue il login con autenticazione di Windows	7-17
Aggiornamento del connettore syslog	7-19
Aggiornamento delle autorizzazioni di gestione degli utenti per v5.0.x a v5.1.3	7-20

Server Crystal Reporting	7-21
Aggiornamento di e-mail Sentinel per l'autenticazione SMTP	7-21

8 Patch per Oracle in Linux 8-1

Patch da v5.1.1.1 a v5.1.3.....	8-1
Aggiornamento del connettore syslog.....	8-2
Server Crystal Reporting	8-2
Aggiornamento di e-mail Sentinel per l'autenticazione SMTP	8-2

9 Crystal Reports per Windows e Solaris 9-1

Panoramica	9-2
Requisiti del sistema	9-2
Requisiti di configurazione	9-2
Installazione di Microsoft Internet Information Server (IIS) e NET.ASP	9-3
Problemi noti	9-4
Uso di Crystal Reports	9-4
Panoramica relativa all'installazione	9-4
Panoramica relativa all'installazione di MS SQL 2000 Server con autenticazione di Windows	9-4
Panoramica relativa all'installazione di MS SQL 2000 Server con autenticazione SQL Server	9-5
Panoramica relativa all'installazione per Oracle	9-5
Installazione	9-5
Installazione di Crystal Server per MS SQL 2000 Server con autenticazione Windows	9-6
Installazione di Crystal Server per MS SQL 2000 Server con autenticazione SQL	9-11
Installazione di Crystal Server per Oracle.....	9-13
Configurazione per tutte le autenticazioni e configurazioni	9-16
Mappatura di Crystal Reports per l'utilizzo con Sentinel.....	9-16
Modelli di Crystal Reports	9-17
Pubblicazione di modelli di report mediante Crystal Publishing Wizard.....	9-18
Impostazione di un account 'Named User' (Utente denominato)	9-19
Configurazione di .NET Administration Launchpad	9-20
Abilitazione dei primi 10 rapporti di Sentinel	9-21
Ottimizzare la creazione di rapporti sugli eventi	9-22
Configurazione di Sentinel per l'integrazione con Crystal Enterprise Server	9-23

10 Crystal Reports per Linux 10-1

Uso di Crystal Reports	10-1
Configurazione	10-2
Installazione	10-2
Operazioni preliminari all'installazione di Crystal BusinessObjects Enterprise™ 11.....	10-2
Installazione di Crystal BusinessObjects Enterprise™ 11	10-4
Applicazione di patch in Crystal Reports per l'utilizzo con Sentinel.....	10-5
Pubblicazione di modelli di Crystal Reports	10-6
Pubblicazione di modelli di rapporti - Crystal Publishing Wizard (Pubblicazione guidata Crystal)	10-6
Pubblicazione di modelli di rapporti – Central Management Console (Console di gestione centrale).....	10-8
Uso del server Web di Crystal Server XI	10-9
Test della connettività al server Web	10-9
Impostazione di un account 'Named User' (Utente denominato).....	10-9
Configurazione dei rapporti	10-10
Abilitazione dei primi 10 rapporti di Sentinel.....	10-10
Aumentare al massimo la generazione di rapporti	10-11
Configurazione di Sentinel sul server Crystal Enterprise Server	10-12
Utility e soluzione dei problemi	10-13
Avvio di MySQL	10-13
Avvio di Tomcat	10-13

Avvio di Server Crystal Server	10-13
Errore del nome host Crystal	10-13
Impossibile connettersi a CMS	10-14
11 Configurazione di Advisor	11-1
Installazione di Advisor	11-1
Configurazione autonoma	11-1
Configurazione download Internet diretto	11-2
Installazione di Advisor	11-2
Importazione dei modelli di Crystal Reports	11-3
Configurazione di Administration Launchpad	11-3
Impostazione dell'integrazione di Sentinel Control Center con rapporti di Advisor	11-3
Aggiornamento dei dati nelle tabelle di Advisor	11-3
Ripristino della password di Advisor (solo download diretto)	11-4
12 Test dell'installazione	12-1
Test dell'installazione mediante i servizi di raccolta di prova	12-1
Configurazione dei servizi di raccolta di prova	12-4
Configurazione del servizio di raccolta SendOneEvent	12-4
Configurazione del servizio di raccolta SendMultipleEvents	12-4
Configurazione del servizio di raccolta DemoEvents	12-5
Configurazione del servizio di raccolta DemoAssetUpload	12-6
Configurazione del servizio di raccolta DemoVulnerabilityUpload	12-6
13 Modifiche al livello di comunicazione (iSCALE)	13-1
Modifiche delle chiavi di cifratura	13-1
14 Aggiunta di componenti a un'installazione esistente	14-1
Aggiunta di componenti in Solaris o Linux	14-1
Aggiunta di componenti in Windows	14-2
15 Disinstallazione del software	15-1
Disinstallazione di Sentinel, Gestione servizi di raccolta e Advisor	15-1
Disinstallazione per Solaris e Linux	15-1
Disinstallazione per Windows	15-1
Disinstallazione mediante il Pannello di controllo	15-2
Operazioni successive alla disinstallazione	15-2
A Questionario preliminare all'installazione	A-1
B Manutenzione relativa alle operazioni preliminari e successive all'installazione per il database Oracle in Solaris	B-1
Elenco di controllo relativo alle operazioni preliminari all'installazione	B-1
Manutenzione successiva all'installazione	B-4
C Manutenzione relativa alle operazioni preliminari e successive all'installazione per il database Oracle in Linux	C-1
Elenco di controllo relativo alle operazioni preliminari all'installazione	C-1
Manutenzione successiva all'installazione	C-4

D	Manutenzione preliminare e successiva all'installazione per il database MS SQL in Windows	D-1
	Elenco di controllo relativo alle operazioni preliminari all'installazione	D-1
	Manutenzione successiva all'installazione	D-3
E	Pulitura manuale delle installazioni precedenti	E-1
	Solaris	E-1
	Linux.....	E-2
	Windows.....	E-4

1

Introduzione

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questa guida verrà illustrata un'installazione di base. La *Guida dell'utente di Sentinel™ 5* include procedure più dettagliate sull'architettura, il funzionamento e l'amministrazione.

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.

Convenzioni utilizzate

Note e avvertenze

NOTA: le Note forniscono ulteriori informazioni che possono rivelarsi utili.

ATTENZIONE: le avvertenze forniscono ulteriori informazioni che possono essere utili per evitare danni al sistema o perdite di dati.

Comandi

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

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

Panoramica di Sentinel 5



Sentinel 5 include tutte le funzionalità che dovrebbe contenere una soluzione per la gestione delle informazioni di sicurezza. Oltre alle funzioni standard tra cui raccolta, aggregazione, correlazione e visualizzazione dei dati evento, Sentinel 5 consente di rispondere ai casi in maniera appropriata e decisiva mediante l'automazione e l'applicazione di processi di identificazione e risoluzione dei casi.

I cinque componenti principali di Sentinel 5 sono: iTRAC™, Active Views™ e iSCALE™ che consentono di gestire, misurare e restare conformi in maniera più efficiente. Con Sentinel 5 è possibile:

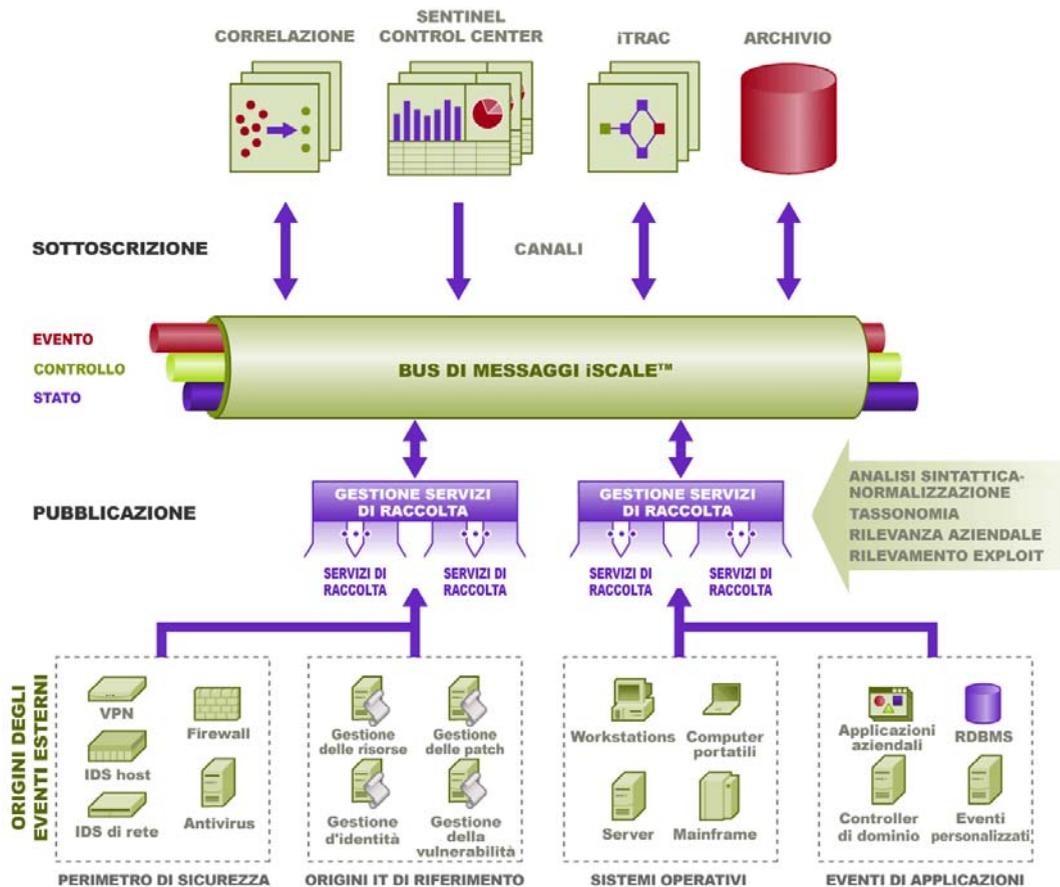
- Ottenere la visibilità e il controllo necessari per gestire l'ambiente di sicurezza in maniera più efficiente in termini di costo
- Rilevare e risolvere i casi più velocemente, pur riducendo i costi operativi
- Distribuire rapporti e sistemi di valutazione appropriati per valutare costantemente lo stato di sicurezza e conformità
- Ottenere e monitorare costantemente la conformità con le politiche interne e le normative legali.

Più operazioni con le risorse correnti eliminando i processi manuali

Sentinel 5 è costituito di più componenti che funzionano insieme per offrire una soluzione di primo piano nel mercato.

- Sentinel Control Center
- Server Sentinel
- Sentinel Advisor
- Gestione dati Sentinel
- Sentinel Wizard
 - Generatore servizi di raccolta di Wizard
 - Gestione servizi di raccolta di Wizard
 - Motore di Wizard

Nella sezione seguente è rappresentata un'**architettura concettuale** del prodotto Sentinel 5 e vengono illustrati i componenti di Sentinel coinvolti nella gestione della protezione.



Moduli del prodotto Sentinel

Sentinel 5 è costituito da tre moduli principali: Sentinel Control Center, Sentinel Wizard (Generatore servizi di raccolta e Gestione servizi di raccolta) e Sentinel Advisor.

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
- Amministratore: 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 rapporti: cronologia dei rapporti e delle misurazioni

Sentinel Wizard

Sentinel Wizard raccoglie i dati dai dispositivi di origine e fornisce un flusso di eventi più corposo immettendovi tassonomia, rilevamento di exploit e rilevanza business prima che gli eventi vengano collegati, 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. Tutte le configurazioni dovrebbero includere una o più procedure guidate per fornire ai clienti la possibilità di distribuire i componenti del prodotto nella propria infrastruttura in base alla topologia della rete in uso.

Sentinel Wizard consente di sviluppare e personalizzare in maniera efficiente i Servizi di raccolta. Ciò consente a Sentinel di raccogliere i dati da numerosi dispositivi all'interno di un'azienda. Questi dispositivi sono costituiti da (ma non limitati a):

- Sistemi di rilevamento delle intrusioni (host)
- Sistemi di rilevamento delle intrusioni (rete)
- Firewall
- Sistemi operativi
- Monitoraggio delle norme
- Autenticazione
- Router e switch
- VPN
- Antivirus
- Server Web
- Database
- Mainframe
- Valutazione delle vulnerabilità
- Servizi di directory
- Gestione di rete
- Sistemi proprietari

I componenti principali di Sentinel Wizard includono:

- Servizio di raccolta: un ricevitore che raccoglie e normalizza gli eventi non elaborati (raw) dai dispositivi e dai sistemi di sicurezza.
- Motore del servizio di raccolta: componente che elabora la logica dei modelli per ogni porta.
- Gestione servizi di raccolta: il componente back-end che gestisce i Servizi di raccolta e messaggi di stato del sistema ed esegue il filtro globale degli eventi.
- Generatore servizi di raccolta: un'applicazione autonoma che consente di creare e configurare Servizi di raccolta.

Sentinel Advisor

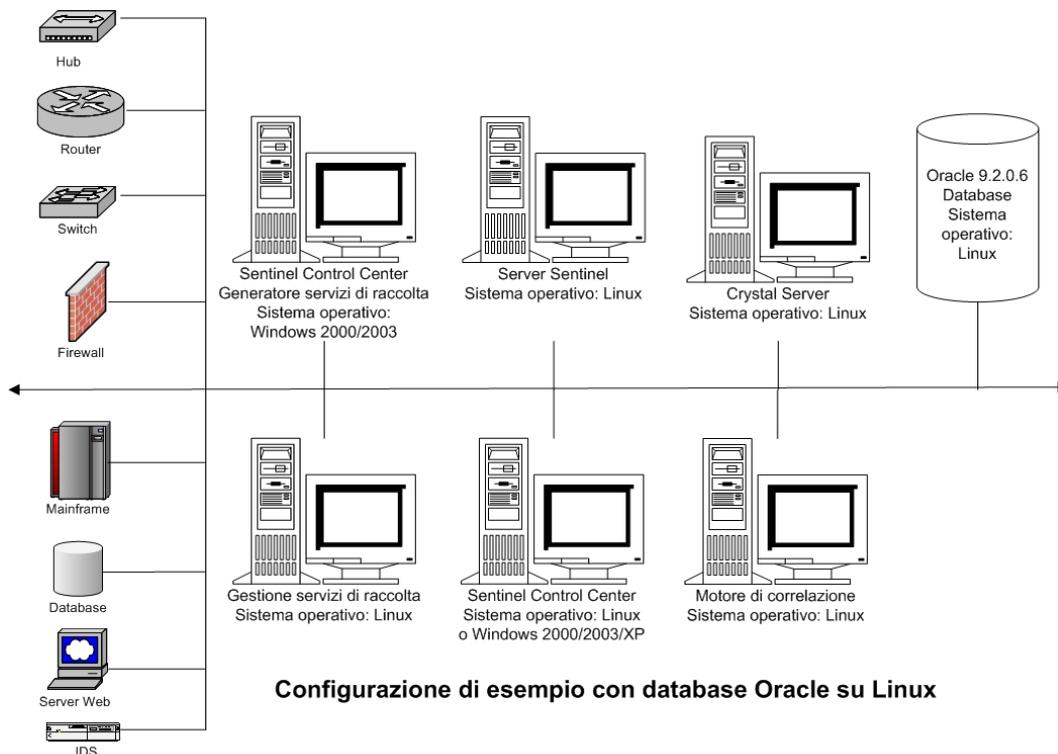
Sentinel Advisor è un modulo aggiuntivo opzionale che collega i dati degli avvisi in tempo reale di Sentinel alle informazioni sulle vulnerabilità e i rimedi noti.

Configurazione standard

Nella sezione seguente sono descritte le configurazioni standard del prodotto Sentinel 5 ed è illustrato come viene eseguita la Gestione della sicurezza. L'implementazione può variare in base all'ubicazione e alla modalità dell'installazione.

NOTA: per informazioni più specifiche su EPS (Eventi al secondo, Events per Second), piattaforme, RAM, requisiti di spazio HDD e CPU, vedere il *Capitolo 2: Procedure consigliate*.

Piattaforme supportate per il server Sentinel in Linux



Configurazione di esempio con database Oracle su Linux

NOTA: Linux fa riferimento a SUSE Linux 9 o Red Hat Enterprise Linux 3

NOTA: per informazioni specifiche sui sistemi operativi, vedere le tabelle seguenti.

Server Sentinel		
SO	Versione	Livello patch
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	Aggiornamento 5 ES (x86)

Database		
Database	Versione	Livello patch
Oracle a 64 bit Enterprise Edition	9i	<ul style="list-style-type: none"> ▪ 9.2.0.6 2617419 oppure ▪ 9.2.0.7

NOTA: per ulteriori informazioni relative a Critical Patch 2617419, vedere il sito Web Oracle e il portale del servizio clienti Novell.

Sentinel Control Center (Interfaccia utente)		
SO	Versione	Livello patch
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

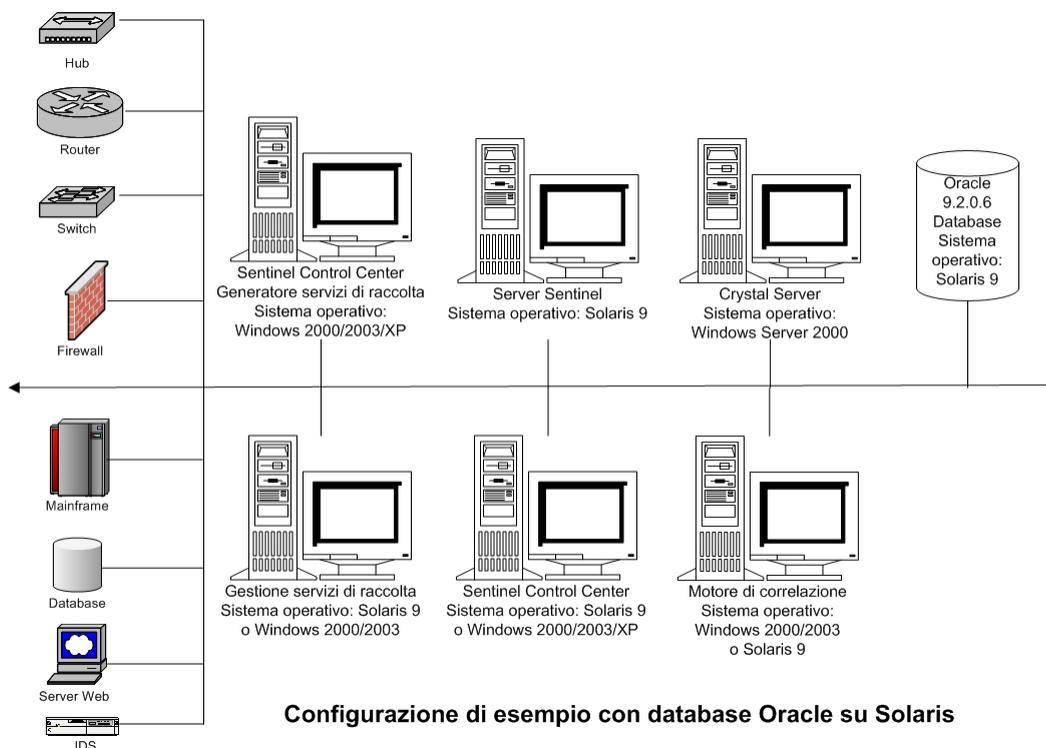
Generatore servizi di raccolta		
SO	Versione	Livello patch
Windows	2000	SP4
Windows	2003	SP1

Gestione servizi di raccolta		
SO	Versione	Livello patch
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Solaris 9 Recommended Patch Cluster DATA: 3 maggio 05
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)

Crystal Server (Scelta di due versioni [Linux (SLES/Red Hat) e Windows])			
Versione Crystal	SO	Versione sistema operativo	Livello patch sistema operativo
Crystal BusinessObjects Enterprise™ 11	SuSE Linux Enterprise Server 9 (SLES 9)	9	
Crystal BusinessObjects Enterprise™ 11	Red Hat Enterprise Linux	3	3 Update 5 ES (x86)
Crystal BusinessObjects Enterprise™ 11	Windows con MS SQL 2000. Sentinel 5 non supporta MSDE.	Windows Server 2003	SP1

NOTA: Sentinel 5 non supporta Crystal XI in Windows® 2000 Server e MSDE.

Piattaforme supportate per il server Sentinel in Solaris



NOTA: per informazioni specifiche sui sistemi operativi, vedere le tabelle seguenti.

Server Sentinel		
SO	Versione	Livello patch
Solaris Enterprise Edition	9	Solaris 9 Recommended Patch Cluster DATA: 3 maggio 05

Database		
Database	Versione	Livello patch
Oracle a 64 bit	9i	<ul style="list-style-type: none"> ▪ 9.2.0.6 2617419 oppure ▪ 9.2.0.7

NOTA: per ulteriori informazioni relative a Critical Patch 2617419, vedere il sito Web Oracle e il portale del servizio clienti Novell.

Sentinel Control Center (Interfaccia utente)		
SO	Versione	Livello patch
Solaris	9	Solaris 9 Recommended Patch Cluster DATA: 3 maggio 05
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

Generatore servizi di raccolta		
SO	Versione	Livello patch
Windows	2000	SP4
Windows	2003	SP1

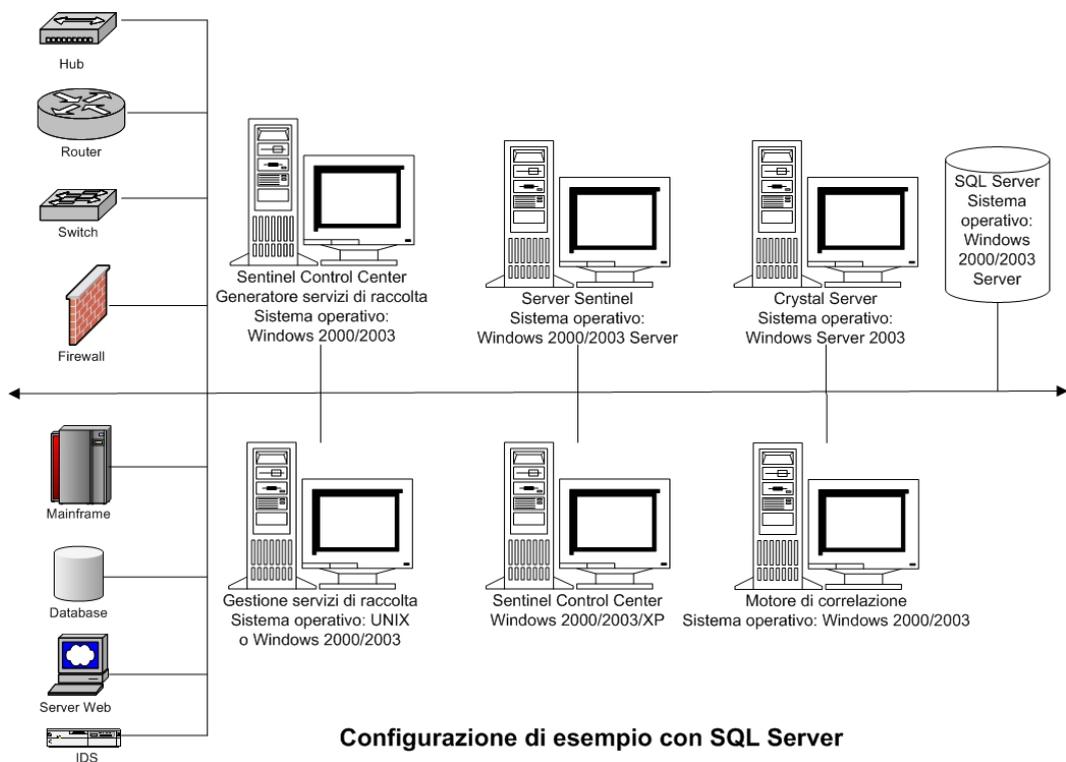
Gestione servizi di raccolta		
SO	Versione	Livello patch
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Solaris 9 Recommended Patch Cluster DATA: 3 maggio 05
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)

Crystal Server			
Versione Crystal	SO	Versione sistema operativo	Livello patch sistema operativo
Crystal BusinessObjects Enterprise™ 11	Windows con MS SQL 2000. Sentinel 5 non supporta MSDE.	Windows Server 2003	SP1

NOTA: Crystal Reports v9 è supportato in Sentinel v5.1 e versioni precedenti oltre che in Sentinel v5.1.1 SP1 e versioni successive. Non è supportato su Sentinel v5.1.1 senza SP1. Se si utilizza Crystal Reports v9 e Sentinel v5.1.1, è necessario applicare Sentinel v5.1.1 Service Pack 1 o eseguire l'upgrade a v5.1.2.

NOTA: Sentinel 5 non supporta Crystal XI in Windows® 2000 Server.

Piattaforme supportate per il server Sentinel in Windows



NOTA: per informazioni specifiche sui sistemi operativi, vedere le tabelle seguenti.

Server Sentinel		
SO	Versione	Livello patch
Windows	2000 Server - Enterprise Edition	SP4
Windows	2003 Server - Enterprise Edition	SP1

Database		
Database	Versione	Livello patch
SQL Server:	2000 Enterprise	SP3a
SQL Server:	2005 Enterprise (Sentinel v5.1.1 SP1 e successive)	

Sentinel Control Center (Interfaccia utente)		
SO	Versione	Livello patch
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

Generatore servizi di raccolta		
SO	Versione	Livello patch
Windows	2000	SP4
Windows	2003	SP1

Gestione servizi di raccolta		
SO	Versione	Livello patch
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Solaris 9 Recommended Patch Cluster DATA: 3 maggio 05
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)

Crystal Server			
Versione Crystal	SO	Versione sistema operativo	Livello patch sistema operativo
Crystal BusinessObjects Enterprise™ 11	Windows con MS SQL 2000. Sentinel 5 non supporta MSDE.	Windows Server 2003	SP1

NOTA: Crystal Reports v9 è supportato in Sentinel v5.1 e versioni precedenti oltre che in Sentinel v5.1.1 SP1 e versioni successive. Non è supportato su Sentinel v5.1.1 senza SP1. Se si utilizza Crystal Reports v9 e Sentinel v5.1.1, è necessario applicare Sentinel v5.1.1 Service Pack 1 o eseguire l'upgrade a v5.1.2.

NOTA: Sentinel 5 non supporta Crystal XI in Windows® 2000 Server.

Altri riferimenti Novell

Sono disponibili i manuali seguenti con i CD di installazione di Sentinel.

- Guida all'installazione di Sentinel™
- Guida dell'utente di Sentinel™
- Guida dell'utente di Sentinel™ Wizard
- Guida di riferimento dell'utente di Sentinel™
- Guida all'integrazione di terze parti di Sentinel™
- Note di rilascio

Come contattare Novell

- Sito Web: <http://www.novell.com>
- Supporto tecnico Novell: <http://www.novell.com/support/index.html>
- Supporto tecnico Novell internazionale:
http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Supporto in autonomia:
http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Per supporto 24x7, 800-858-4000

2

Procedure consigliate

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo vengono trattati le procedure consigliate e i suggerimenti per utilizzare Sentinel nel modo migliore. Gli argomenti trattati sono i seguenti:

- Procedure consigliate per l'installazione
 - [Requisiti hardware](#)
 - [Configurazione di array di dischi](#)
 - [Configurazione di rete](#)
 - [Installazione di Oracle e MS SQL Server](#)
 - [Patch del database di Sentinel](#)
 - [Impostazioni del kernel UNIX consigliate](#)
 - [Parametri di configurazione per la creazione di un'istanza di database](#)
 - [Installazione di Sentinel](#)
 - [Ottimizzazione della creazione di rapporti su eventi](#)
 - [Rapporti disponibili in Sentinel](#)
 - [Suggerimenti per lo sviluppo di Crystal Reports personalizzati](#)
- Procedure consigliate per la manutenzione
 - [Analisi del database](#)
 - [Verifica dello stato del database](#)
 - [Automazione dell'archiviazione dei dati e dell'aggiunta di partizioni \(solo Windows\)](#)
 - [Motore di correlazione](#)
 - [Log delle transazioni](#)
 - [Ubicazioni di log](#)

Procedure consigliate per l'installazione

Nella tabella seguente sono riportati i valori delle prestazioni per gli attributi specifici di Sentinel.

Attributo	Classificazione	Commenti
▪ EPS per l'inserimento del database degli eventi	1250	L'inserimento è influenzato dalle regole di correlazione e dal servizio di mappatura.
▪ EPS per ogni istanza di Gestione servizi di raccolta	350	
▪ EPS per servizio di raccolta (Checkpoint, Win2K, ecc...)	300	
▪ Numero massimo di Servizi di raccolta supportato da Gestione servizi di raccolta	10	

Attributo	Classificazione	Commenti
▪ Numero massimo di Manager di servizi di raccolta per istanza Sentinel	20	
▪ Numero di regole distribuite per motore di correlazione	20-80	EPS basso (150 EPS) = 80 EPS alto (1250 EPS) = 20
▪ Numero di istanze Active Views™ per istanza Sentinel	35 - 50	
▪ Numero massimo di utenti simultanei	20	
▪ Numero massimo di visualizzazione per Sentinel Control Center	10	
▪ Numero massimo di mappature per Sentinel	10	
▪ Dimensioni massime di ogni mappatura	10 MB	
▪ Numero massimo di righe per mappatura	350k	

La specifica di riferimento CPU è basata su:

- Windows - Xeon 3,2 GHz
- SuSE Linux – Xeon 3,2 GHz
- Solaris - Sparc-3 1,1 GHz
- Linux – Xeon 3,2 GHz

La configurazione è valida per i sistemi operativi seguenti:

- Windows 2000 Server con SP4
- Windows 2003 Server con SP1
- SuSE Linux Enterprise Server 9 (SLES 9)
- Solaris 9 con patch con la versione Generic_112233-11 del cluster di patch consigliato
- Red Hat Enterprise Linux 3 Update 5 ES (x86)

Il database è uno dei seguenti:

- MSSQL 2000 con SP3a
- Oracle 9i Enterprise Edition 9.2.0.6 o 9.2.0.7 con partizionamento

Configurazione semplice autonoma (utilizzo demo)

Questa installazione installa tutti i componenti (incluso il database) in un'unica piattaforma. Questa operazione è eseguita principalmente a scopo dimostrativo. Non è consigliabile eseguirla per l'uso attuale. I requisiti hardware sono:

Componenti	Minimo		Consigliato	
	RAM (GB)	CPU	RAM (GB)	CPU
Computer 1	2	2	4	2
<ul style="list-style-type: none"> ▪ Tutti i componenti di Sentinel ▪ Gestione servizi di raccolta ▪ Servizi di raccolta ▪ Database ▪ Array di dischi 				

Componenti	Minimo		Consigliato	
	RAM (GB)	CPU	RAM (GB)	CPU
In Windows: <ul style="list-style-type: none"> ▪ Crystal Server ▪ Generatore servizi di raccolta Per Linux: <ul style="list-style-type: none"> ▪ Crystal Server 				
Computer 2 (solo per installazioni UNIX) Per Solaris: <ul style="list-style-type: none"> ▪ Crystal Server ▪ Generatore servizi di raccolta (Windows) Per Linux: <ul style="list-style-type: none"> ▪ Generatore servizi di raccolta (Windows) 	1.0	1	2.0	2

Installazione di prova: Configurazione autonoma

Questa installazione installa tutti i componenti, tranne il database, in un'unica piattaforma. Questa configurazione viene generalmente utilizzare come prova per testare le funzionalità sotto carichi normali. In questo caso, il database viene eseguito in un computer separato dal resto dei processi Sentinel.

Componenti	Minimo		Consigliato	
	RAM (GB)	CPU	RAM (GB)	CPU
Computer 1 <ul style="list-style-type: none"> ▪ Tutti i componenti di Sentinel ▪ Gestione servizi di raccolta ▪ Servizi di raccolta In Windows: <ul style="list-style-type: none"> ▪ Crystal Server ▪ Generatore servizi di raccolta Per Linux: <ul style="list-style-type: none"> ▪ Crystal Server 	4.0	2	4	4
Computer 2 <ul style="list-style-type: none"> ▪ Database ▪ Array di dischi 	4	2	4	4
Computer 3 (solo per installazioni UNIX) Per Solaris: <ul style="list-style-type: none"> ▪ Crystal Server ▪ Generatore servizi di raccolta (Windows) Per Linux: <ul style="list-style-type: none"> ▪ Generatore servizi di raccolta (Windows) 	2.0	2	4.0	2

Produzione: Configurazione distribuita

Una configurazione distribuita corrisponde a un'installazione personalizzata progettata per i sistemi standard e aziendali.

Poiché Sentinel dispone di 8 componenti separati oltre a Crystal Reports, è possibile generare numerose configurazioni differenti. Vengono illustrate due diverse configurazioni.

Poiché il database dipende dall'IO è consigliabile installare il database in un computer separato. Il server del database richiede un'array di risorse di memorizzazione ad alta velocità che soddisfi i requisiti di IO in base alla frequenza di inserimento degli eventi.

Gli host distribuiti devono essere connessi agli altri host del server Sentinel tramite un singolo switch ad alta velocità (GIGE) allo scopo di impedire colli di bottiglia nel traffico di rete.

Produzione – Configurazione distribuita (Opzione 1)

Configurazione a 4 computer

Componenti	Minimo		Consigliato	
	RAM (GB)	CPU	RAM (GB)	CPU
Computer 1 <ul style="list-style-type: none">▪ Motore di correlazione▪ DAS▪ iSCALE (Bus messaggi)▪ Advisor	4.0	4	8.0	8
Computer 2 <ul style="list-style-type: none">▪ Gestione servizi di raccolta▪ Servizi di raccolta	1.0	2	2.0	2
Computer 3 <ul style="list-style-type: none">▪ Crystal Server	2.0	2	4.0	4
Computer 4 <ul style="list-style-type: none">▪ Database▪ Array di dischi	4	4	16	8

Produzione – Configurazione distribuita (Opzione 2)

Configurazione a 5 computer

Componenti	Minimo		Consigliato	
	RAM (GB)	CPU	RAM (GB)	CPU
Computer 1 <ul style="list-style-type: none">▪ DAS▪ iSCALE (Bus messaggi)▪ Advisor	4.0	4	8.0	8
Computer 2 <ul style="list-style-type: none">▪ Motore di correlazione	1.0	2	2.0	2
Computer 3 <ul style="list-style-type: none">▪ Gestione servizi di raccolta▪ Servizi di raccolta	1.0	2	2.0	2

Componenti	Minimo		Consigliato	
	RAM (GB)	CPU	RAM (GB)	CPU
Computer 4 ▪ Crystal Server	2.0	2	4.0	4
Computer 5 ▪ Database ▪ Array di dischi	4	4	16	8

Norme di supporto delle patch

Sentinel certificherà le patch del database e dei sistemi operativi entro 60 giorno dalla pubblicazione.

Indicazioni sull'hardware

Server Sentinel Motore di correlazione			
EPS	RAM	Spazio	CPU
250	2 GB	72 GB	Windows - 2 x 3.0 GHz Xeon SuSE Linux o Redhat Linux – Xeon 2 x 3,0 GHz Solaris - V280 2 x 1.1 GHz Ultra Sparc III
500	4 GB	72 GB	Windows - 4 x 3.0 GHz Xeon SuSE Linux o Redhat Linux – Xeon 4 x 3,0 GHz Solaris - V480 4 x 1.1 GHz Ultra Sparc III
1000+	8 GB	72 GB	Windows - 8 x 3.0 GHz Xeon SuSE Linux o Redhat Linux – Xeon 8 x 3,0 GHz Solaris - V880 8 x 1.1 GHz Ultra Sparc III

Gestione servizi di raccolta			
EPS	RAM	Spazio	CPU
250	2 GB	36 GB	Windows - 2 x 3.0 GHz Xeon SuSE Linux o Redhat Linux – Xeon 2 x 3,0 GHz Solaris - V280 2 x 1.1 GHz Ultra Sparc III
350+	4 GB	36 GB	Windows - 4 x 3.0 GHz Xeon SuSE Linux o Redhat Linux – Xeon 4 x 3,0 GHz Solaris - V480 4 x 1.1 GHz Ultra Sparc III

Sentinel Control Center Generatore servizi di raccolta (solo Windows) Gestione dati Sentinel			
RAM	Spazio	CPU	
2 GB	15 GB	Windows 2000 o 2003 - 2 Xeon a 3,0 GHz Windows XP (solo Control Center) – Xeon 2 x 3,0 GHz SuSE Linux o Redhat Linux – Xeon 2 x 3,0 GHz Sun Solaris 9 - V280 2 x 1.1 GHz Ultra Sparc III	

Database			
EPS	RAM	Spazio	CPU
250	8 GB	500 GB	Windows - 4 x 3.0 GHz Xeon SuSE Linux o Redhat Linux – Xeon 4 x 3,0 GHz Solaris - V480 4 x 1.1 GHz Ultra Sparc III

Database			
EPS	RAM	Spazio	CPU
500	12 GB	1.0 TB	Windows - 4 x 3.0 GHz Xeon SuSE Linux o Redhat Linux – Xeon 4 x 3,0 GHz Solaris - V880 6 x 1.1 GHz Ultra Sparc III
1000+	16 GB	2,0 TB	Windows - 8 x 3.0 GHz Xeon SuSE Linux o Redhat Linux – Xeon 8 x 3,0 GHz Solaris - V880 8 x 1.1 GHz Ultra Sparc III

Configurazione dell'array di dischi

Per il server Novell Sentinel 5 in un ambiente di produzione è necessario un array di dischi ad alta velocità per gli host del database e di Sentinel. In questa sezione vengono trattati i consigli su una tipica configurazione di dischi (RAID). Nell'elenco seguente sono riportati i componenti principali che vengono influenzati dalle prestazioni dell'hardware del disco:

- Componente del database (MSSQL/Oracle): Sono influenzati la frequenza degli Eventi al secondo (Events per Second; EPS) e le funzionalità di Interrogazione (prestazioni di Interrogazione rapida / Crystal performance).
- DAS-RT (Data Access Service Real Time Component): Viene influenzata la funzione Active Views.
- DAS-Aggregation: Viene influenzato il numero di riepiloghi che è possibile attivare.

Requisiti minimi per l'installazione Enterprise (1000 EPS o più)

È consigliabile utilizzare almeno una configurazione RAID 5, la più efficiente in termini di costo. Questa configurazione non sacrifica alcune prestazioni e la ridondanza in termini di costo. Si noti tuttavia che questi sono solo suggerimenti e devono essere utilizzati come guida. Per le installazioni di produzione aziendali su vasta scala è necessaria un'analisi più dettagliata dei requisiti di velocità, velocità effettiva e ridondanza.

- Gruppo RAID 1 – DB (Dati, indici, log delle transazioni e così via)
- RAID gruppo 2 – DAS del server Sentinel (dir Dati, DIR* Temp)
- Dischi minimi: 13 per gruppo di RAID
- Tipo di disco: 12k+ RPM, Fiber Channel o SCSI
- LUN 1 (RAID Gruppo 1): 5 GB - 144 GB+ per disco
- LUN 2 (RAID Gruppo 2): 5 GB - 144 GB+ per disco

Configurazione ottimale

Per una configurazione ottimale delle prestazioni e della ridondanza, è possibile utilizzare un gruppo RAID 1+0 con le stesse impostazioni sopra menzionate. Può essere tuttavia necessario disporre di gruppi RAID e LUN che seguono le stesse linee guida sopra illustrate per ottenere maggiore parallelismo e IO per determinati database.

NOTA: Per istruzioni su come fare in modo che la DIR TEMP DAS faccia riferimento a un'altra ubicazione, vedere la sezione [Installazione di Sentinel](#).

Esempio di una configurazione di dispositivi di memorizzazione per un'installazione MS SQL

Nell'esempio seguente viene utilizzato il sottosistema di memorizzazione EMC² CLARiiON con:

- 1 TB di spazio di memorizzazione
- 60 unità, 36 GB, 15K RPM

Gruppi RAID

Array	Gruppo RAID	Numero di unità	Unità assegnate (bus, chassis, disco)	Nome
1	0	8	0-0-13, 0-0-14, 1-0-13, 1-0-14, 2-0-13, 2-0-14, 3-0-13, 3-0-13	Gruppo 0 RAID
1	1	8	0-0-11, 0-0-12, 1-0-11, 1-0-12, 2-0-11, 2-0-12, 3-0-11, 3-0-12	Gruppo 1 RAID
1	2	8	0-0-9, 0-0-10, 1-0-9, 1-0-10, 2-0-9, 2-0-10, 3-0-9, 3-0-10	Gruppo 2 RAID
1	3	8	0-0-7, 0-0-8, 1-0-7, 1-0-8, 2-0-7, 2-0-8, 3-0-7, 3-0-8	Gruppo 3 RAID
1	4	8	0-0-5, 0-0-6, 1-0-5, 1-0-6, 2-0-5, 2-0-6, 3-0-5, 3-0-6	Gruppo 4 RAID
1	5	8	0-0-3, 0-0-4, 1-0-3, 1-0-4, 2-0-3, 2-0-4, 3-0-3, 3-0-4	Gruppo 5 RAID
1	6	12	0-0-0, 0-0-1, 0-0-2, 1-0-0, 1-0-1, 1-0-2, 2-0-0, 2-0-1, 2-0-2, 3-0-0, 3-0-1, 3-0-2	Gruppo 6 RAID

Assegnazioni LUN

Array	LUN	Tipo RAID	Gruppo RAID	Dimensioni (GB)	Processore di memorizzazione	Nome
1	0	0	0	263	A	LUN 0
1	1	0	1	263	B	LUN 1
1	2	0	2	263	A	LUN 2
1	3	0	3	263	B	LUN 3
1	4	0	4	263	A	LUN 4
1	5	0	5	214	B	LUN 5
1	6	0	6	160	A	LUN 6
1	7	0	6	160	B	LUN 7

Gruppi di memorizzazione

Array	Gruppo di memorizzazioni	LUN	Host	Lettera unità	Nome
1	Sentinel	0	E2P0 (E3P0)	E:	SQLData1
1	Sentinel	1	E2P0 (E3P0)	F:	SQLData2
1	Sentinel	2	E2P0 (E3P0)	G:	SQLData3
1	Sentinel	3	E2P0 (E3P0)	H:	SQLData4
1	Sentinel	4	E2P0 (E3P0)	I:	SQLIndex1
1	Sentinel	5	E2P0 (E3P0)	J:	SQLIndex2
1	Sentinel	6	E2P0 (E3P0)	L:	SQLLog
1	Sentinel	7	E2P0 (E3P0)	T:	TempDB

Esempio di una configurazione di memorizzazione per Oracle

volume 1	RAID 1	Home di Oracle
volume 2	RAID 1	log di ripetizione membro a
volume 3	RAID 1	log di ripetizione membro b
volume 4	RAID 0+1 o RAID 5	Spazi delle tabelle temporanei e di annullamento
volume 5	RAID 0+1 o RAID 5	Spazi delle tabelle dei dati Sentinel
volume 6	RAID 0+1 o RAID 5	Spazi delle tabelle di indice Sentinel
volume 7	RAID 0+1 o RAID 5	Spazi delle tabelle dei dati Sentinel
volume 8	RAID 0+1 o RAID 5	Spazi delle tabelle di indice riepilogo Sentinel
volume 9	RAID 1	file log di archivio

Configurazione di rete

Componenti del server Sentinel: Questi componenti devono essere collegati tra di loro mediante un unico switch da 1 GB che include Database, Communication Server, Advisor, Servizi di base Sentinel, Motore di correlazione e DAS.

Sentinel Control Center, Generatore servizi di raccolta e Gestione servizi di raccolta. È necessario connettere questi componenti al server Sentinel mediante switch FULL DUPLEX di almeno 100 Mbit.

Installazione del server Oracle e MS SQL

NOTA: È possibile modificare quasi tutti i parametri di installazione del database dopo che questo viene installato mediante Enterprise Manager o la riga di comando.

1. Per motivi connessi alle prestazioni, a seconda che si stia eseguendo l'installazione in RAID e che l'ambiente RAID lo consenta, è necessario installare i log seguenti nel disco con scrittura più veloce disponibile.
 - Redo log (Oracle)
 - Log delle transazioni (MS SQL)
2. Per determinare in maniera più accurata le dimensioni del database, può essere opportuno iniziare con un piccolo database e quindi estenderne le dimensioni dopo aver avviato ed eseguito il sistema per un breve periodo. Ciò consente di osservare lo sviluppo del database in base alla frequenza di inserimento degli eventi e quindi determinare i requisiti dello spazio del database del sistema.
3. Per motivi di ripristino, è consigliabile eseguire regolarmente backup pianificati del database.
4. Nel caso delle installazioni Oracle, il programma di installazione Sentinel disattiva per default la registrazione nell'archivio. 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 per evitare che il database interrompa l'accettazione degli eventi se la capacità della destinazione dei log di archiviazione si esaurisce.
5. Per motivi correlati alle prestazioni, le ubicazioni di memorizzazione dovrebbero fare riferimento a posizioni diverse per evitare conflitti di I/O.
 - Directory dati
 - Directory indice
 - Directory dati di riepilogo

- Directory indice di riepilogo
- Directory log (solo MS SQL)
- Directory dei file temporanei e dello spazio delle tabelle di annullamento (solo Oracle)
- Directory log di ripetizione membro A (solo Oracle)
- Directory log di ripetizione membro B (solo Oracle)

Patch del database Sentinel

Solo nel caso di MS SQL, quando si applicano patch al database di Sentinel, verranno aggiunti nuovi indici solo in *_P_MAX. Le partizioni già esistenti non verranno aggiornate. Per migliorare le prestazioni delle interrogazioni in esecuzione sulle partizioni esistenti, è quindi necessario aggiungere gli indici manualmente a queste partizioni.

Impostazioni consigliate per il kernel UNIX

I seguenti sono i valori minimi consigliati. Per ulteriori informazioni consultare la documentazione del sistema e di Oracle.

valori minimi dei parametri del kernel per Linux

Per ulteriori informazioni su come visualizzare e impostare i parametri del kernel, vedere *la sezione Installazione di Sentinel 5 per Oracle – Operazioni preliminari all'installazione di Oracle in Linux nel capitolo 3*.

```
shmmax=2147483648 (valore minimo)
shmmni=4096
semmns=32000
semmni=1024
semmsl=1024
semopm=100
```

Valori minimi dei parametri del kernel per Solaris

Selezionare i parametri del kernel UNIX per Oracle in /etc/system e impostare i valori seguenti:

```
shmmax=4294967295
shmmni=1
shmseg=50
shmmni=400
semmns=14000
semmni=1024
semmsl=1024
shmopm=100
shmvmx=32767
```

Configurazione di parametri durante la creazione di un'istanza personale del database

Nella tabella seguente sono riportate le impostazioni consigliate durante la creazione di un'istanza personale del database. Le impostazioni possono variare in base alla configurazione e ai requisiti del sistema.

Nell'istanza Oracle sarà necessario creare:

- I parametri di inizializzazione di Oracle (questi valori dipendono dalle dimensioni e dalla configurazione del sistema in uso)
- I parametri di configurazione per gli spazi delle tabelle necessari a Sentinel per Solaris e Linux

Parametri consigliati per la configurazione minima	
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
optimizer_index_caching	50
optimizer_index_cost_adj	55

Parametri minimi per le dimensioni dello spazio delle tabelle		
Spazio delle tabelle	Dimensioni esempio	Note
REDO	3 x 100 M	<ul style="list-style-type: none"> ▪ Corrisponde al valore minimo. Nel caso di EPS elevato creare log di ripetizione di dimensioni maggiori.
SYSTEM	500 M	<ul style="list-style-type: none"> ▪ Valore minimo
TEMP	1 G	<ul style="list-style-type: none"> ▪ Valore minimo
UNDO	1 G	<ul style="list-style-type: none"> ▪ Valore minimo
ESENTD	5 G	<ul style="list-style-type: none"> ▪ Valore minimo ▪ Per i dati evento
ESENTD2	500 M	<ul style="list-style-type: none"> ▪ Valore minimo ▪ Dati per configurazione, risorse, vulnerabilità e associazioni (estensione automatica abilitata)
ESENTWFD	250 M	<ul style="list-style-type: none"> ▪ Per dati di iTrac (estensione automatica abilitata)
ESENTWFX	250 M	<ul style="list-style-type: none"> ▪ Per l'indice di iTrac (estensione automatica abilitata)
ESENTX	3 G	<ul style="list-style-type: none"> ▪ Valore minimo ▪ Per indice evento

Parametri minimi per le dimensioni dello spazio delle tabelle		
Spazio delle tabelle	Dimensioni esempio	Note
ESENTX2	500 M	<ul style="list-style-type: none"> ▪ Valore minimo ▪ Indice per configurazione, risorse, vulnerabilità e associazioni (estensione automatica abilitata)
SENT_ADVISORD	200 M	<ul style="list-style-type: none"> ▪ Valore minimo ▪ Per dati di Advisor (estensione automatica abilitata)
SENT_ADVISORX	100 M	<ul style="list-style-type: none"> ▪ Valore minimo ▪ Per indice di Advisor (estensione automatica abilitata)
SENT_LOBS	100 M	<ul style="list-style-type: none"> ▪ Valore minimo ▪ Per oggetti di database di grandi dimensioni (estensione automatica abilitata)
SENT_SMRYD	3 G	<ul style="list-style-type: none"> ▪ Valore minimo ▪ Per aggregazione, dati di riepilogo
SENT_SMRYX	2 G	<ul style="list-style-type: none"> ▪ Valore minimo ▪ Per aggregazione, indice di riepilogo

Installazione di Sentinel

Quando si installa Sentinel, è necessario tenere considerare gli aspetti seguenti per le prestazioni e il backup.

1. Quando si esegue un'installazione completa di Sentinel dopo aver rimosso una precedente versione di Sentinel installata, è vivamente necessario rimuovere alcuni file e impostazioni del sistema che possono essere rimasti dalla precedente installazione. Se non si rimuovono tali file, la nuova installazione completa potrebbe non riuscire. Questa operazione deve essere eseguita su ogni computer sul quale si sta eseguendo una nuova installazione. Per ulteriori informazioni sui file che è necessario rimuovere, vedere *l'Appendice E*.
2. Le prestazioni di Active Views e di Mappatura possono migliorare notevolmente se la directory temporanea dei processi DAS_RT e DAS_Query fa riferimento a un disco veloce, ad esempio a un array di dischi. Per fare in modo che la directory temporanea faccia riferimento a un disco veloce, eseguire le operazioni seguenti sul computer in cui è installato DAS.
 - a. Creare una directory sul disco veloce in cui archiviare i file temporanei. In un sistema UNIX, questa directory deve appartenere ed essere scrivibile da parte dell'utente esecadm e del gruppo exec.
 - b. Creare una copia di backup del file %ESEC_HOME%\configuration.xml.
 - c. Aprire il file %ESEC_HOME%\configuration.xml in un editor di testo.
 - d. Per i processi DAS_RT e DAS_Query aggiungere l'argomento JVM java.io.tmpdir impostandolo sulla directory appena creata.
 - e. Per apportare questa modifica al processo DAS_RT, individuare la riga che contiene il testo
-Dsrv_name=DAS_RT

e aggiungere l'argomento

```
-Djava.io.tmpdir=<tmp_directory>
```

subito dopo. Un esempio di come dovrebbe apparire la riga (gli argomenti -Xmx, -Xms e -XX possono essere diversi) è:

```
<process component="DAS"
  image="&quot;$(ESEC_JAVA_HOME)/java&quot;; -server -
  Dsrv_name=DAS_RT -Djava.io.tmpdir=D:\Temp2 -Xmx310m
  -Xms103m -XX:+UseParallelGC -Xss128k -Xrs -
  Desecurity.dataobjects.config.file=/xml/BaseMetaDat
  a.xml -
  Djava.util.logging.config.file=../config/das_rt_log
  .prop -
  Dcom.esecurity.configurationfile=../../configuratio
  n.xml -
  Djava.security.auth.login.config=../config/auth.log
  in -Djava.security.krb5.conf=../../lib/krb5.conf -
  jar ../../lib/ccsbase.jar ../config//das_rt.xml"
  min_instances="1" post_startup_delay="5"
  shutdown_command="cmd //C
  &quot;$(ESEC_HOME)/sentinel/scripts/stop_container.
  bat&quot;; localhost DAS_RT"
  working_directory="$(ESEC_HOME)/sentinel/bin"/>
```

- f. Per apportare questa modifica al processo DAS_Query, individuare la riga che contiene il testo

```
-Dsrv_name=DAS_Query
```

e aggiungere l'argomento

```
-Djava.io.tmpdir=<tmp_directory>
```

subito dopo. Un esempio di come dovrebbe apparire la riga (gli argomenti -Xmx, -Xms e -XX possono essere diversi) è:

```
<process component="DAS"
  image="&quot;$(ESEC_JAVA_HOME)/java&quot;; -server -
  Dsrv_name=DAS_Query -Djava.io.tmpdir=D:\Temp2 -
  Xmx256m -Xms85m -XX:+UseParallelGC -Xss128k -Xrs -
  Desecurity.dataobjects.config.file=/xml/BaseMetaDat
  a.xml,/xml/WorkflowMetaData.xml -
  Djava.util.logging.config.file=../config/das_query_
  log.prop -
  Djava.security.auth.login.config=../config/auth.log
  in -Djava.security.krb5.conf=../../lib/krb5.conf -
  Desecurity.execution.config.file=../config/executio
  n.properties -
  Dcom.esecurity.configurationfile=../../configuratio
```

```
n.xml -jar ../../lib/ccsbase.jar
  ../../config//das_query.xml" min_instances="1"
post_startup_delay="5" shutdown_command="cmd //C
  &quot;$(ESEC_HOME)/sentinel/scripts/stop_container.
bat&quot; localhost DAS_Query"
working_directory="$(ESEC_HOME)/sentinel/bin"/>
```

Aumentare al massimo la generazione di rapporti di eventi 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 report sarà necessario riconfigurare Crystal Page Server.

Riconfigurazione di Crystal Page Server (solo Windows Crystal Server)

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 Page Server* quindi scegliere *Interrompi*.
3. Fare clic con il pulsante destro del mouse su *Crystal Page Server* quindi scegliere *Proprietà*.
4. Nel campo Comando sotto la scheda Proprietà, aggiungere al termine della riga di comando>

```
maxDBResultRecords <valore maggiore di 20000 o 0 per
  disabilitare il limite di default>
```

5. Riavviare *Crystal Page Server*.

Riconfigurazione di Crystal Page Server (server Crystal per Linux o Windows Crystal)

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

Per i server Crystal Linux:

```
http://<DNS o IP del
  server_Crystal>:8080/businessobjects/enterprisell/a
  dminlaunch
```

Per i server Crystal Windows:

```
http://<nome DNS o indirizzo IP del server
  Web>/businessobjects/enterprisell/WebTools/adminlau
  nch/default.aspx
```

2. Fare clic su *Central Management Console (Console di gestione centrale)*.
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 (Esegui login)*.
5. Fare clic su *Server*.
6. Fare clic su *<nome server>.pageserver*

7. 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), fare clic sul pulsante di scelta *'Unlimited records'* (Senza limite di record).
8. Fare clic su *Applica*.
9. Verrà visualizzato un prompt per il riavvio del page server. Fare clic su *OK*.
10. È possibile che vengano richiesti un nome di accesso e una password per accedere al manager dei servizi del sistema operativo.

Rapporti forniti da Sentinel

1. A partire dalla versione 5.1.1 SP1 le prime 10 interrogazioni di rapporti aggregano tabelle anziché una tabella con gli eventi dettagliati. Assicurarsi che i servizi EventFileRedirectService e Aggregation (riepiloghi) siano attivati.
EventFileRedirectService si trova sul computer DAS e può essere abilitato mediante la modifica del file `das_binary.xml`.
I tre riepiloghi che è necessario attivare sono:
 - EVT_DEST_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1

NOTA: Per informazioni su EventFileRedirectService e i tre riepiloghi di aggregazione, vedere *il capitolo SDM nella Guida dell'utente* di Sentinel oppure i capitoli relativi all'installazione di Crystal nella *Guida all'installazione di Sentinel*.

2. I rapporti che interrogano un vasto intervallo di date possono venire eseguiti lentamente. È consigliabile pianificarli anziché eseguirli interattivamente.

NOTA: per informazioni sulla pianificazione di Crystal Reports vedere la documentazione su *Crystal BusinessObjects Enterprise™ 11*.

Suggerimenti per lo sviluppo di report Crystal personalizzati

Per i report personalizzati è consigliabile:

1. Utilizzare il più possibile tabelle aggregate.
2. Se i report possono utilizzare tabelle aggregate predefinite, scegliere la tabella aggregata che comporta l'elaborazione della minore quantità di dati.
3. Provare a inserire quasi tutti i dati da elaborare nel motore del database.
4. Per diminuire il sovraccarico dei processi di elaborazione in Crystal Server, ridurre al minimo la quantità di dati da recuperare sul server di Crystal.

Procedure consigliate per la manutenzione

Analisi del database per Oracle

Quando gli eventi vengono inseriti continuamente nel database di Sentinel, le statistiche di quest'ultimo devono essere aggiornate regolarmente per garantire prestazioni di interrogazione ottimali. L'utilizzo di analisi del database aggiorna le statistiche del database in merito ai dati evento per Oracle. Per ottimizzare le prestazioni, è consigliabile pianificare l'esecuzione regolare di tale utility.

NOTA: questa utility comprende uno script SQL necessario aggiornabile periodicamente. È consigliabile controllare periodicamente la disponibilità di eventuali aggiornamenti nel portale del servizio clienti Novell.

È necessario eseguire regolarmente i due script di shell seguenti mediante cron o un altro strumento di pianificazione:

- AnalyzePartitions.sh

Analisi di partizioni

Lo script AnalyzePartitions.sh analizza le partizioni che sono state compilate di recente. È consigliabile pianificare questo script in modo che aggiorni quotidianamente le statistiche del database nelle partizioni compilate il giorno precedente. È consigliabile eseguire questo script due ore dopo mezzanotte quando gli eventi del giorno precedente sono stati inseriti nel database.

Questo script si trova in \$ESEC_HOME/utilities/db e deve essere eseguito a livello locale sul server in cui è installato il database di Sentinel. Il conto utente UNIX che esegue lo script deve inoltre essere collegato al database come sysdba, ad esempio oracle.

NOTA: Se si è scaricata una nuova versione di questa utility rispetto a quella correntemente installata nel computer, sarà necessario installare sp_exec_dba_utl.sql.

Installazione di sp_exec_dba_utl.sql

1. Eseguire il login come proprietario del software Oracle.
2. Mediante SQL*Plus, connettersi al database come ESECDBA.
3. Installare il pacchetto ESEC_DBA_UTL. Al prompt SQL (SQL>), digitare:

```
@sp_exec_dba_utl.sql
```
4. Uscire da SQL*Plus.

Esecuzione di AnalyzePartitions.sh

1. Nel computer server del database Oracle, passare a:

```
$ESEC_HOME/utilities/db/
```

o passare all'ubicazione in cui si è scaricato l'ultimo file.
2. Al prompt dei comandi, digitare:
Per Solaris:

```
./AnalyzePartitions.sh <SID_ORACLE> >> <NomeFileLog>
```


Per Linux:

```
ksh ./AnalyzePartitions.sh <SID_ORACLE> >>  
<NomeFileLog>
```

 - SID_ORACLE: il nome dell'istanza Oracle per il database.
 - NomeFileLog: il percorso completo del file in cui si desidera scrivere i messaggi di log.

Se l'esecuzione dello script riesce, verrà chiuso con codice restituito 0. Se invece l'esecuzione dello script non riesce, verrà chiuso con codice restituito 1. Pianificare lavori di conseguenza in modo che da controllare il codice restituito. Se il processo di analisi ha esito negativo, controllare il file di log per i messaggi di errore dettagliati.

Controllo dello stato del database per Oracle

dbHealthCheck.sh è uno script che raccoglie le informazioni sul database Oracle di Sentinel. Lo script:

- Consente di verificare se l'istanza del database è attiva
- Consente di verificare se il listener Oracle è attivo
- Consente di visualizzare l'utilizzo dello spazio
- Consente di verificare l'esistenza di indici non utilizzabili
- Consente di verificare l'esistenza di oggetti di database non validi
- Consente di verificare l'esistenza di analisi di database

È consigliabile eseguire lo script regolarmente mediante cron o un altro strumento di pianificazione:

NOTA: Questa utility che comprende uno script SQL necessario può essere aggiornata periodicamente. È consigliabile controllare periodicamente la disponibilità di eventuali aggiornamenti nel portale del servizio clienti Novell.

Installazione ed esecuzione di dbHealthCheck.sh

NOTA: Se si è scaricata una nuova versione di questa utility rispetto a quella correntemente installata nel computer, sarà necessario installare sp_exec_dba_utl.sql.

Installazione di sp_exec_dba_utl.sql

1. Eseguire il login come proprietario del software Oracle.
2. Nel server del database, verificare che \$ORACLE_HOME e \$ORACLE_SID siano impostati nell'ambiente in uso.
3. Mediante SQL*Plus, connettersi al database come ESECDBA.
4. Installare il pacchetto ESEC_DBA_UTL. Al prompt SQL (SQL>), digitare:

```
@sp_exec_dba_utl.sql
```

5. Uscire da SQL*Plus.

Esecuzione di dbHealthCheck.sh

NOTA: È necessario eseguire lo script utilizzando il conto del proprietario del software Oracle oppure un altro conto che possa connettersi "AS SYSDBA"

NOTA: È necessario eseguire localmente dbHealthCheck.sh nel server del database.

1. Nel server del database, verificare che \$ORACLE_HOME e \$ORACLE_SID siano impostati nell'ambiente in uso.
2. Nel computer server del database Oracle, passare a:
\$ESEC_HOME/utilities/db/
o passare all'ubicazione in cui si è scaricato l'ultimo file.
3. Al prompt dei comandi, digitare:

Per Solaris:

```
./dbHealthCheck.sh
```

Le informazioni sul database di Sentinel verranno visualizzate sullo schermo o sarà possibile scrivere i risultati in un file.

```
./dbHealthCheck.sh >> <nomefile>
```

Per Linux:

```
ksh ./dbHealthCheck.sh
```

Le informazioni sul database di Sentinel verranno visualizzate sullo schermo o sarà possibile scrivere i risultati in un file.

```
ksh ./dbHealthCheck.sh >> <nomefile>
```

Archiviazione automatica di dati e aggiunta di partizioni (solo Windows)

NOTA: Se con il computer in uso non è possibile accedere a DAS_Binary e DAS_Query, utilizzare l'opzione della riga di comando di Gestione dati Sentinel anziché l'interfaccia utente.

Questa procedura può essere applicata solo a Windows. Assicurarsi che durante l'esecuzione delle operazioni preliminari di configurazione e di configurazione effettive vengano eseguite le operazioni seguenti:

- Assicurarsi che sdm.connect venga inizializzato mediante l'interfaccia utente grafica di Gestione dati Sentinel o la riga di comando.
- Assicurarsi che la directory di archiviazione sia esistente.
- Assicurarsi che i giorni di archiveConfig e dropPartitions si equivalgano.
- Assicurarsi che i file batch vengano eseguiti correttamente dal prompt dei comandi almeno una volta prima di pianificarne l'esecuzione automatica.

NOTA: se il task pianificato non riesce, non verrà inviata alcuna notifica ma verrà registrato in SDM_*.log

Operazioni preliminari alla configurazione

Prima di impostare automaticamente l'archiviazione di dati e l'aggiunta di partizioni, è necessario:

- [Salvare le proprietà di connessione](#)
- [Stabilire i parametri di archiviazione](#)

Salvataggio di proprietà di connessione in Gestione dati Sentinel

Questa operazione deve essere eseguita prima di utilizzare le opzioni della riga di comando di Gestione dati Sentinel. Per salvare la connessione (saveConnection) in Gestione dati Sentinel, è necessario eseguire la riga di comando di Gestione dati Sentinel con l'azione saveConnection.

Se è necessario eseguire l'interfaccia utente grafica di Gestione dati Sentinel, è possibile utilizzare il file sdm.connect creato dall'interfaccia utente grafica, il quale si trova in %ESEC_HOME%\sentinel\config.

L'azione saveConnection salva i dettagli di connessione in connectFile. Le battute a cui viene fatto riferimento nel file configuration.xml vengono utilizzate per cifrare la password prima di salvarla in connectFile.

Per impostare i dettagli della connessione sono disponibili le opzioni della riga di comando seguenti dell'azione saveConnection:

-filesToImport	-server
-<oracle or mssql>	Mssql
-Indirizzo IP o nome host SMTP	<indirizzo IP dell'host del database o nome host a cui connettersi>
-<numero di porta del database a cui connettersi [default di Oracle:	<numero di porta del database a cui connettersi [il valore di default per SQL Server è: 1433]>
-<nome/SID del database a cui connettersi>	<nome/SID del database a cui connettersi>
-Utente di autenticazione posta	<nome utente del database>
-Password per l'utente di autenticazione posta	<password del database>
-Utilizzato per l'autenticazione di Windows	utilizzato per l'autenticazione di Windows. Quando si utilizza questa opzione, non utilizzare -user e -password.
-<nome file per salvare i dettagli della connessione [scelto dall'utente]>	<nome del file scelto dall'utente in cui salvare i dettagli della connessione>

I dettagli di connessione in alto vengono salvati nel file specificato insieme alla password cifrata. Per eseguire le altre azioni della riga di comando di Gestione dati Sentinel, questa applicazione utilizza i dettagli della connessione salvati. È necessario completare questo passaggio la prima volta che si avvia l'applicazione e ogni volta che si desidera modificare i dettagli della connessione.

Esecuzione di saveConnection

1. Eseguire il comando nel modo seguente:

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

Nell'esempio seguente i dettagli della connessione vengono salvati nel file `sdm.connect` relativo al database `esec` in un host con indirizzo IP `172.16.0.36` e porta `1433` che autentica con utente `esecdba`.

```
sdm -action saveConnection -server mssql -host
172.16.0.36 -port 1433 -database esec -user esecdba
-password XXXXXX -connectFile sdm.connect
```

Nell'esempio di autenticazione di Windows seguente i dettagli della connessione vengono salvati nel file `sdm.connect` relativo al database `esec_51` in un host con indirizzo IP `172.16.1.1` e porta `1433` che autentica mediante l'Autenticazione di Windows.

```
sdm -action saveConnection -server mssql -host
172.16.1.3 -port 1433 -database esec_51 -winAuth -
connectFile sdm.connect
```

I dettagli della connessione vengono salvati nel file `sdm.connect`. Tutte le altre azioni della riga di comando utilizzano questo nome di file come input per effettuare la connessione al database specificato ed eseguire le relative azioni.

NOTA: Se si crea un file di connessione in un'ubicazione o con un nome diversi da quelli specificati nell'esempio, sarà necessario modificare il file `manage_data.bat`.

Definizione di parametri di archiviazione

È possibile eseguire questa operazione mediante la riga di comando di Gestione dati Sentinel.

L'azione `archiveConfig` viene utilizzata per configurare l'archiviazione. Questa configurazione determina la modalità di archiviazione dei dati delle tabelle del database Sentinel.

Con questa azione vengono utilizzati i flag seguenti:

<code>filesToImport</code>	<code>-dirPath</code>
<percorso di directory valido in cui scrivere i file archiviati>	<percorso di directory valido in cui scrivere i file archiviati>
<numero di giorni di permanenza>	<numero di giorni di permanenza>
<nome del file in cui salvare i dettagli della connessione [scelto dall'utente]>	<percorso del file salvato da " saveConnection ">

Definizione di parametri di archiviazione tramite la riga di comando

1. Creare una directory di output di archiviazione denominata `SDM_archive` nella directory radice (`c:\SDM_archive`).

NOTA: se si crea una directory di output o un'ubicazione diversa, sarà necessario modificare il file `manage_data.bat`.

2. Eseguire il comando come nell'esempio seguente:

```
sdm -action archiveConfig -dirPath <percorso di
directory in cui scrivere i file archiviati> -
keepDays <numero di giorni di permanenza> -
connectFile <percorso del file salvato da
"saveConnection">
```

Nell'esempio seguente viene illustrata l'archiviazione nella directory `c:\SDM_archive` di dati risalenti a 30 giorni prima.

```
sdm -action archiveConfig -dirpath c:\SDM_archive -
keepDays 30 -connectFile sdm.connect
```

Definizione di parametri di archiviazione tramite l'interfaccia utente grafica

1. Creare una directory di output di archiviazione denominata `SDM_archive` nella directory radice (`c:\SDM_archive`).

NOTA: se si crea una directory di output o un'ubicazione diversa, sarà necessario modificare il file `manage_data.bat`.

2. Per l'interfaccia utente grafica di gestione dati Sentinel non sono necessari parametri di archivio. L'interfaccia utente grafica supporta infatti l'archiviazione diretta dei dati senza che sia necessario definire parametri di archivio.

Eliminazione di dati (rilascio di partizioni)

Questa azione (deleteData) determina l'eliminazione di dati anteriori a "keepDays" nelle tabelle seguenti.

- CORRELATED_EVENTS
- EVT_DEST_EVT_NAME_SMRY_1

Questa azione non comporta per default il rilascio di tutte le partizioni non archiviate. Se si desidera eliminare partizioni non archiviate, è necessario specificare il flag facoltativo "forceDelete" impostando il valore true. Se si utilizza forceDelete:

false oppure valore non specificato vengono rilasciate solo le partizioni archiviate anteriori a keepDays. Le partizioni non archiviate non vengono eliminate anche se anteriori a keepDays.

abbandona tutte le partizioni precedenti al valore di keepDays incluse le partizioni non archiviate vengono abbandonate tutte le partizioni anteriori al valore di keepDays incluse le partizioni non archiviate

Con questo comando vengono utilizzati i flag seguenti:

filesToImport	deleteData
<numero di giorni di permanenza>	<numero di giorni di permanenza>
[-forceDelete]	<true o false>
<nome del file in cui salvare i dettagli della connessione [scelto dall'utente]>	<percorso del file salvato da " saveConnection ">

Esecuzione di deleteData

1. Eseguire il comando come nell'esempio seguente:

```
sdm -action deleteData -keepDays <numero di giorni di permanenza> -connectFile <percorso del file salvato da "saveConnection">
```

Nell'esempio seguente vengono rilasciate le partizioni delle tabelle EVENTS e CORRELATED_EVENTS anteriori a 30 giorni, verificando che tutte le partizioni rilasciate siano archiviate. Al termine, verranno elencate le eventuali partizioni non eliminate in quanto non archiviate.

```
sdm -action deleteData -keepDays 30 -connectFile sdm.connect
```

Pianificazione dell'archiviazione dei dati e dell'aggiunta di partizioni

NOTA: il file manage_data.bat è impostato su un valore keepDay di 30, l'archivio viene salvato in c:\SDM_archive e il file di connessione in %ESEC_HOME%\SDM\sdm.connect. Se i valori sono diversi, sarà necessario modificare il file.

Se sono stati impostati le proprietà di connessione e i parametri di archivio, eseguire dal prompt dei comandi per garantirne il corretto funzionamento.

Per archiviare i dati e aggiungere le partizioni automaticamente

NOTA: i passaggi seguenti possono essere applicati a Windows 2000 Professional. I passaggi per Windows 2000 Server, XP e 2003 Server possono essere diversi ma simili.

1. In Windows fare clic su *Start > Impostazioni > Pannello di controllo*.
2. Fare doppio clic su *'Operazioni pianificate'*.
3. Fare doppio clic su *'Aggiungi operazione pianificata'*. Fare clic su *Avanti*.
4. Fare clic sul *pulsante Sfoglia*, quindi individuare il file `manage_data.bat` (`%ESEC_HOME%\sdm`).
5. Assegnare un nome all'operazione pianificata, ad esempio `SDM_Archivio`. Selezionare *Ogni giorno* in *"Esegui questa operazione"*. Fare clic su *Avanti*.
6. Selezionare un'ora del giorno in cui eseguire questa operazione. Fare clic su *Avanti*.
7. Immettere l'ora e la data desiderate. Fare clic su *Avanti*.



8. Immettere un utente in cui verrà eseguita questa operazione. L'utente non può corrispondere al conto del sistema locale. L'operazione deve essere eseguita come utente specifico. Se per connettersi al database si utilizza l'Autenticazione di Windows, è necessario utilizzare l'utente Windows amministratore del database Sentinel. Fare clic su *Avanti*.
9. Fare clic su *Fine* per completare l'operazione pianificata.

Motore di correlazione

NOTA: Per il corretto funzionamento del motore di correlazione Sentinel è necessario che l'ora di sistema del computer sia sincronizzata entro ± 30 secondi con tutti i computer che eseguono Gestione servizi di raccolta. È consigliabile che tutti i computer di motore di correlazione e Gestione servizi di raccolta siano connessi a un server NTP (Network Time Protocol) o a un altro tipo di server di orario.

Informazioni generali sulle regole di correlazione avanzate

La regola di correlazione avanzata viene utilizzata per rilevare le relazioni tra due eventi, ad esempio quando si verifica un particolare evento (evento B) dopo l'evento A con una relazione tra i due eventi. In questo caso, l'evento B corrisponde all'evento B attuale e deve essere identificato con un filtro immesso nel riquadro della procedura guidata Criteri di filtro eventi. L'evento A corrisponde all'evento precedente e deve essere identificato con un filtro immesso nel riquadro della procedura guidata Criteri di filtro eventi precedenti. La relazione tra i due eventi, ad esempio se dispongono degli stessi indirizzi IP di origine e destinazione, deve essere immessa nel riquadro della procedura guidata Evento rispetto ai criteri di eventi precedenti. In questa riquadro è inoltre possibile specificare l'intervallo massimo che si desidera rilevare tra i due eventi. Questa è la finestra del tempo. Se un evento utilizza tutti questi criteri, è possibile raggrupparlo e assegnarli un valore soglia indicato nel riquadro della procedura guidata Criteri raggruppamento e soglia.

Controllo del tempo

Alle operazioni Finestra e Trigger è associata una finestra del tempo. Più grande è la finestra del tempo e più eventi (ovvero parti di informazioni sugli eventi) possono essere memorizzati nella memoria in merito a questa finestra. I dati memorizzati per l'operazione Finestra dipendono dal filtro specificato per gli eventi precedenti. Quanto più specifico è questo filtro e tanto minori sono gli eventi memorizzati nella finestra del tempo con la conseguente possibilità di utilizzare un arco di tempo più ampio, se necessario). Per l'operazione Trigger lo spazio massimo totale di memorizzazione che è possibile utilizzare dipende dalla cardinalità del discriminatore (ovvero più raggruppamenti è possibile raccogliere e più eventi vengono memorizzati nel tempo) fino al valore soglia per ogni gruppo. Se per l'operazione Trigger si riduce molte volte il valore della soglia e del periodo di tempo, verranno restituiti risultati equivalenti.

Informazioni generali sull'aggiornamento di Trigger

Si supponga di ricevere un evento correlato per una regola con un numero di eventi correlati inferiore al previsto. Ciò è dovuto al comportamento di aggiornamento dell'operazione Trigger. Nell'operazione Trigger è possibile specificare di attivare un evento correlato quando si verifica un gruppo di 'n' eventi in un periodo di tempo 't'. Ogni volta che il motore di correlazione rileva il gruppo di eventi 'n' in un periodo 't', attiva l'evento di correlazione. Se all'attivazione viene determinato che è stato precedentemente già attivato (per lo stesso gruppo) e che esiste almeno un membro impostato in comune, tali membri vengono aggiunti all'evento correlato originale e non viene invece creato un nuovo evento correlato.

Le espressioni booleane supportano analisi concise

I confronti tra numeri sono più veloci rispetto a quelli tra stringhe che però risultano più rapidi rispetto ai confronti tra espressioni. L'operazione Filtro esegue un'analisi concisa nelle espressioni Booleane. Un accurato ordinamento dell'espressione può migliorare la velocità di valutazione.

Formato libero

Se non è possibile esprimere una regola di correlazione utilizzando i tre modelli predefiniti della procedura guidata (Watchlist, Di base o Avanzata), costruire una regola a formato libero. Tutti i modelli compongono alla fine una regola a formato libero per l'utente. Per visualizzare una rappresentazione del formato libero, modificare una regola impostandone il tipo sul formato libero. Questo può essere un facile metodo per estendere una regola che non è possibile esprimere con una delle altre tre opzioni.

Log delle transazioni

Per default i database Sentinel per SQL Server vengono creati in un modello di completo recupero in cui lo spazio del log delle transazioni viene liberato solo dopo l'esecuzione di una copia di backup del log. Per evitare che lo spazio del log delle transazioni raggiunga la massima capacità, è consigliabile pianificare diversi backup al giorno del log in SQL Server, circa 3 o 4 volte in base alla frequenza degli eventi. Se l'organizzazione non necessita della funzionalità di recupero dal punto di errore, è possibile impostare il modello di recupero del database su semplice. In questo caso, lo spazio del log delle transazioni viene liberato automaticamente da SQL Server, senza l'esecuzione di alcuna copia di backup.

Ubicazioni dei file di log di Sentinel

Alcuni log di Sentinel consentono di risolvere i problemi del sistema. Questi log inoltre possono essere utilizzati con il Supporto tecnico Novell perché estremamente utili per la risoluzione dei problemi.

Gestione dati Sentinel

Attività dei log eseguite con Gestione dati Sentinel per il client specifico in esecuzione sul computer.

In Windows:

```
%ESEC_HOME%\sdm\SDM_*.0.log
```

In UNIX:

```
$ESEC_HOME/sdm/SDM_*.0.log
```

iTRAC

Attività di log correlate a iTRAC.

In Windows:

```
%ESEC_HOME%\sentinel\log\das_itrac_0.*.log
```

In UNIX:

```
$ESEC_HOME/sentinel/log/das_itrac_0.*.log
```

Advisor

Attività di log correlate allo scaricamento e all'elaborazione dei dati di Advisor.

In Windows:

```
%ESEC_HOME%\sentinel\log\advisor.log  
%ESEC_HOME%\sentinel\log\Advisor_0.*.log
```

In UNIX:

```
$ESEC_HOME/sentinel/log/advisor.log  
$ESEC_HOME/sentinel/log/Advisor_0.*.log
```

Inserimento di eventi

Attività di log correlate all'inserimento di eventi nel database.

In Windows:

```
%ESEC_HOME%\sentinel\log\das_binary0.*.log
```

In UNIX:

```
$ESEC_HOME/sentinel/log/das_binary0.*.log
```

Interrogazioni database

Attività di log correlate a interrogazioni del database, servizi di raccolta, Gestione servizi di raccolta, stato e altre attività DAS non eseguite da altri componenti DAS.

In Windows:

```
%ESEC_HOME%\sentinel\log\das_query0.*.log
```

In UNIX:

```
$ESEC_HOME/sentinel/log/das_query0.*.log
```

Visualizzazioni Active Views

Attività di log correlate ad Active Views.

In Windows:

```
%ESEC_HOME%\sentinel\log\das_rt0.*.log
```

In UNIX:

```
$ESEC_HOME/sentinel/log/das_rt0.*.log
```

Aggregation

Attività di log correlate all'aggregazione.

In Windows:

```
%ESEC_HOME%\sentinel\log\das_aggregation0.*.log
```

In UNIX:

```
$ESEC_HOME/sentinel/log/das_aggregation0.*.log
```

Sorveglianza Sentinel

Attività di log correlate a Sorveglianza Sentinel.

NOTA: il file `sentinel_wrapper.log` è per il wrapper di servizio.

In Windows:

```
%ESEC_HOME%\sentinel\log\sentinel0.*.log  
%ESEC_HOME%\sentinel\log\sentinel_wrapper.log
```

In UNIX:

```
$ESEC_HOME/sentinel/log/sentinel0.*.log  
$ESEC_HOME/sentinel/log/sentinel_wrapper.log
```

Gestione servizi di raccolta

Attività di log correlate a Gestione servizi di raccolta.

NOTA: il file `agent-wrapper.log` è per il wrapper di servizio.

In Windows:

```
%ESEC_HOME%\wizard\logs\agent-manager.log  
%ESEC_HOME%\wizard\logs\am0.*.log
```

In UNIX:

```
$ESEC_HOME/wizard/logs/agent-manager.log  
$ESEC_HOME/wizard/logs/am0.*.log
```


3

Installazione di Sentinel 5 per Oracle in Solaris

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo viene descritto come installare Sentinel Enterprise Security Management Sentinel 5 per Oracle in Solaris.

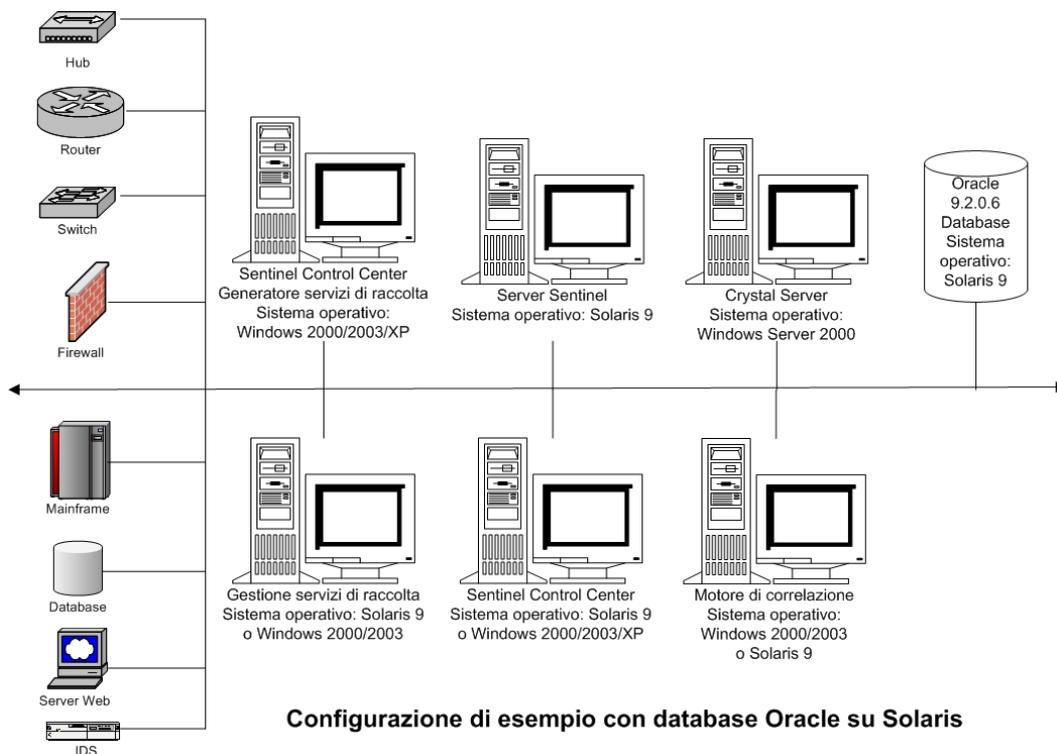
Operazioni preliminari all'installazione di Sentinel 5 per Oracle in Solaris

NOTA: prima dell'installazione, verificare che il computer in uso soddisfi i requisiti minimi di sistema e che il sistema operativo sia stato ottimizzato utilizzando le procedure consigliate correnti per la sicurezza.

NOTA: installare Oracle Enterprise con partizionamento. In Gestione dati Sentinel questa funzione è necessaria per la gestione del database di Sentinel.

NOTA: quando si esegue un'installazione completa di Sentinel dopo averne rimosso una precedente, è necessario rimuovere alcuni file e impostazioni del sistema derivanti dall'installazione precedente. Se non si rimuovono tali file o impostazioni la nuova installazione completa potrebbe non riuscire. Questa operazione deve essere eseguita su ogni computer sul quale si sta eseguendo una nuova installazione. Per ulteriori informazioni, vedere *l'appendice E*.

Le configurazioni tipiche di Solaris per Sentinel sono le seguenti. La configurazione dell'utente potrebbe essere diversa, a seconda dell'ambiente in uso. Indipendentemente dalla configurazione selezionata, è necessario installare prima il database.



NOTA: per ulteriori informazioni sui sistemi operativi supportati, vedere la sezione *sulle piattaforme supportate per il server Sentinel su Solaris nel capitolo 1 "Introduzione"*.

Per ottenere un codice di licenza

Per l'installazione e l'esecuzione del servizio DAS (Database Access Service) del server Sentinel è necessario disporre di un codice di licenza valido. Tale codice di licenza è bloccato per il computer nel quale si installa DAS. Il codice di licenza emesso per un computer non funzionerà su un computer diverso.

Per ottenere il codice di licenza, è necessario determinare l'ID host e fornire tali informazioni a Novell che provvederà all'assegnazione di un codice di licenza.

Per determinare l'ID dell'host (Solaris)

1. Immettere il comando seguente:

```
host
```

2. Inviare l'ID host al Supporto tecnico Novell. Il Supporto clienti fornirà il codice di licenza richiesto.

Database di Sentinel

Prima di installare il database di Sentinel, sarà necessario accertarsi di disporre di quanto segue:

- Per i requisiti hardware, vedere i *capitoli 1 e 2*.
- Server Sun SPARC Solaris con l'esecuzione di Solaris 9 Recommended Patch Cluster DATE: 3 maggio 05
- Oracle 9i Enterprise Edition 9.2.0.6 o 9.2.0.7 con partizionamento
- Per Solaris una copia di Oracle Note: 148673.1 SOLARIS: Quick Start Guide

- Utente del sistema operativo Oracle (default: oracle)
- Verificare che siano impostate le seguenti variabili di ambiente per il sistema operativo Oracle:
 - ORACLE_HOME
 - ORACLE_BASE
 - PATH (deve essere \$ORACLE_HOME/bin)
 - Sebbene non sia consigliabile, se si crea manualmente l'istanza del database Oracle, vedere [Creazione di un'istanza di Oracle per il database di Sentinel](#) per istruzioni sulla creazione dell'istanza di Oracle. Se si seleziona questa opzione, è comunque necessario utilizzare il programma di installazione per aggiungere gli oggetti di database all'istanza del database Oracle creata manualmente, (vedere [Installazione personalizzata](#) per istruzioni sull'esecuzione di questa operazione).

NOTA: se si utilizza un'istanza di database Oracle esistente o creata manualmente, è necessario che sia vuota con l'eccezione della presenza dell'utente esecdba.

- Se si utilizza il programma di installazione per creare l'istanza di database Oracle (opzione consigliata), sarà necessario conoscere i percorsi di directory in cui ubicare i file di database. Tali directory devono esistere prima di eseguire il programma di installazione perché non sarà possibile crearle durante l'installazione. È inoltre necessario che tali directory siano accessibili in scrittura dall'utente del sistema operativo Oracle (ovvero – oracle).

NOTA: per motivi connessi alle prestazioni, a seconda che si stia eseguendo l'installazione in RAID e che l'ambiente RAID lo consenta, il Redo Log dovrebbe fare riferimento al disco con scrittura più veloce disponibile.

NOTA: per default, il programma di installazione imposta gli spazi delle tabelle seguenti perché le dimensioni NON aumentino automaticamente: ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX. Tutti gli altri spazi delle tabelle sono impostati per l'aumento automatico delle relative dimensioni. Il motivo per il quale non viene consentito l'aumento automatico di ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX è che contengono dati di eventi e dati di eventi di riepilogo. L'utilizzo dello spazio per gli eventi e i riepiloghi può essere notevolmente dinamico. È necessario monitorare ed estendere questi spazi di tabelle degli eventi in maniera controllata, in base alla configurazione del file system e tenendo in considerazione il bilanciamento IO e le attività di backup e recupero del database.

La gestione della partizione SDM (archiviazione, eliminazione e aggiunta di partizioni) dovrebbe essere pianificata per mantenere dimensioni controllate per gli eventi.

Server Sentinel

NOTA: se non si intende installare il database di Sentinel contemporaneamente al server Sentinel, è necessario installare prima il database di Sentinel.

Prima di installare il server Sentinel, sarà necessario accertarsi di disporre di quanto segue:

- Per i requisiti hardware, vedere i *capitoli 1 e 2*.
- Server Sun SPARC Solaris con l'esecuzione di Solaris 9 Recommended Patch Cluster DATE: 3 maggio 05
- Numero di serie e codice licenza per Novell Sentinel 5 (per DAS). Per ulteriori informazioni, vedere [Per ottenere un codice di licenza](#).
- Server SMTP – Necessario per l'invio di e-mail da Sentinel.

Sentinel Control Center e Wizard

Prima di installare il server Sentinel, sarà necessario accertarsi di disporre di quanto segue:

- Per i requisiti hardware, vedere il *capitolo 1 e 2*
- Uno dei sistemi operativi seguenti:
 - Server Sun SPARC Solaris che esegue Solaris con la patch consigliata Solaris 9 Recommended Patch Cluster DATE: 03 maggio 2005
 - (solo Generatore servizio di raccolta) – Windows 2000 o 2003

Advisor

Per installare Advisor, sarà necessario ottenere un ID Advisor e una password da Sentinel. Download Internet diretto utilizza la porta 443.

NOTA: se si intende utilizzare Advisor solo per il rilevamento dell'utilizzo, non sarà necessario installare il software Crystal Enterprise. È infatti necessario solo se si intende eseguire Crystal Reports for Sentinel. Per ulteriori informazioni, vedere il *capitolo 8, Configurazione di Advisor*.

verifica del layout di Solaris (Requisiti patch per il sistema operativo)

Verifica del layout di Solaris

1. Visitare il sito Internet di Sun e scaricare il gruppo di patch consigliate per Solaris 9:
 - Patch Cluster DATE: 3 maggio 05

NOTA: consultare il file README e l'altra documentazione inclusa. Prima di applicare qualsiasi patch, è vivamente consigliato eseguire una copia di backup completa del sistema.

2. Eseguire il login come utente root, quindi installare il gruppo di patch e le patch del kernel applicabili.
3. Al termine dell'applicazione delle patch, eliminare il file *_Recommended.zip e i file espansi inclusi nelle directory create dalla patch, quindi riavviare il server.

Operazioni preliminari all'installazione di Oracle in Solaris

Per installare Oracle in Solaris per Sentinel, è necessario avere eseguito le operazioni seguenti:

- Impostazione dei valori del kernel
- Creazione di un gruppo e di un conto utente per Oracle
- Impostazione delle variabili d'ambiente
- Installazione di Oracle 9.2.0.6 o 9.2.0.7
- Patch di Oracle 9.2.0.6 o 9.2.0.7

Impostazione dei valori del Kernel per Oracle in Solaris

Per Oracle in Solaris è necessario impostare i valori del kernel seguenti in /etc/system.

ESCLUSIONE DI GARANZIA: i seguenti sono i valori minimi consigliati. Per ulteriori informazioni consultare l'amministratore del sistema e la documentazione Oracle.

- shmmax=4294967295
- shmmin=1
- shmseg=50
- shmmni=400
- semmns=14000
- semmni=1024
- semmsl=1024
- shmopm=100
- shmvmx=32767

NOTA: se i valori del kernel sono uguali o superiori ai requisiti indicati, non è necessario modificare le impostazioni.

1. Eseguire il login come utente radice.
2. Creare una copia di backup di /etc/system
3. In un editor di testo, modificare le impostazioni del kernel nel file /etc/system come indicato nella tabella sopra.
4. Riavviare.

Operazioni preliminari all'installazione di Oracle in Solaris

ESCLUSIONE DI GARANZIA: le istruzioni seguenti 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 /export/home/oracle e che Oracle venga installato in /opt/oracle. La configurazione specifica può essere diversa. Per ulteriori informazioni consultare documentazione del sistema operativo e di Oracle.

NOTA: quando si installa il software Oracle, è consigliabile scegliere l'installazione "standard". Se invece si sceglie l'installazione personalizzata, assicurarsi di selezionare l'Interfaccia JDBC/OCI Oracle. Per ulteriori informazioni, vedere la documentazione di Oracle.

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:

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

3. Per impostare le variabili d'ambiente necessarie per Oracle, è consigliabile aggiungere le informazioni seguenti nel file local.cshrc:

```
umask 022

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
```

4. Seguire i passaggi descritti in Oracle Note: 148673.1 SOLARIS: Guida di riferimento rapido
5. Installare Oracle 9i Release 2 come utente oracle. Verranno richiesti due CD-ROM aggiuntivi. Per ogni CD-ROM aggiuntivo + necessario spostarsi su directory differenti.
6. Applicare al sistema la patch per la versione 9.2.0.6.0 o 9.2.0.7.0. Per le procedure di applicazione delle patch, fare riferimento alla documentazione di Oracle.
7. Per verificare il livello della patch come utente UNIX Oracle, immettere:

```
sqlplus '/as sysdba'
```

Verrà restituita la versione 9.2.0.6.0 o 9.2.0.7.0. Per uscire, immettere quit.

8. Rimuovere la directory creata per la patch.
9. Dopo aver installato le patch, rimuoverne le directory e i file.
10. Riavviare.

Installazione di Sentinel 5 per Oracle in Solaris

Sentinel 5 supporta due tipi di installazione. ovvero:

- Semplice – L'opzione di installazione integrata. Servizi Sentinel, i servizi di raccolta e le applicazioni con Oracle nello stesso computer. Questo tipo di installazione è eseguita solo a scopo dimostrativo.
- Personalizzata – Consente un'installazione completamente distribuita.

Installazione semplice in Solaris

Con questa installazione vengono installati in un singolo computer i componenti più comuni (non sono inclusi Generatore servizi di raccolta o funzionalità di integrazione di terze parti). Questa operazione è eseguita principalmente a scopo dimostrativo. Non si tratta dell'installazione consigliata per l'uso in un ambiente di test o di produzione.

NOTA: con l'installazione Semplice non è supportata l'autenticazione con password di Gestione servizi di raccolta.

Come eseguire una installazione semplice

1. Verificare di aver raccolto le informazioni, eseguito i task e soddisfatto i requisiti specificati nella sezione [Operazioni preliminari all'installazione di Sentinel 5 per Oracle](#) per i componenti da installare.
2. Verificare l'impostazione di [Solaris Oracle](#).
3. Eseguire il login come utente radice.
4. Inserire e montare il CD di installazione di Sentinel.
5. Avviare il programma di installazione passando alla directory di installazione sul CD-ROM e digitare:

Per la modalità GUI:

```
./setup.sh
```

oppure

Per la modalità testuale ("headless"):

```
./setup.sh -console
```

6. Nel riquadro successivo, fare clic sulla freccia giù e selezionare una delle lingue seguenti.
 - English (Inglese)
 - French (Francese)
 - German (Tedesco)
 - Italiano
 - Portuguese (Portoghese)
 - Spanish (Spagnolo)
7. Seguire i prompt del programma di installazione.
8. Dopo aver letto la schermata introduttiva, fare clic su *Avanti*.
9. Accettare le condizioni del Contratto di *licenza* per l'utente finale e fare clic su *Avanti*.
10. Accettare la directory di installazione di default o fare clic su Sfoglia per specificare il percorso di installazione. Fare clic su *Avanti*.

Fare clic su Avanti per installare "Sentinel 5" in questa cartella oppure fare clic su Sfoglia per installarlo in una cartella diversa.

Nome directory:

11. Selezionare *Semplice*. Fare clic su *Avanti*.

Simple

 All-In-One easy installation.

Custom

 Allows the user to configure a custom installation.

12. Immettere le informazioni di configurazione
 - Numero di serie e codice licenza
 - Server SMTP (nome DNS o indirizzo IP) – se si desidera avere la possibilità di inviare e-mail in Sentinel
 - E-mail – Specificare un indirizzo e-mail valido al quale vengano inviate le e-mail di notifica di Advisor (ad esempio Sent_Server@myserver.com).
 - Password di sistema globale – specificare una password e la password di conferma corrispondente. Questa diventerà la password per tutti gli utenti di default. Sono inclusi sia gli utenti esecadm del sistema operativo che gli utenti del database. Per l'elenco degli utenti del database di default creato durante l'installazione vedere [Database di Sentinel](#) nella sezione [Operazioni successive all'installazione di Sentinel 5 per Oracle](#).
 - Directory dati: l'ubicazione di tutti i file di dati scaricati per il database e Advisor, se installato. Per modificare il percorso di default, fare clic sul pulsante ... e selezionare un'ubicazione. Quella di default è \$ESEC_HOME/data

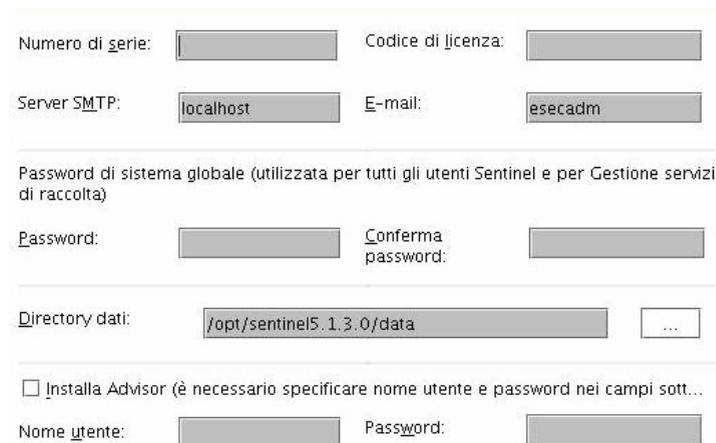
NOTA: gli utenti oracle ed esecadm devono disporre delle autorizzazioni di lettura, scrittura ed esecuzione per Directory dati. Poiché questa installazione è solo a scopo dimostrativo, è consigliabile assegnare questi diritti a tutti gli utenti. A questo scopo, eseguire il comando seguente:

```
chmod 777 <directory_percorso>
```

NOTA: se si sta installando Advisor, l'installazione Semplice consentirà di configurare Advisor per l'uso di Download Internet diretto con un intervallo di aggiornamento di 12 ore e tutte le notifiche via e-mail abilitate.

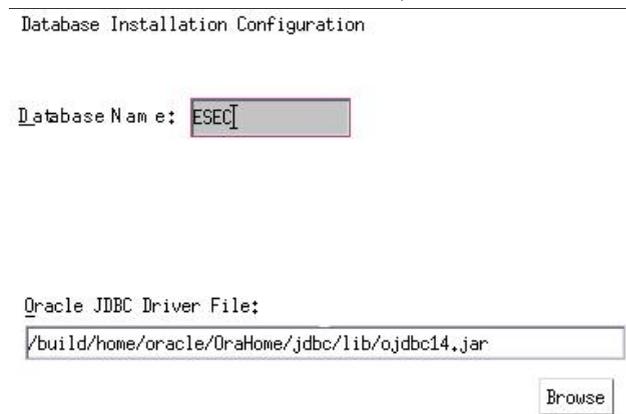
- Per installare Advisor, selezionare *Installa Advisor*. Specificare nome utente e password. Se non è possibile verificare nome utente o password, dopo aver fatto clic su *Avanti* verrà chiesto se si desidera continuare (non consigliabile). Se si sceglie di continuare, digitare di nuovo la password di Advisor nella finestra di conferma della password. In caso contrario correggere la password di Advisor.

Fare clic su *Avanti*.

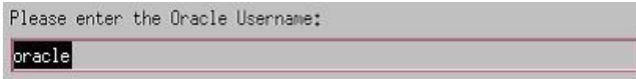


13. Immettere le informazioni di configurazione per il database:

- Nome database - Nome dell'istanza del database Oracle per creare e installare oggetti del database di Sentinel. Un database con questo nome non deve essere già esistente.
- File del driver JDBC Oracle. Percorso completo del file jar, in genere \$ORACLE_HOME/jdbc/lib/ojdbc14.jar (in questo campo non è possibile utilizzare variabili di ambiente).



14. Fare clic su *OK* sul nome utente Oracle di default.



15. Leggere le informazioni presenti nella schermata visualizzata e al termine fare clic su *Avanti*. Una volta completata l'installazione, sarà necessario riavviare il sistema.

NOTA: se si desidera installare software di integrazione di terze parti (HP Service Desk o Remedy Integration), dopo aver riavviato il computer, eseguire di nuovo il programma di installazione e selezionare il software di integrazione di terze parti che si desidera installare. Per ulteriori informazioni, vedere la *Guida all'integrazione con soluzioni di terze parti*.

16. Il programma di installazione di Sentinel, per default, 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 per evitare che il database interrompa l'accettazione degli eventi.

Installazione personalizzata in Solaris

Come eseguire una installazione Personalizzata

1. Verificare di aver raccolto le informazioni, eseguito i task e soddisfatto i requisiti specificati nella sezione [Operazioni preliminari all'installazione di Sentinel 5 per Oracle](#) per i componenti da installare.
2. Verificare l'impostazione di [Solaris Oracle](#).
3. Eseguire il login come utente radice.
4. Inserire e montare il CD di installazione di Sentinel.
5. Avviare il programma di installazione passando alla directory di installazione sul CD-ROM e digitare:
Per la modalità GUI:

```
./setup.sh
```


oppure
Per la modalità testuale ("headless"):

```
./setup.sh -console
```
6. Fare clic sulla freccia a discesa e selezionare una delle opzioni di lingua seguenti:
 - English (Inglese)
 - Italiano
 - French (Francese)
 - Portoghese (Portoghese)
 - German (Tedesco)
 - Spanish (Spagnolo)
7. Dopo aver letto la schermata introduttiva, fare clic su *Avanti*.
8. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.

9. Accettare la directory di installazione di default o fare clic su *Sfoggia* per specificare il percorso di installazione. Fare clic su *Avanti*.

Fare clic su *Avanti* per installare "Sentinel 5" in questa cartella oppure fare clic su *Sfoggia* per installarlo in una cartella diversa.

Nome directory:

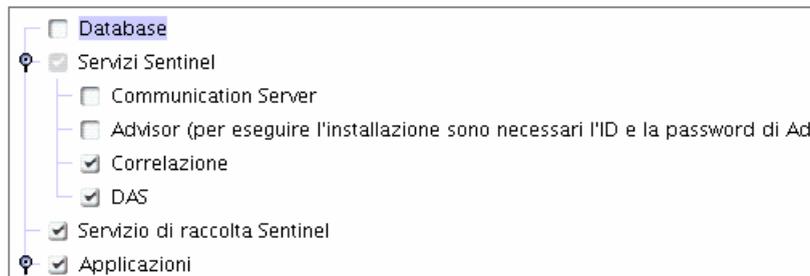
10. Selezionare *Personalizzata* (default). Fare clic su *Avanti*.

11. Selezionare le funzioni da installare.

NOTA: per ulteriori informazioni su quali componenti è possibile installare e in quale posizione per configurazioni diverse, vedere il *capitolo 1, Requisiti di sistema*.

Sono disponibili le opzioni seguenti:

Selezionare le funzioni di "Sentinel 5" che si desidera installare:



- | | |
|--|--|
| <input type="checkbox"/> Database – Consente di installare il database di Sentinel | <input type="checkbox"/> DAS |
| <input type="checkbox"/> Communication Server – Consente di installare il bus di messaggi (iSCALE) | <input type="checkbox"/> Servizi di raccolta |
| <input type="checkbox"/> Advisor | <input type="checkbox"/> Sentinel Control Center |
| <input type="checkbox"/> Motore di correlazione | <input type="checkbox"/> Gestione dati Sentinel |
| | <input type="checkbox"/> HP OpenView Service Desk* |
| | <input type="checkbox"/> Remedy Integration |

NOTA: *per informazioni sull'installazione di HP OpenView Service Desk o Remedy Integration, vedere la *Guida all'integrazione con soluzioni di terze parti*.

NOTA: se nessuna delle funzioni secondarie dei "Servizi Sentinel" è selezionata, deselegionare anche la funzione "Servizi Sentinel". Verrà visualizzata in grigio con un segno di spunta bianco se è ancora selezionata ma tutte le relative funzioni secondarie sono state deselegionate.

NOTA: come parte dell'installazione del componente del database di Sentinel, il programma di installazione inserirà i file nella cartella \$ESEC_HOME/utilities/db.

12. Se si è scelto di installare DAS, verrà richiesto di specificare:

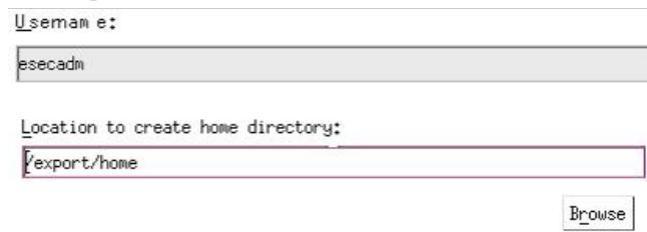
- Numero di serie
- Codice di licenza

13. Se si è scelto di installare componenti di integrazione di terze parti, verrà richiesto di specificare una password per sbloccare i componenti di terze parti selezionati.

Per ulteriori informazioni, vedere la *Guida all'integrazione con soluzioni di terze parti*.

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



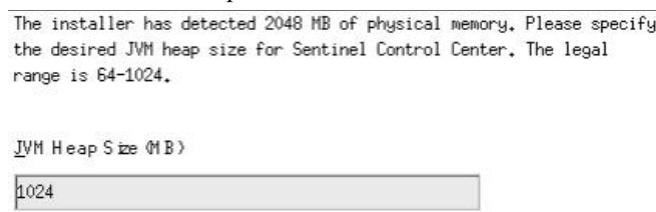
The screenshot shows a dialog box with two text input fields. The first field is labeled "User name:" and contains the text "esecadm". The second field is labeled "Location to create home directory:" and contains the text "/export/home". Below the second field is a "Browse" button.

NOTA: se viene creato un nuovo utente, sarà necessario impostare la relativa password in modo manuale, non nel programma di installazione. È consigliabile eseguire questa operazione direttamente eseguendo il login al sistema dopo l'installazione del prodotto.

per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, Sentinel richiede una password con le caratteristiche seguenti:

1. Scegliere password costituite da un minimo di 8 caratteri, di cui almeno uno MAIUSCOLO, uno minuscolo, uno speciale (!@#\$_) e uno numerico (0-9). Non utilizzare spazi.
2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.
3. La password non deve essere una parola "comune", ovvero una parola inclusa nel dizionario o di uso gergale.
4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione di password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.
5. È consigliabile scegliere una password facile da ricordare e allo stesso tempo complessa. Ad esempio, Mfhq5#a0 (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#3a (Vivo a Napoli Da Quasi 3 anni).

15. Se si è scelto di installare Sentinel Control Center, verrà visualizzato un prompt di dimensioni heap JVM (Java Virtual Machine):
- Dimensioni heap JVM (MB) – Per default, è impostato sulla metà della memoria fisica rilevata nel computer, con un limite massimo di 1024 MB. Si tratterà delle dimensioni heap JVM massime utilizzate solo da Sentinel Control Center.



The screenshot shows a text-based prompt: "The installer has detected 2048 MB of physical memory. Please specify the desired JVM heap size for Sentinel Control Center. The legal range is 64-1024." Below this text is a label "JVM Heap Size (MB)" and a text input field containing the value "1024".

16. Se si sceglie di installare il *servizio di raccolta*, sarà possibile decidere di proteggere o meno Gestione servizi di raccolta di Wizard con una password. Se si sceglie di

proteggere Gestione servizi di raccolta di Wizard, verrà chiesto di creare un'apposita password.

NOTA: la protezione del servizio di raccolta di Wizard con una password richiederà di specificare la password per il caricamento, lo scaricamento o il debug di raccolte in Gestione servizi di raccolta di Wizard. Questa password va aggiunta al nome utente e alla password di Sentinel necessari per eseguire il login a Gestione servizi di raccolta di Wizard.

NOTA: per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, Sentinel richiede una password con le caratteristiche seguenti:

1. Scegliere password costituite da un minimo di 8 caratteri, di cui almeno uno MAIUSCOLO, uno minuscolo, uno speciale (!@#\$\$%^&*()_+) e uno numerico (0-9).
 2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.
 3. La password non deve essere una parola "comune", ovvero una parola inclusa nel dizionario o di uso gergale.
 4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione di password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.
 5. È consigliabile scegliere una password facile da ricordare e allo stesso tempo complessa. Ad esempio, Mfhq5!ao (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#3a (Vivo a Napoli Da Quasi 3 anni).
-

Opzioni di protezione con password di Gestione servizi di raccolta:

- Non proteggere Gestione servizi di raccolta con password
- Proteggi Gestione servizi di raccolta tramite password

Password:

Conferma password:

17. Se si è scelto di installare DAS, selezionare la quantità di RAM del sistema che si desidera allocare per Data Access Service. Per gli ambienti distribuiti, è consigliabile selezionare la quantità massima di memoria (4 GB). Per gli ambienti indipendenti, è consigliabile selezionare metà della memoria RAM.

Selezionare la quantità di memoria (RAM) da allocare ai processi del server di accesso ai dati di Sentinel. Per ottenere prestazioni ottimali, allocare la massima quantità di memoria possibile.

1 Gigabyte ▼

18. Per l'installazione del database, saranno visualizzati i prompt seguenti
- Selezionare la piattaforma del server di database di destinazione come Oracle 9i e selezionare una delle opzioni seguenti:
 - Creare un nuovo database con oggetti di database – Consente di creare una nuova istanza di database Oracle e di inserire automaticamente nella nuova istanza gli oggetti di database.
 - Aggiungi oggetti di database a un database vuoto esistente - Consente solo di aggiungere il database a un'istanza di database Oracle esistente. L'istanza di database esistente deve essere vuota con l'eccezione della presenza dell'utente esecdba.
 - Specificare la directory dei log di installazione del database (default: \$ESEC_HOME/logs/db). Accettare la directory dei log di installazione del database di default o fare clic su *Sfoggia* per specificare un'ubicazione diversa.

Selezionare la piattaforma server del database di destinazione:

Oracle 9i ▼

- Creare un nuovo database con oggetti di database.
- Aggiungi oggetti di database a un database vuoto esistente.

Directory log di installazione database:

/opt/sentinel5.1.3.0/logs/db

Sfoggia

- Fare clic su *OK* sul nome utente Oracle di default.

Please enter the Oracle Username:

oracle

- Se si è scelto di creare un nuovo database, specificare gli elementi seguenti:
 - Il percorso per il file del driver JDBC Oracle (in genere il nome del file jar è ojdbc14.jar). Percorso completo del file jar, in genere \$ORACLE_HOME/jdbc/lib/ojdbc14.jar (in questo campo non è possibile utilizzare variabili di ambiente).
 - Nome host – Il nome host del computer in cui installare il database. Questo campo non è configurabile se si sta creando una nuova istanza del database.
 - Nome database – Il nome dell'istanza di database da installare.

Oracle Configuration

Select the Oracle JDBC driver (ojdbc14.jar):

/export/home/oracle/OraHome/jdbc/lib/ojdbc14.jar

Host Name: 192.168.2.1

Database Name: ESEC

- Se si è scelto di aggiungere oggetti di database a un database Oracle esistente vuoto, verrà richiesto di specificare le informazioni seguenti.

- Il percorso per il file del driver JDBC Oracle (in genere il nome del file jar è ojdbc14.jar). Percorso completo del file jar, in genere \$ORACLE_HOME/jdbc/lib/ojdbc14.jar (in questo campo non è possibile utilizzare variabili di ambiente).
- Nome database o indirizzo IP – Il nome o l'indirizzo IP dell'host in cui si trova il database di Oracle al quale si desidera aggiungere oggetti di database. Può essere il nome host locale o un nome host remoto.
- Nome database – Il nome dell'istanza di database vuoto Oracle esistente al quale si desidera aggiungere oggetti di database (il valore di default è ESEC). Questo nome di database deve essere visualizzato come nome di servizio nel file tnsnames.ora (nella directory \$ORACLE_HOME/network/admin/) del computer dal quale si sta eseguendo il programma di installazione.

NOTA: se il nome del database non è presente nel file tnsnames.ora, il programma di installazione non visualizzerà un errore a questo punto dell'installazione (poiché verifica la connessione utilizzando una connessione JDBC diretta), ma l'installazione del database non riuscirà quando il programma di installazione tenterà di connettersi al database via sqlplus. Se l'installazione del database ha esito negativo, a questo punto, è possibile tornare a questo prompt e correggerne il nome.

- Porta di database (il valore di default è 1521)
- Per l'utente amministratore del database di Sentinel (DBA), specificare la password per l'utente "esecdba". Il campo nome utente in questo prompt non è modificabile.

- f. Se si è scelto di creare un nuovo database, verrà visualizzato il prompt seguente:
- Memoria Oracle (MB) – La quantità di RAM da allocare a questa istanza del database di Oracle.
 - Porta listener – La porta sulla quale creare un listener Oracle (il valore di default è 1521).
 - Password dell'utente SYS e conferma password - SYS è l'utente di default di Oracle La password utente verrà impostata sul valore specificato in questo campo.
 - Password dell'utente SYSTEM e conferma password - SYSTEM è l'utente di default di Oracle La password utente verrà impostata sul valore specificato in questo campo.

Oracle Configuration

Oracle Memory (MB):

ListenerPort:

SYS User Credentials SYSTEM User Credentials

Password: Password:

Confirm Password: Confirm Password:

- g. Se si è scelto di creare un nuovo database, verrà richiesto di specificare le dimensioni del database: Sono disponibili le opzioni seguenti:
- Standard (20 GB)
 - Grandi (400 GB)
 - Personalizzate (specificare le dimensioni manualmente). Se si seleziona questa opzione verrà richiesto di specificare:
 - dimensione iniziale di ogni file di database in MB (100 – 10.000)
 - dimensione massima di ogni file di database in MB (2.000 – 100.000)
 - dimensione di tutti i file di database in MB (7.000 – 2.000.000)
 - dimensione di ogni file di log in MB (100 – 100.000)

Please select Standard, Large, or Custom database size.

Standard (20,000MB, 30 day capacity @ 500,000 events per day)

Large (400,000MB, 30 day capacity @ 10,000,000 events per day)

Custom (specify database sizing manually)

- h. Se si è scelto di creare un nuovo database, verrà richiesto di specificare l'ubicazione di memorizzazione per i file di database seguenti.

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

Il programma di installazione non creerà tali directory, per cui è necessario crearle esternamente prima di continuare.

È necessario che tali directory siano accessibili in scrittura dall'utente Oracle.

- Directory dati
- Directory indice
- Directory dati di riepilogo
- Directory indice di riepilogo
- Directory dei file temporanei e dello spazio delle tabelle di annullamento
- Directory log di ripetizione membro A
- Directory log di ripetizione membro B

Please enter the storage location for the following database files.

Data Directory:	<input type="text" value="/opt/oracle"/>	...
Index Directory:	<input type="text" value="/opt/oracle"/>	...
Summary Data Directory:	<input type="text" value="/opt/oracle"/>	...
Summary Index Directory:	<input type="text" value="/opt/oracle"/>	...
Temp and Undo Directory:	<input type="text" value="/opt/oracle"/>	...
Redo Log Member A Directory:	<input type="text" value="/opt/oracle"/>	...
Redo Log Member B Directory:	<input type="text" value="/opt/oracle"/>	...

- i. Se si è scelto di creare un nuovo database, specificare le informazioni di autenticazione per l'amministratore del database di Sentinel (DBA). Corrisponde a esecdba, il proprietario degli oggetti di database.
 - j. Specificare le informazioni di autenticazione per l'utente del database dell'applicazione Sentinel. Corrisponde a esecapp, il nome utente dell'applicazione Sentinel utilizzato dai processi Sentinel per la connessione al database.
 - k. Specificare le informazioni di autenticazione per l'utente del database amministratore di Sentinel. Corrisponde a esecadm, l'utente amministratore di Sentinel.
 - l. Fare clic su *Avanti* nella finestra di riepilogo dell'installazione del database.
19. Se si è scelto di installare DAS ma di non installare il database di Sentinel, verrà richiesto di specificare le informazioni del database di Sentinel di Oracle seguenti. Queste informazioni saranno utilizzate per configurare DAS perché faccia riferimento al database di Sentinel.
- Nome host del database o indirizzo IP – Il nome o l'indirizzo IP del database di Sentinel di Oracle esistente per il quale si desidera configurare la connessione da parte del componente DAS.
 - Nome database – Il nome o dell'istanza di database vuoto Oracle esistente per il quale si desidera configurare la connessione da parte del componente DAS (il valore di default è ESEC).
 - Porta di database (il valore di default è 1521)
 - Per l'utente del database dell'applicazione Sentinel, specificare il login "esecapp" e immettere la password impostata per questo utente durante l'installazione del database di Sentinel.

Oracle Configuration

Select the Oracle JDBC driver (ojdbc14.jar):

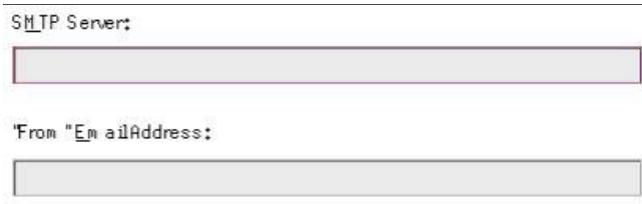
Host name:

Database Name:

Port:

Login: Password:

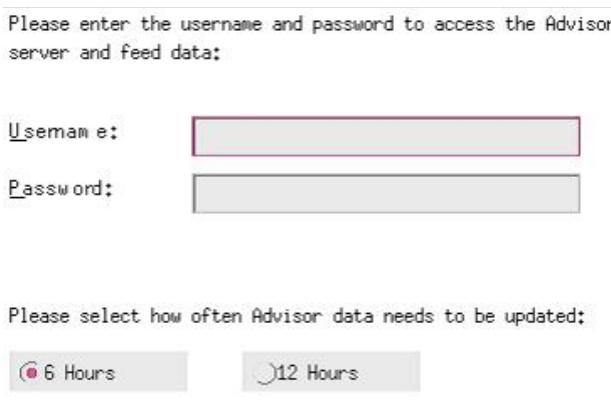
20. Se si è scelto di installare DAS, configurare il supporto e-mail di Sentinel. Specificare il server SMTP e l'indirizzo e-mail del mittente che dovrà essere utilizzato dal servizio di esecuzione per l'invio di messaggi (facoltativo – è possibile modificarlo manualmente dopo l'installazione [\$ESEC_HOME\sentinel\config\execution.properties]):



SMTP Server:

From "EmailAddress:"

21. Se si è scelto di installare Advisor, selezionare il tipo di installazione di Advisor (se l'opzione di Advisor prevedeva la scelta di un nome utente e una password)
- Download Internet diretto – Il computer che esegue Advisor è connesso direttamente a Internet. In questa configurazione, gli aggiornamenti vengono scaricati da Sentinel automaticamente e a scadenze regolari mediante Sentinel.
 - Autonomo - Advisor è configurato come sistema isolato che necessita di interventi manuali per ricevere aggiornamenti da Sentinel.
22. Se si è scelto di installare Advisor e si è selezionato di utilizzare l'opzione Download Internet diretto, specificare nome utente e password Advisor e la frequenza di aggiornamento dei dati di Advisor. Se non è possibile verificare nome utente o password, dopo aver fatto clic su *Avanti* verrà chiesto se si desidera continuare (non consigliabile). Se si sceglie di continuare, digitare di nuovo la password di Advisor nella finestra di conferma della password. In caso contrario correggere la password di Advisor.



Please enter the username and password to access the Advisor server and feed data:

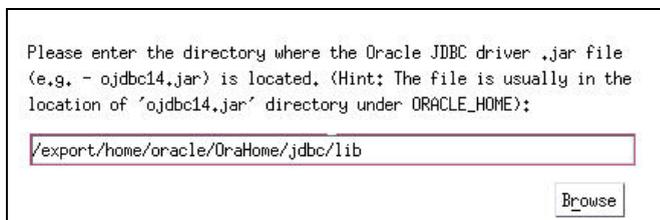
Username:

Password:

Please select how often Advisor data needs to be updated:

6 Hours 12 Hours

23. se si è scelto di installare Advisor, immettere il percorso della directory che contiene il driver Oracle JDBC, generalmente il nome del file è ojdbc14.jar. Percorso completo della directory contenente il file jar del driver, in genere \$ORACLE_HOME/jdbc/lib/ojdbc14.jar (in questo campo non è possibile utilizzare variabili di ambiente).



Please enter the directory where the Oracle JDBC driver .jar file (e.g. - ojdbc14.jar) is located. (Hint: The file is usually in the location of 'ojdbc14.jar' directory under ORACLE_HOME):

Browse

24. Se si è scelto di installare Advisor, specificare:

- La directory in cui saranno memorizzati i file di feed di dati di Advisor. Questa è l'ubicazione in cui vengono salvati i file di attacchi e di flussi di articoli scaricati.

NOTA: la directory con i file dei flussi di dati di Advisor deve disporre delle impostazioni di proprietà seguenti:

Utente – esecadm

Gruppo – esec

Se la directory non dispone di questi diritti di proprietà, eseguire il comando seguente come root:

```
chown esecadm:esec <percorso_directory>
```

-
- L'indirizzo del mittente, visualizzato nelle notifiche di e-mail.
 - L'indirizzo del destinatario, per l'invio delle notifiche di e-mail.

NOTA: dopo l'installazione è possibile cambiare gli indirizzi e-mail di Advisor modificando i file `attackcontainer.xml` e `alertcontainer.xml` nella directory `$ESEC_HOME/sentinel/config`. Per ulteriori informazioni, vedere il *capitolo 7 – Scheda Advisor della Guida dell'utente di Sentinel*.

-
- Selezionare Sì o No a seconda che si desideri ricevere e-mail relative alla riuscita degli aggiornamenti di Advisor. Le notifiche di errori saranno inviate sempre.

Specificare la directory in cui i file di feed di dati di Advisor...

/u01/sentinel5

Sfogli...

Immettere l'indirizzo del destinatario per l'invio delle notifiche tramite e-mail:

Specificare gli indirizzi (separati da virgole) a cui inviare le notifiche tramite e-mail:

Si desidera ricevere notifiche tramite e-mail relative agli aggiornamenti di Advisor eseguiti correttamente (le notifiche degli errori verranno inviate comunque)?

Sì No

25. Se si è scelto di installare HP Service Desk o Remedy Integration, verrà richiesto di specificare altre informazioni. Per ulteriori informazioni, vedere la *Guida all'integrazione con soluzioni di terze parti di Sentinel*.

26. Leggere le informazioni presenti nella schermata visualizzata e al termine fare clic su *Avanti*. Una volta completata l'installazione, verrà chiesto di riavviare il sistema. Fare clic su *Fine* per riavviare il sistema.

27. Il programma di installazione di Sentinel, per default, 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 per evitare che il database interrompa l'accettazione degli eventi.

28. Se si prevede un'elevata frequenza di eventi (superiore ai 500 eventi al secondo), sarà necessario seguire le istruzioni aggiuntive per la configurazione riportate nella sezione [Impostazione della strategia di inserimento di eventi OCI \(Oracle Call Interface\)](#).

Operazioni successive all'installazione di Sentinel 5 per Oracle

Aggiornamento di e-mail Sentinel per l'autenticazione SMTP

Se nel sistema è necessaria l'autenticazione SMTP, sarà necessario aggiornare il file `execution.properties`. Il file si trova nel computer in cui è installato DAS. Nella directory `$ESEC_HOME/sentinel/config`. Per configurare questo file, eseguire `mailconfig.sh` per modificare il file e `mailconfigtest.sh` per eseguire il test delle modifiche.

Per configurare il file `execution.properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
$ESEC_HOME/sentinel/config
```

2. Eseguire il comando `mailconfig` come indicato di seguito:

```
./mailconfig.sh -host <server SMTP> -from <indirizzo e-mail di origine> -user <utente autenticazione posta> -password
```

Esempio:

```
./mailconfig.sh -host 10.0.1.14 -from my_name@domain.com -user my_user_name -password
```

Dopo aver immesso questo comando verrà richiesto di specificare una nuova password.

```
Immettere la password:*****
```

```
Confermare la password:*****
```

NOTA: quando si utilizza l'opzione relativa alla password, deve trattarsi dell'ultimo argomento.

Per eseguire il test della configurazione del file `execution properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
$ESEC_HOME/sentinel/config
```

2. Eseguire il comando `mailconfigtest` come indicato di seguito:

```
./mailconfigtest.sh -to <indirizzo e-mail di destinazione>
```

Se l'invio del messaggio e-mail è riuscito correttamente, il messaggio sarà ricevuto all'indirizzo di destinazione e verrà visualizzato il messaggio seguente sullo schermo dell'utente.

```
Messaggio e-mail inviato.
```

Controllare la casella postale e-mail per confermare la ricezione del messaggio.

La riga dell'oggetto e il contenuto dovrebbero essere:

```
Oggetto: Testing Sentinel mail property
```

This is a test for Sentinel mail property set up. If you see this message, your Sentinel mail property has been configured correctly to send emails

Database di Sentinel

Dopo aver installato il database di Sentinel, il database conterrà gli utenti di default seguenti:

- esecdba – Proprietario schema database. I privilegi DBA non sono concessi all'utente esecdba per motivi di sicurezza. Per utilizzare Enterprise Manager, creare un utente con privilegi DBA.
- esecapp – Utente applicazione database. Corrisponde all'utente dell'applicazione utilizzata per la connessione al database.
- esecadm – Utente di database corrispondente all'amministratore di Sentinel. Non corrisponde allo stesso conto utente utilizzato dall'utente esecadm del sistema operativo.
- esecrpt – Utente rapporti database
- SYS – Utente database SYS
- SYSTEM – Utente database SYSTEM

Servizio di raccolta

Durante l'installazione del servizio di raccolta, saranno installati i servizi di raccolta seguenti per l'esecuzione di ognuno dei quali sarà impostata una porta del servizio di raccolta.

Prodotto	Nome servizio di raccolta
Servizi di raccolta dimostrativi	
Test per il caricamento di risorse, funziona con servizio di raccolta DemoEvents	DemoAssetUpload
Test degli eventi demo, funziona con servizi di raccolta DemoAssetUpload e DemoVulnerabilityUpload	DemoEvents
Test per il caricamento di vulnerabilità, funziona con servizio di raccolta DemoEvents	DemoVulnerabilityUpload
Test per l'invio di un evento	SendOneEvent
Test per l'invio di più eventi	SendMultipleEvents

NOTA: per ulteriori informazioni relative alla configurazione dei servizi di raccolta dimostrativi, vedere il *capitolo 12, Test dell'installazione*.

NOTA: per servizi di raccolta aggiuntivi, visitare il portale del servizio clienti Sentinel. Per ulteriori informazioni (anche sulla configurazione) utilizzare la documentazione fornita per ogni servizio di raccolta in:

[\\$WORKBENCH_HOME/Elements/<nome servizio di raccolta>/Docs/](#)

Per installare altri servizi di raccolta, eseguire lo script del Service Pack sul CD del Service Pack. Lo script installerà i servizi di raccolta in locale.

In Windows:

```
.\service_pack.bat
```

In UNIX:

```
./service_pack.sh
```

Per istruzioni sull'installazione del Service Pack e per un elenco dei servizi di raccolta, vedere le *Note di rilascio del Service Pack*.

Aggiornamento del codice di licenza

Aggiornamento del codice di licenza (Solaris)

1. Eseguire il login come utente esecadm.
2. Aprire \$ESEC_HOME/utilities.
3. Immettere il comando seguente:

```
./softwarekey
```
4. Immettere il numero 1 per specificare la chiave primaria. Premere Invio.

Creazione di un'istanza Oracle per il database di Sentinel

NOTA: questa procedura viene riportata come esempio della creazione di spazi delle tabelle personali anziché utilizzare la funzione di creazione di spazi delle tabelle fornita nel CD di installazione. I valori relativi alle dimensioni possono essere diversi a seconda della configurazione e dei requisiti del sistema. Gli spazi delle tabelle devono essere denominati esattamente come segue.

Nell'istanza Oracle sarà necessario configurare:

- parametri
- spazi delle tabelle

Creazione di 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.

Parametri consigliati per la configurazione minima di Solaris	
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

Parametri consigliati per la configurazione minima di Solaris	
Parametri	Dimensioni (byte o specificato diversamente)
open_cursors	500
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Parametri minimi per le dimensioni dello spazio delle tabelle in Solaris		
Spazio delle tabelle	Dimensioni esempio	Note
REDO	3 x 100 M	Corrisponde al valore minimo. Nel caso di EPS elevato creare log di ripetizione di dimensioni maggiori.
SYSTEM	500 M	Valore minimo
TEMP	1 G	Valore minimo
UNDO	1 G	Valore minimo
ESENTD	5 G	Valore minimo Per i dati evento
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 evento
ESENTX2	500 M	Valore minimo Indice per configurazione, risorse, vulnerabilità e associazioni (estensione automatica abilitata)
SENT_ADVISORD	200 M	Valore minimo Per dati di Advisor (estensione automatica abilitata)
SENT_ADVISORX	100 M	Valore minimo Per indice di Advisor (estensione automatica abilitata)
SENT_LOBS	100 M	Valore minimo Per oggetti di database di grandi dimensioni (estensione automatica abilitata)
SENT_SMRYD	3 G	Valore minimo Per aggregazione, dati di riepilogo
SENT_SMRYX	2 G	Valore minimo Per aggregazione, indice di riepilogo

3. Eseguire lo script createEsecdba.sh presente 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.

Impostazione della strategia di inserimento eventi OCI (Oracle Call Interface)

Sentinel 5.1 fornisce un framework per l'utilizzo di strategie diverse per inserire eventi nel database. Sentinel 5.1 fornisce due strategie per inserire eventi nel database Oracle.

- JDBCLoadStrategy
- OCILoadStrategy

La strategia da utilizzare per l'inserimento di eventi è regolata dalla proprietà `insert.strategy` del componente `EventStoreService` in `das_binary.xml`.

La strategia JDBC è la strategia di default configurata pronta per l'utilizzo.

La strategia OCI è una strategia di inserimento nativa per l'inserimento di eventi più rapido. Per questa strategia è necessario che le librerie OCI Oracle siano installate nel computer che esegue il componente DAS. La strategia OCI deve essere utilizzata in configurazioni in cui si prevede un'elevata frequenza di eventi.

Il numero di eventi da raggruppare per l'inserimento nel database è regolato dalla proprietà `insert.batchsize`. La proprietà `insert.batchsize` è utilizzata da tutte le strategie di inserimento di eventi.

Per cambiare la strategia di inserimento eventi di Sentinel da quella di default JDBC alla strategia OCI, è necessario eseguire alcune operazioni.

Modifica della strategia di inserimento di eventi da JDBC a OCI

1. Verificare che le librerie OCI Oracle siano installate nel computer che esegue il componente DAS di Sentinel. Sarà necessario conoscere il percorso di `ORACLE_HOME` nei passaggi seguenti.
2. Eseguire il login al computer come utente `esecadm` dal passaggio 1.
3. Creare un file “.profile” nella home directory dell'utente `esecadm`. Inserirvi il testo seguente (modificare il percorso di `ORACLE_HOME` in modo che sia conforme all'installazione in uso):

```
ORACLE_HOME=/build/home/oracle/OraHome
export ORACLE_HOME
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

4. Aprire il file `$ESEC_HOME/sentinel/config/das_binary.xml` per la modifica in qualsiasi editor di testo.
5. Eseguire una ricerca del testo seguente:

```
JDBCLoadStrategy
```

6. Modificare il testo in:

```
OCILoadStrategy
```

7. Salvare la modifica nel file `das_binary.xml`.
8. Riavviare l'applicazione DAS Binary. Il riavvio di DAS Binary può essere eseguito più facilmente eseguendo il comando `"ps -ef | grep DAS_Binary"` per ottenere l'ID del processo, interrompendo il processo e consentendo alla sorveglianza di Sentinel di riavviare automaticamente il processo.

Una volta riavviato DAS Binary, verrà caricata la libreria \$ESEC_HOME/sentinel/lib/libocievent.so che sarà utilizzata per eseguire l'inserimento di eventi nel database tramite OCI.

Altre opzioni per l'inserimento di eventi OCI

Oltre a specificare "OCILoadStrategy" nel file das_binary.xml, è possibile configurare diverse altre opzioni relative a OCI.

- insert.batchsize – Questa impostazione consente di configurare il numero massimo di eventi da inserire nel database contemporaneamente.
- insert.oci.workerCount – Questa impostazione consente di configurare il numero di thread da utilizzare per inserire dati di eventi nel database.
- insert.oci.queueWaitTime – Questa impostazione consente di specificare il tempo massimo di attesa in secondi per l'inserimento dei dati dalla coda in entrata nel database. Quando si riceve un "batchsize" di eventi completo, viene inserito l'intero batch. Ma se il flusso di eventi in entrata è lento, il tempo di attesa della coda viene utilizzato per determinare quando eseguire l'inserimento nel database (anche se non è stato ancora ricevuto un batch completo di eventi).
- insert.oci.highWatermark – Il limite massimo della coda di eventi.
- insert.oci.lowWatermark – Il limite minimo della coda di eventi.
- insert.oci.optimizationFlag – Flag di ottimizzazione. "Attivo" o "Disattivo".

Suggerimenti per il debug di OCI

L'interfaccia OCI registra i messaggi nel file \$ESEC_HOME/sentinel/log/ocievent.log. I messaggi iniziali scritti nel file di log devono includere messaggi relativi a corretta o non riuscita connessione al database... Si tratta di una buona occasione per verificare che la libreria OCI sia stata caricata e configurata correttamente.

L'interfaccia OCI registra anche gli errori nel file di log das_binary memorizzato nella directory \$ESEC_HOME/sentinel/log. Gli errori registrati nel file di log das_binary comprendono errori di individuazione/caricamento della libreria libocievent.so, errori di connessione al database ed errori di inserimento eventi/ associazioni di eventi.

Se i messaggi di errore indicano che il file "libocievent.so" non è stato individuato o caricato, sarà necessario controllare tre cose:

1. Verificare che le librerie OCI Oracle siano installate.
2. Verificare che il file "libocievent.so" sia memorizzato nella directory \$ESEC_HOME/sentinel/lib.
3. Verificare che la directory "\$ESEC_HOME/sentinel/lib" sia in "LD_LIBRARY_PATH" dell'utente "esecadm". In caso contrario sarà possibile aggiornare LD_LIBRARY_PATH nel profilo dell'utente "esecadm".
4. Verificare che le variabili di ambiente ORACLE_HOME e LD_LIBRARY_PATH siano aggiornate correttamente nelle variabili di ambiente dell'utente esecadm come descritto nella sezione "Modifica della strategia di inserimento di eventi da JDBC a OCI".

4

Installazione di Sentinel 5 per Oracle in Linux

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo viene descritto come installare Sentinel Enterprise Security Management Sentinel 5 per Oracle in SuSE Linux Enterprise Server e Red Hat Enterprise Linux

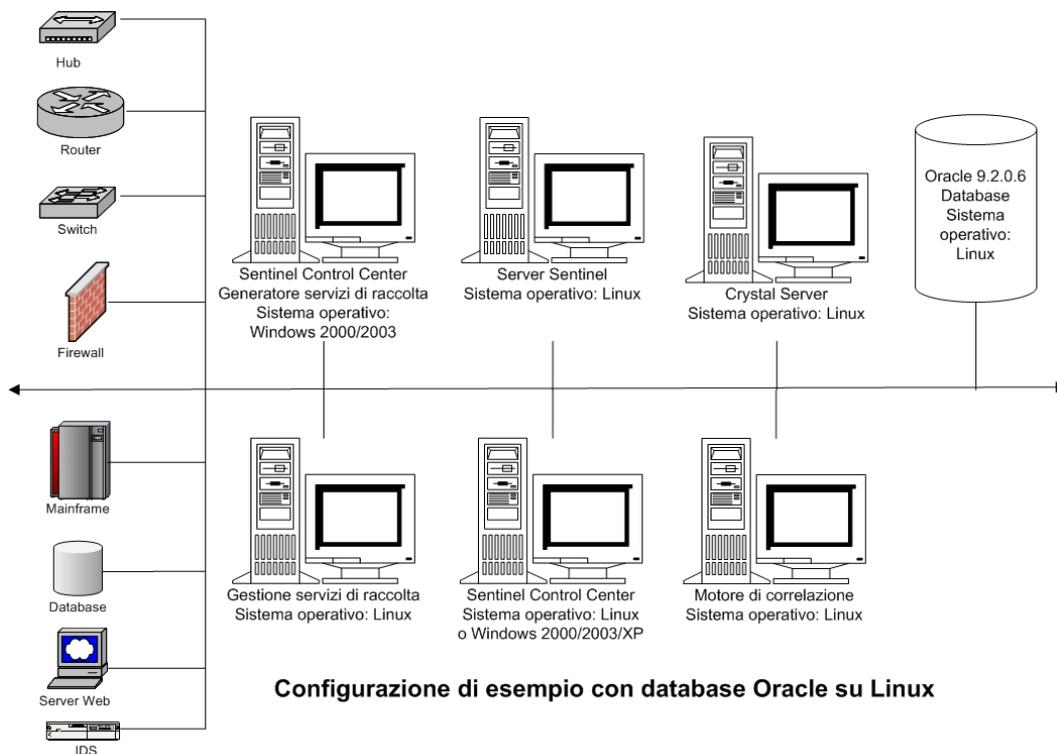
Operazioni preliminari all'installazione di Sentinel 5 per Oracle in Linux

NOTA: prima dell'installazione, verificare che il computer in uso soddisfi i requisiti minimi di sistema e che il sistema operativo sia stato ottimizzato utilizzando le procedure consigliate correnti per la sicurezza.

NOTA: installare Oracle Enterprise con partizionamento. In Gestione dati Sentinel questa funzione è necessaria per la gestione del database di Sentinel.

NOTA: quando si esegue un'installazione completa di Sentinel dopo averne rimosso una precedente, è necessario rimuovere alcuni file e impostazioni del sistema derivanti dall'installazione precedente. Se non si rimuovono tali file o impostazioni la nuova installazione completa potrebbe non riuscire. Questa operazione deve essere eseguita su ogni computer sul quale si sta eseguendo una nuova installazione. Per ulteriori informazioni, vedere *l'appendice E*.

Le configurazioni tipiche di Linux per Sentinel sono le seguenti. La configurazione dell'utente potrebbe essere diversa, a seconda dell'ambiente in uso. Indipendentemente dalla configurazione selezionata, è necessario installare prima il database.



NOTA: Linux fa riferimento a SUSE Linux 9 o Red Hat Enterprise Linux 3

NOTA: per ulteriori informazioni sui sistemi operativi supportati, vedere la *sezione sulle piattaforme supportate per il server Sentinel su Linux nel capitolo 1 "Introduzione"*.

Per ottenere un codice di licenza

Per l'installazione e l'esecuzione del servizio DAS (Database Access Service) del server Sentinel è necessario disporre di un codice di licenza valido. Tale codice di licenza è bloccato per il computer nel quale si installa DAS. Il codice di licenza emesso per un computer non funzionerà su un computer diverso.

Per ottenere il codice di licenza, è necessario determinare l'ID host e fornire tali informazioni a Novell che provvederà all'assegnazione di un codice di licenza.

Per determinare l'ID dell'host (Linux)

1. Eseguire il login come utente radice.
2. Inserire e montare il CD di installazione di Sentinel.
3. Passare alla directory utilities/linux, quindi immettere:

```
./esehostid
```

4. Inviare l'ID host al Supporto tecnico Novell. Il Supporto clienti fornirà il codice di licenza richiesto.

Database di Sentinel

Prima di installare il database di Sentinel, sarà necessario accertarsi di disporre di quanto segue:

- Per i requisiti hardware, vedere i *capitoli 1 e 2*.
- SuSE Linux Enterprise Server 9 con SP2 o Red Hat Enterprise Linux 3 Update 5 ES (x86)
- Oracle 9i Enterprise Edition 9.2.0.6 (solo SuSE Linux) o 9.2.0.7 con partizionamento
- Utente del sistema operativo Oracle (default: oracle)
- Verificare che siano impostate le seguenti variabili di ambiente per il sistema operativo Oracle:

ORACLE_HOME

ORACLE_BASE

PATH (deve essere \$ORACLE_HOME/bin)

- Sebbene non sia consigliabile, se si crea manualmente l'istanza del database Oracle, vedere [Creazione di un'istanza di Oracle per il database di Sentinel](#) per istruzioni sulla creazione dell'istanza di Oracle. Se si seleziona questa opzione, è comunque necessario utilizzare il programma di installazione per aggiungere gli oggetti di database all'istanza del database Oracle creata manualmente, (vedere [Installazione personalizzata](#) per istruzioni sull'esecuzione di questa operazione).

NOTA: se si utilizza un'istanza di database Oracle esistente o creata manualmente, è necessario che sia vuota con l'eccezione della presenza dell'utente esecdba.

La sezione [Creazione di un'istanza di Oracle per il database di Sentinel](#) include le istruzioni per la creazione di questo utente, se non esiste già.

- Se si utilizza il programma di installazione per creare l'istanza di database Oracle (opzione consigliata), sarà necessario conoscere i percorsi di directory in cui ubicare i file di database. Tali directory devono esistere prima di eseguire il programma di installazione perché non sarà possibile crearle durante l'installazione. È inoltre necessario che tali directory siano accessibili in scrittura dall'utente del sistema operativo Oracle (ovvero – oracle).

NOTA: per motivi connessi alle prestazioni, a seconda che si stia eseguendo l'installazione in RAID e che l'ambiente RAID lo consenta, il Redo Log dovrebbe fare riferimento al disco con scrittura più veloce disponibile.

NOTA: per default, il programma di installazione imposta gli spazi delle tabelle seguenti perché le dimensioni NON aumentino automaticamente: ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX. Tutti gli altri spazi delle tabelle sono impostati per l'aumento automatico delle relative dimensioni. Il motivo per il quale non viene consentito l'aumento automatico di ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX è che contengono dati di eventi e dati di eventi di riepilogo. L'utilizzo dello spazio per gli eventi e i riepiloghi può essere notevolmente dinamico. È necessario monitorare ed estendere questi spazi di tabelle in maniera controllata in base alla configurazione del file system e tenendo in considerazione il bilanciamento IO e le attività di backup e recupero del database.

È consigliabile pianificare la gestione della partizione di Gestione dati Sentinel (archiviazione, eliminazione e aggiunta di partizioni) per limitare le dimensioni dei dati degli eventi.

Server Sentinel

NOTA: se non si intende installare il database di Sentinel contemporaneamente al server Sentinel, è necessario installare prima il database di Sentinel.

Prima di installare il server Sentinel, sarà necessario accertarsi di disporre di quanto segue:

- Per i requisiti hardware, vedere i *capitoli 1 e 2*.
- SuSE Linux Enterprise Server 9 con SP2 o Red Hat Enterprise Linux 3 Update 5 ES (x86)
- Numero di serie e codice licenza per Novell Sentinel 5 (per DAS). Per ulteriori informazioni, vedere [Per ottenere un codice di licenza](#).
- Server SMTP – Necessario per l'invio di e-mail da Sentinel.

Sentinel Control Center e Wizard

Prima di installare il server Sentinel, sarà necessario accertarsi di disporre di quanto segue:

- Per i requisiti hardware, vedere il *capitolo 1 e 2*
- SuSE Linux Enterprise Server 9 con SP2 o Red Hat Enterprise Linux 3 Update 5 ES (x86) o
- (Generatore servizi di raccolta Sentinel e Sentinel Control Center) – Windows 2000 o 2003

Advisor

Per installare Advisor, sarà necessario ottenere un ID Advisor e una password da Sentinel. Download Internet diretto utilizza la porta 443.

NOTA: se si intende utilizzare Advisor solo per il rilevamento dell'utilizzo, non sarà necessario installare il software Crystal Enterprise. È infatti necessario solo se si intende eseguire Crystal Reports for Sentinel. Per ulteriori informazioni, vedere il *capitolo 10, Configurazione di Advisor*.

Operazioni preliminari all'installazione di Oracle in Linux

Per installare Oracle in Linux per Sentinel, è necessario avere eseguito le operazioni seguenti:

- Impostazione dei valori del kernel
- Creazione di un gruppo e di un conto utente per Oracle
- Impostazione delle variabili d'ambiente per l'utente Oracle.
- Collegamento di gcc
- Applicazione di patch del sistema operativo Linux per l'installazione Oracle 9.2.0.4 (ottenere la patch p3006854_9204_LINUX direttamente da Oracle)
- Installazione di Oracle 9.2.0.4 (ottenere questo software direttamente da Oracle)
- Applicazione di patch da Oracle 9.2.0.4 a Oracle 9.2.0.6 (solo SuSE Linux) o 9.2.0.7 (ottenere la patch Oracle 9.2.0.6 o 9.2.0.7 direttamente da Oracle)

Impostazione dei valori del kernel per Oracle su Linux (SuSE e Red Hat)

Per Oracle in Linux è necessario impostare i valori seguenti.

ESCLUSIONE DI GARANZIA: i seguenti sono i valori minimi consigliati. Se le impostazioni di sistema sono maggiori di quelle specificate nella tabella seguente, non modificarle. Per ulteriori informazioni consultare l'amministratore del sistema e la documentazione Oracle.

- | | |
|-------------------------------------|---------------|
| ▪ shmmax=2147483648 (valore minimo) | ▪ semmni=1024 |
| ▪ shmmni=4096 | ▪ semmsl=1024 |
| ▪ semmns=32000 | ▪ semopm=100 |

1. Eseguire il login come utente radice.
2. Impostare i parametri del kernel aggiungendo il testo seguente alla fine del file “/etc/sysctl.conf”:

NOTA: le impostazioni seguenti corrispondono ai valori minimi consigliati. Se le impostazioni correnti sono maggiori di quelle seguenti, non modificarle. Per determinare l’opzione correntemente impostata per un particolare parametro del kernel, eseguire il comando:

```
sysctl <kernel_parametro>
```

Per controllare ad esempio il valore corrente del parametro del kernel “kernel.sem”, eseguire il comando:

```
sysctl kernel.sem
```

```
# Kernel settings for Oracle
# kernel.sem = <SEMMSL> <SEMNS> <SEMOPM> <SEMMNI>
kernel.sem = 1024          32000    100      1024
kernel.shmmax = 2147483648
kernel.shmmni = 4096
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
```

3. Per caricare le modifiche nel file “/etc/sysctl.conf”, eseguire il comando seguente:

```
sysctl -p
```

4. 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”. Se l’id utente di Oracle è diverso, sostituire “oracle” nel testo seguente con il proprio ID utente corrispondente.

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

Operazioni preliminari all’installazione di Oracle in SuSE Linux

Operazioni preliminari all’installazione di Oracle in SuSE Linux

ESCLUSIONI DI GARANZIA: le istruzioni seguenti non devono essere considerate sostitutive della documentazione Oracle. Si tratta solo di un esempio di uno scenario di impostazione. È consigliabile attenersi scrupolosamente a queste istruzioni. La configurazione specifica può essere diversa. Per ulteriori informazioni consultare documentazione del sistema operativo e di Oracle.

1. Attenersi alle istruzioni di installazione disponibili nel manuale di installazione di SLES 9. Installare SLES 9 con i pacchetti di default insieme al *compilatore C/C++ e agli strumenti*.

NOTA: se si è già installato SuSE Linux, è possibile utilizzare YaST nell'interfaccia utente grafica per installare il *compilatore C/C++ e gli strumenti*.

2. Eseguire il login come utente radice.
3. Accedere per controllare il livello del kernel.

```
uname -r
```

È necessario un valore kernel di 2.6*. Ad esempio, un livello kernel 2.6.5-7.97 è appropriato.

4. Installare gcc_old-2.95.3-175.2.i586.rpm incluso nel CD 1 di SLES 9 SP2.

```
rpm -i <path>/ gcc_old-2.95.3-175.2.i586.rpm
```

5. Accedere per verificare che sia in esecuzione SP2:

```
SPident
```

oppure

```
cat /etc/SuSE-release
```

Il risultato dovrebbe essere:

```
CONCLUSION: System is up-to-date!
```

```
Found SLES-9-i386-SP2
```

oppure

```
SUSE LINUX Enterprise Server (i586)
```

```
VERSION = 9
```

```
PATCHLEVEL = 2
```

6. Per automatizzare al massimo i task di preinstallazione di Oracle e creare l'utente oracle, installare orarun-1.8-109.15.i586.rpm.

NOTA: consultare la documentazione di installazione di Oracle per un elenco completo di prerequisiti.

```
rpm -i <path>/orarun-1.8-109.15.i586.rpm
```

NOTA: orarun è inoltre disponibile sul sito all'indirizzo <http://www.novell.com>:

```
export LD_ASSUME_KERNEL=2.4.21
```

```
export LD_PRELOAD=/usr/lib/libInternalSymbols.so
```

7. 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 /etc/passwd.
8. Impostare una nuova password per l'utente oracle mediante YaST o accedendo.

```
/usr/bin/passwd oracle
```

9. Per impostare i parametri del kernel, eseguire

```
/usr/sbin/rcoracle start
```

Ignorare eventuali errori.

10. Per installare Oracle 9.2.0.4 dal disco 1, eseguire lo script:

```
./runinstaller
```

11. 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.

- Quando viene richiesto il nome del gruppo UNIX, immettere: dba
- Quando viene richiesto di specificare il tipo di installazione, scegliere Personalizzata.

Selezionare i componenti seguenti per installarli:

- Oracle 9i 9.2.0.4.0
- Enterprise Edition Options 9.2.0.1.0
 - Oracle Partitioning 9i 9.2.0.4.0
- Oracle Net Services 9.2.0.1.0
 - Oracle Net Listener 9.2.0.4.0
- Prodotti di Oracle Enterprise Manager 9.2.0.1.0 (Tutti)
- Development kit di Oracle 9i 9.2.0.1.0 (Completo)
- Oracle 9i per la documentazione UNIX 9.2.0.1.0
- Oracle HTTP Server 9.2.0.1.0 (Completo)
- iSQL*Plus 9.2.0.4.0 (Completo)
- Interfacce di Oracle JDBC/OCI 9.2.0.1.0

12. Quando viene chiesto se si desidera creare il database, scegliere NO.

13. In alternativa, annullare tutti gli assistenti della configurazione avviati dal programma di installazione.

14. Modificare il file `/opt/oracle/network/admin/sqlnet.ora` (oppure crearlo se non esiste) in modo che contenga il testo seguente (rimuovere dal file tutte le informazioni esistenti senza commenti):

```
NAMES DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
```

15. Per applicare la patch Oracle 9.2.0.6 a Oracle Installer, dal disco 1 di distribuzione della patch Oracle 9.2.0.6, eseguire lo script:

NOTA: la patch Oracle 9.2.0.6 viene applicata solo dopo l'applicazione delle patch a Oracle Installer.

```
./runInstaller
```

16. 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 introduttiva, fare clic su *Avanti*.
- Nella schermata Specify File Locations (Specifica ubicazione file), per Destination Name (Nome destinazione) scegliere *"OUIHome"* nell'elenco a discesa (o qualsiasi cosa si sia specificato come Destination Name (Nome destinazione) durante l'installazione di Oracle 9.2.0.4). Fare quindi clic su *Avanti*.
- Nella schermata Select Product to Install (Seleziona prodotto da installare), scegliere *"Oracle Universal Installer 10.1.0.3.0"*. Quindi fare clic su *Avanti*.
- Nella schermata di riepilogo, esaminare il riepilogo dell'installazione e fare clic su *Install (Installa)*.
- Nella schermata di completamento dell'installazione fare clic su *Exit (Esci)*.

17. Per applicare la patch Oracle 9.2.0.6 o 9.2.0.7 a Oracle, dal disco 1 di distribuzione della patch Oracle 9.2.0.6 o 9.2.0.7, eseguire lo script:

```
./runInstaller
```

18. 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 introduttiva, fare clic su *Avanti*.
 - Nella schermata Specify File Locations (Specifica ubicazione file), per Destination Name (Nome destinazione) scegliere "OUIHome" nell'elenco a discesa (o qualsiasi cosa si sia specificato come Destination Name (Nome destinazione) durante l'installazione di Oracle 9.2.0.4). Fare quindi clic su *Avanti*.
 - In base alla versione in uso, nella schermata Select Product to Install (Seleziona prodotto da installare) scegliere "Oracle 9iR2 Patchset 9.2.0.6.0". Quindi fare clic su *Avanti*.
 - Nella schermata di riepilogo, esaminare il riepilogo dell'installazione e fare clic su *Install (Installa)*.
 - Nella schermata di completamento dell'installazione fare clic su *Exit (Esci)*.

Operazioni preliminari all'installazione di Oracle in Red Hat Linux

Operazioni preliminari all'installazione di Oracle in Red Hat Linux

ESCLUSIONI DI GARANZIA: le istruzioni seguenti 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 **/export/home/oracle** e che Oracle venga installato in **/opt/oracle**. La configurazione specifica può essere diversa. Per ulteriori informazioni consultare documentazione del sistema operativo e di Oracle.

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 dba
```
3. Aggiungere l'utente Oracle come root:

```
useradd -g dba -s /bin/bash -d /export/home/oracle -m oracle
```
4. Creare una directory per ORACLE_HOME e ORACLE_BASE:

```
mkdir -p /opt/oracle/
```
5. Modificare la proprietà della directory ORACLE_BASE e passare a un livello inferiore di oracle/dba:

```
chown -R oracle:dba /opt/oracle
```
6. Passare all'utente Oracle:

```
su - oracle
```
7. 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 esecadm.

```
# Set the LD_ASSUME_KERNEL environment variable only for
  Red Hat 9,
# RHEL AS 3, and RHEL AS 4 !!
# Use the "Linuxthreads with floating stacks"
  implementation instead of NPTL:
# for RH 9 and RHEL AS 3
export LD_ASSUME_KERNEL=2.4.1
# for RHEL AS 4
# export LD_ASSUME_KERNEL=2.4.19
# Oracle Environment
export ORACLE_BASE=/opt/oracle
export ORACLE_HOME=$ORACLE_BASE/
export ORACLE_SID=test
export ORACLE_TERM=xterm
# export TNS_ADMIN= Set if sqlnet.ora, tnsnames.ora, etc.
  are not in $ORACLE_HOME/network/admin
export NLS_LANG=AMERICAN;
export ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data
LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
export LD_LIBRARY_PATH
# Set shell search paths
export PATH=$PATH:$ORACLE_HOME/bin
```

8. Eseguire di nuovo il login come utente oracle per caricare le modifiche apportate alle variabili d'ambiente nell'ultimo passaggio:

```
exit
su - oracle
```

9. Collegare gcc alla versione 2.9.6

NOTA: se /usr/bin/gcc296 o /usr/bin/g++296 non esiste, significa che gcc o g++ non è stato installato. In questo caso, installare questi componenti quindi ritornare al passaggio corrente.

```
su - root
ln -s /usr/bin/gcc296 /usr/bin/gcc
ln -s /usr/bin/g++296 /usr/bin/g++
```

10. Uscire per tornare al prompt utente di Oracle.

```
exit
```

11. Eseguire la patch Oracle p3006854_9204_LINUX.zip per il sistema operativo Linux in cui è installato Oracle. È possibile ottenere la patch da Oracle.

```
su - root
unzip p3006854_9204_LINUX.zip
cd 3006854
sh rhel3_pre_install.sh
```

12. Uscire per tornare al prompt utente di Oracle.

```
exit
```

13. Per installare Oracle 9.2.0.4 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.
- Quando viene richiesto il nome del gruppo UNIX, immettere: dba
 - Quando viene richiesto di specificare il tipo di installazione, scegliere Personalizzata.

Selezionare i componenti seguenti per installarli:

- Oracle 9i 9.2.0.4.0
 - Enterprise Edition Options 9.2.0.1.0
 - Oracle Partitioning 9i 9.2.0.4.0
 - Oracle Net Services 9.2.0.1.0
 - Oracle Net Listener 9.2.0.4.0
 - Prodotti di Oracle Enterprise Manager 9.2.0.1.0 (Tutti)
 - Development kit di Oracle 9i 9.2.0.1.0 (Completo)
 - Oracle 9i per la documentazione UNIX 9.2.0.1.0
 - Oracle HTTP Server 9.2.0.1.0 (Completo)
 - iSQL*Plus 9.2.0.4.0 (Completo)
 - Interfacce di Oracle JDBC/OCI 9.2.0.1.0
15. Quando viene chiesto se si desidera creare il database, scegliere NO.
16. In alternativa, annullare tutti gli assistenti della configurazione avviati dal programma di installazione.
17. Modificare il file '/opt/oracle/network/admin/sqlnet.ora' (oppure crearlo se non esiste) in modo che contenga il testo seguente (rimuovere dal file tutte le informazioni esistenti senza commenti):

```
NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
```

18. Per applicare la patch Oracle 9.2.0.6 o 9.2.0.7 a Oracle Installer, dal disco 1 di distribuzione della patch Oracle 9.2.0.6 o 9.2.0.7, eseguire lo script:

NOTA: la patch Oracle 9.2.0.6 viene applicata solo dopo l'applicazione delle patch a Oracle Installer.

```
./runInstaller
```

19. 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 introduttiva, fare clic su *Avanti*.
 - Nella schermata Specify File Locations (Specifica ubicazione file), per Destination Name (Nome destinazione) scegliere "OUIHome" nell'elenco a discesa (o qualsiasi cosa si sia specificato come Destination Name (Nome destinazione) durante l'installazione di Oracle 9.2.0.4). Fare quindi clic su *Avanti*.
 - Nella schermata Select Product to Install (Seleziona prodotto da installare), scegliere "Oracle Universal Installer 10.1.0.3.0". Quindi fare clic su *Avanti*.
 - Nella schermata di riepilogo, esaminare il riepilogo dell'installazione e fare clic su *Install (Installa)*.
 - Nella schermata di completamento dell'installazione fare clic su *Exit (Esci)*.
20. Per applicare la patch Oracle 9.2.0.6 o 9.2.0.7 a Oracle, dal disco 1 di distribuzione della patch Oracle 9.2.0.6 o 9.2.0.7, eseguire lo script:

```
./runInstaller
```

21. 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 introduttiva, fare clic su *Avanti*.
 - Nella schermata Specify File Locations (Specifica ubicazione file), per Destination Name (Nome destinazione) scegliere "OUIHome" nell'elenco a discesa (o qualsiasi cosa si sia specificato come Destination Name (Nome destinazione) durante l'installazione di Oracle 9.2.0.4). Fare quindi clic su *Avanti*.
 - In base alla versione in uso, nella schermata Select Product to Install (Seleziona prodotto da installare) scegliere "Oracle 9iR2 Patchset 9.2.0.6.0". Quindi fare clic su *Avanti*.
 - Nella schermata di riepilogo, esaminare il riepilogo dell'installazione e fare clic su *Install (Installa)*.
 - Nella schermata di completamento dell'installazione fare clic su *Exit (Esci)*.

22. Scollegare gcc:

```
su - root  
rm /usr/bin/gcc  
rm /usr/bin/g++
```

23. Uscire per tornare al prompt utente di Oracle.

```
exit
```

Installazione di Sentinel 5 per Oracle in Linux

Sentinel 5 supporta due tipi di installazione. ovvero:

- Semplice – L'opzione di installazione integrata. Servizi Sentinel, i servizi di raccolta e le applicazioni con Oracle nello stesso computer. Questo tipo di installazione è eseguita solo a scopo dimostrativo.
- Personalizzata – Consente un'installazione completamente distribuita.

Installazione semplice in Linux

Con questa installazione vengono installati in un singolo computer i componenti più comuni (non sono inclusi Generatore servizi di raccolta o funzionalità di integrazione di terze parti). Questa operazione è eseguita principalmente a scopo dimostrativo. Non si tratta dell'installazione consigliata per l'uso in un ambiente di test o di produzione.

NOTA: con l'installazione Semplice non è supportata l'autenticazione con password di Gestione servizi di raccolta.

Come eseguire un'installazione semplice

1. Verificare di aver raccolto le informazioni, eseguito i task e soddisfatto i requisiti specificati nella sezione [Operazioni preliminari all'installazione di Sentinel 5 per Oracle](#) per i componenti da installare.
2. Verificare l'impostazione di [Linux Oracle](#).
3. Eseguire il login come utente radice.
4. Inserire e montare il CD di installazione di Sentinel.
5. Avviare il programma di installazione passando alla directory di installazione sul CD-ROM e digitare:

Per la modalità GUI:

```
./setup.sh
```

oppure

Per la modalità testuale ("headless"):

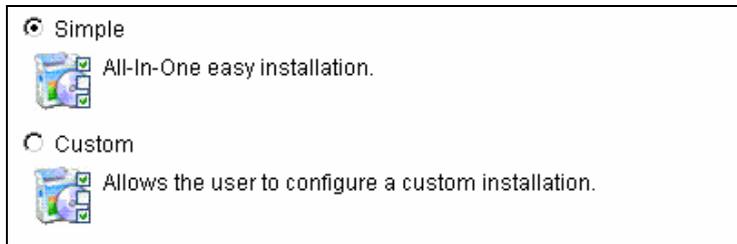
```
./setup.sh -console
```

6. Nel riquadro successivo, fare clic sulla freccia giù e selezionare una delle lingue seguenti.
 - English (Inglese)
 - French (Francese)
 - German (Tedesco)
 - Italiano
 - Portuguese (Portoghese)
 - Spanish (Spagnolo)
7. Seguire i prompt del programma di installazione.
8. Dopo aver letto la schermata introduttiva, fare clic su *Avanti*.
9. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
10. Accettare la directory di installazione di default o fare clic su *Sfoggia* per specificare il percorso di installazione. Fare clic su *Avanti*.

Fare clic su *Avanti* per installare "Sentinel 5" in questa cartella oppure fare clic su *Sfoggia* per installarlo in una cartella diversa.

Nome directory:

11. Selezionare *Semplice*. Fare clic su *Avanti*.



12. Immettere le informazioni di configurazione

- Numero di serie e codice licenza
- Server SMTP (nome DNS o indirizzo IP) – se si desidera avere la possibilità di inviare e-mail in Sentinel
- E-mail – Specificare un indirizzo e-mail valido al quale vengano inviate le e-mail di notifica di Advisor (ad esempio Sent_Server@myserver.com).
- Password di sistema globale – specificare una password e la password di conferma corrispondente. Questa diventerà la password per tutti gli utenti di default. Sono inclusi sia gli utenti esecadm del sistema operativo che gli utenti del database. Per l'elenco degli utenti del database di default creato durante l'installazione vedere [Database di Sentinel](#) nella sezione [Operazioni successive all'installazione di Sentinel 5 per Oracle](#).
- Directory dei dati – il percorso dei file di dati del database. Per modificare il percorso di default, fare clic sul pulsante ... e selezionare un'ubicazione. Quella di default è \$ESEC_HOME/data

NOTA: la directory dei dati deve essere accessibile in scrittura dall'utente Oracle. A questo scopo, eseguire i comandi seguente come utente radice:

```
chown -R oracle:dba <percorso_directory>
chmod -R 770 <percorso_directory>
```

presumendo che "oracle" sia il nome utente Oracle e "dba" il nome gruppo Oracle.

NOTA: se si sta installando Advisor, l'installazione Semplice consentirà di configurare Advisor per l'uso di Download Internet diretto con un intervallo di aggiornamento di 12 ore e tutte le notifiche via e-mail abilitate.

- Per installare Advisor, selezionare *Installa Advisor*. Specificare nome utente e password. Se non è possibile verificare nome utente o password, dopo aver fatto clic su *Avanti* verrà chiesto se si desidera continuare (non consigliabile). Se si sceglie di continuare, digitare di nuovo la password di Advisor nella finestra di conferma della password. In caso contrario correggere la password di Advisor.

Fare clic su *Avanti*.

Numero di serie: Codice di licenza:

Server SMTP: E-mail:

Password di sistema globale (utilizzata per tutti gli utenti Sentinel e per Gestione servizi di raccolta)

Password: Conferma password:

Directory dati:

Installa Advisor (è necessario specificare nome utente e password nei campi sotto...)

Nome utente: Password:

13. Immettere le informazioni di configurazione per il database:

- Nome database - Nome dell'istanza del database Oracle per creare e installare oggetti del database di Sentinel. Un database con questo nome non deve essere già esistente.
- File del driver JDBC Oracle. Percorso completo del file jar, in genere \$ORACLE_HOME/jdbc/lib/ojdbc14.jar (in questo campo non è possibile utilizzare variabili di ambiente).

Database Installation Configuration

Database Name:

Oracle JDBC Driver File:

14. Fare clic su OK sul nome utente Oracle di default.

Please enter the Oracle Username:

15. Leggere le informazioni presenti nella schermata visualizzata e al termine fare clic su *Avanti*. Una volta completata l'installazione, sarà necessario riavviare il sistema.

NOTA: se si desidera installare software di integrazione di terze parti (HP Service Desk o Remedy Integration), dopo aver riavviato il computer, eseguire di nuovo il programma di installazione e selezionare il software di integrazione di terze parti che si desidera installare. Per ulteriori informazioni, vedere la *Guida all'integrazione con soluzioni di terze parti*.

16. Il programma di installazione di Sentinel, per default, 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 per evitare che il database interrompa l'accettazione degli eventi.

Installazione personalizzata in Linux

Come eseguire una installazione personalizzata

1. Verificare di aver raccolto le informazioni, eseguito i task e soddisfatto i requisiti specificati nella sezione [Operazioni preliminari all'installazione di Sentinel 5 per Oracle](#) per i componenti da installare.
2. Verificare l'impostazione di [Linux Oracle](#).
3. Eseguire il login come utente radice.
4. Inserire e montare il CD di installazione di Sentinel.
5. Avviare il programma di installazione passando alla directory di installazione sul CD-ROM e digitare:

Per la modalità GUI:

```
./setup.sh
```

oppure

Per la modalità testuale ("headless"):

```
./setup.sh -console
```

6. Nel riquadro successivo, fare clic sulla freccia giù e selezionare una delle lingue seguenti.
 - English (Inglese)
 - French (Francese)
 - German (Tedesco)
 - Italiano
 - Portuguese (Portoghese)
 - Spanish (Spagnolo)
7. Dopo aver letto la schermata introduttiva, fare clic su *Avanti*.
8. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
9. Accettare la directory di installazione di default o fare clic su *Sfogli* per specificare il percorso di installazione. Fare clic su *Avanti*.

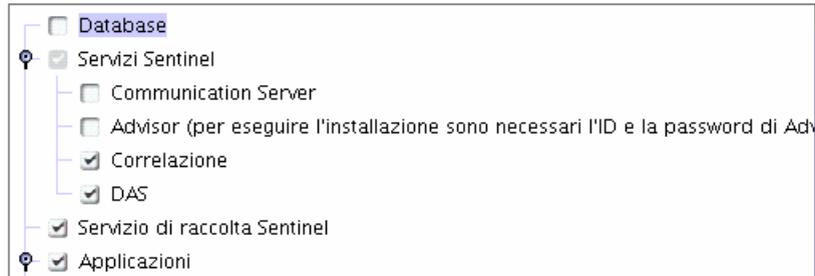
Fare clic su *Avanti* per installare "Sentinel 5" in questa cartella oppure fare clic su *Sfogli* per installarlo in una cartella diversa.

Nome directory:

10. Selezionare *Personalizzata* (default). Fare clic su *Avanti*.
11. Selezionare le funzioni da installare.

NOTA: per ulteriori informazioni su quali componenti è possibile installare e in quale posizione per configurazioni diverse, vedere il *capitolo 1, Requisiti di sistema*.

Selezionare le funzioni di "Sentinel 5" che si desidera installare:



Sono disponibili le opzioni seguenti:

- Database – Consente di installare il database di Sentinel
- Communication Server – Consente di installare il bus di messaggi (iSCALE)
- Advisor
- Motore di correlazione
- DAS
- Servizi di raccolta
- Sentinel Control Center
- Gestione dati Sentinel
- HP OpenView Service Desk**
- Remedy Integration**

NOTA: **per informazioni sull'installazione di HP OpenView Service Desk o Remedy Integration, vedere la *Guida all'integrazione con soluzioni di terze parti*.

NOTA: se nessuna delle funzioni secondarie dei "Servizi Sentinel" è selezionata, deselegionare anche la funzione "Servizi Sentinel". Verrà visualizzata in grigio con un segno di spunta bianco se è ancora selezionata ma tutte le relative funzioni secondarie sono state deselegionate.

NOTA: come parte dell'installazione del componente del database di Sentinel, il programma di installazione inserirà i file nella cartella \$ESEC_HOME/utilities/db.

12. Se si è scelto di installare DAS, verrà richiesto di specificare:
 - Numero di serie
 - Codice di licenza
13. Se si è scelto di installare componenti di integrazione di terze parti, verrà richiesto di specificare una password per sbloccare i componenti di terze parti selezionati. Per ulteriori informazioni, vedere la *Guida all'integrazione con soluzioni di terze parti*.
14. 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 sistema operativo – Il valore di default è esecadm
 - Home directory utente amministratore sistema operativo – Il valore di default è "/export/home" Se esecadm è il nome utente, la home directory dell'utente sarà /export/home/esecadm.

Username:

Location to create home directory:

NOTA: se viene creato un nuovo utente, sarà necessario impostare la relativa password in modo manuale, non nel programma di installazione. È consigliabile eseguire questa operazione direttamente eseguendo il login al sistema dopo l'installazione del prodotto.

per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, Sentinel richiede una password con le caratteristiche seguenti:

1. Scegliere password costituite da un minimo di 8 caratteri, di cui almeno uno MAIUSCOLO, uno minuscolo, uno speciale (!@#\$_) e uno numerico (0-9). Non utilizzare spazi.
2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.
3. La password non deve essere una parola "comune", ovvero una parola inclusa nel dizionario o di uso gergale.
4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione di password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.
5. È consigliabile scegliere una password facile da ricordare e allo stesso tempo complessa. Ad esempio, Mfhq5#ao (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#3a (Vivo a Napoli Da Quasi 3 anni).

-
15. Se si è scelto di installare Sentinel Control Center, verrà visualizzato un prompt di dimensioni heap JVM (Java Virtual Machine):
- Dimensioni heap JVM (MB) – Per default, è impostato sulla metà della memoria fisica rilevata nel computer, con un limite massimo di 1024 MB. Si tratterà delle dimensioni heap JVM massime utilizzate solo da Sentinel Control Center.

The installer has detected 2048 MB of physical memory. Please specify the desired JVM heap size for Sentinel Control Center. The legal range is 64-1024.

JVM Heap Size (MB)

16. Se si sceglie di installare il servizio di raccolta, sarà possibile decidere di proteggere o meno Generatore servizi di raccolta di Wizard con una password. Se si sceglie di proteggere Gestione servizi di raccolta di Wizard, verrà chiesto di creare un'apposita password.

NOTA: la protezione dei servizi di raccolta di Wizard con una password richiederà di specificare la password per il caricamento, lo scaricamento o il debug di raccolte in Gestione servizi di raccolta di Wizard. Questa password va aggiunta al nome utente e alla password di Sentinel necessari per eseguire il login a Generatore servizi di raccolta di Wizard.

NOTA: per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, Sentinel richiede una password con le caratteristiche seguenti:

1. Scegliere password costituite da un minimo di 8 caratteri, di cui almeno uno MAIUSCOLO, uno minuscolo, uno speciale (!@#\$\$%^&*()_+) e uno numerico (0-9).
 2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.
 3. La password non deve essere una parola "comune", ovvero una parola inclusa nel dizionario o di uso gergale.
 4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione di password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.
 5. È consigliabile scegliere una password facile da ricordare e allo stesso tempo complessa. Ad esempio, Mfhq5!ao (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#3a (Vivo a Napoli Da Quasi 3 anni).
-

Opzioni di protezione con password di Gestione servizi di raccolta:

- Non proteggere Gestione servizi di raccolta con password
- Proteggi Gestione servizi di raccolta tramite password

Password:

Conferma password:

17. Se si è scelto di installare DAS, selezionare la quantità di RAM del sistema che si desidera allocare per Data Access Service. Per gli ambienti distribuiti, è consigliabile selezionare la quantità massima di memoria (4 GB). Per gli ambienti indipendenti, è consigliabile selezionare metà della memoria RAM.

Selezionare la quantità di memoria (RAM) da allocare ai processi del server di accesso ai dati di Sentinel. Per ottenere prestazioni ottimali, allocare la massima quantità di memoria possibile.

18. Per l'installazione del database, saranno visualizzati i prompt seguenti
- a. Selezionare la piattaforma del server di database di destinazione come Oracle 9i e selezionare una delle opzioni seguenti:
 - Creare un nuovo database con oggetti di database – Consente di creare una nuova istanza di database Oracle e di inserire automaticamente nella nuova istanza gli oggetti di database.

- Nome database – Il nome dell'istanza di database vuoto Oracle esistente al quale si desidera aggiungere oggetti di database (il valore di default è ESEC). Questo nome di database deve essere visualizzato come nome di servizio nel file tnsnames.ora (nella directory \$ORACLE_HOME/network/admin/) del computer dal quale si sta eseguendo il programma di installazione.

NOTA: se il nome del database non è presente nel file tnsnames.ora, il programma di installazione non visualizzerà un errore a questo punto dell'installazione (poiché verifica la connessione utilizzando una connessione JDBC diretta), ma l'installazione del database non riuscirà quando il programma di installazione tenterà di connettersi al database via sqlplus. Se l'installazione del database si interrompe a questo punto, senza uscire dal programma di installazione modificare il Service Name (Nome servizio) per il database nel file tnsnames.ora presente nel computer, quindi tornare al programma di installazione e riprendere l'installazione. In questo modo verrà ritentata l'installazione del database con i nuovi valori presenti nel file tnsnames.ora.

- Porta di database (il valore di default è 1521)
- Per l'utente amministratore del database di Sentinel (DBA), specificare la password per l'utente "esecdba". Il campo nome utente in questo prompt non è modificabile.

Oracle Configuration

Select the Oracle JDBC driver (ojdbc14.jar):

/build/home/oracle/OraHome/jdbc/lib/ojdbc14.jar

Host name:

Database Name:

Port:

Login: Password:

- f. Se si è scelto di creare un nuovo database, verrà visualizzato il prompt seguente:
- Memoria Oracle (MB) – La quantità di RAM da allocare a questa istanza del database di Oracle.
 - Porta listener – La porta sulla quale creare un listener Oracle (il valore di default è 1521).
 - Password utente SYS e conferma password – SYS è un utente Oracle di default che verrà creato nella nuova istanza del database. La password utente verrà impostata sul valore specificato in questo campo.
 - Password utente SYSTEM e conferma password – SYSTEM è un utente Oracle di default che verrà creato nella nuova istanza del database. La password utente verrà impostata sul valore specificato in questo campo.

Oracle Configuration

Oracle Memory (MB):

ListenerPort:

SYS User Credentials SYSTEM User Credentials

Password: Password:

Confirm Password: Confirm Password:

- g. Se si è scelto di creare un nuovo database, verrà richiesto di specificare le dimensioni del database: Sono disponibili le opzioni seguenti:
- Standard (20 GB)
 - Grandi (400 GB)
 - Personalizzate (specificare le dimensioni manualmente). Se si seleziona questa opzione verrà richiesto di specificare:
 - dimensione iniziale di ogni file di database in MB (100 – 10.000)
 - dimensione massima di ogni file di database in MB (2.000 – 100.000)
 - dimensione di tutti i file di database in MB (7.000 – 2.000.000)
 - dimensione di ogni file di log in MB (100 – 100.000)

Please select Standard, Large, or Custom database size.

Standard (20,000MB, 30 day capacity @ 500,000 events per day)

Large (400,000MB, 30 day capacity @ 10,000,000 events per day)

Custom (specify database sizing manually)

- h. Se si è scelto di creare un nuovo database, verrà richiesto di specificare l'ubicazione di memorizzazione per i file di database seguenti.

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

Il programma di installazione non creerà tali directory, per cui è necessario crearle esternamente prima di continuare.

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>
```

presumendo che "oracle" sia il nome utente Oracle e "dba" il nome gruppo Oracle.

- Directory dati
- Directory indice
- Directory dati di riepilogo
- Directory indice di riepilogo
- Directory dei file temporanei e dello spazio delle tabelle di annullamento

- Directory log di ripetizione membro A
- Directory log di ripetizione membro B

Please enter the storage location for the following database files.

Data Directory:	<input type="text" value="/opt/oracle"/>	<input type="button" value="..."/>
Index Directory:	<input type="text" value="/opt/oracle"/>	<input type="button" value="..."/>
Summary Data Directory:	<input type="text" value="/opt/oracle"/>	<input type="button" value="..."/>
Summary Index Directory:	<input type="text" value="/opt/oracle"/>	<input type="button" value="..."/>
Temp and Undo Directory:	<input type="text" value="/opt/oracle"/>	<input type="button" value="..."/>
Redo Log Member A Directory:	<input type="text" value="/opt/oracle"/>	<input type="button" value="..."/>
Redo Log Member B Directory:	<input type="text" value="/opt/oracle"/>	<input type="button" value="..."/>

- i. Se si è scelto di creare un nuovo database, specificare le informazioni di autenticazione per l'amministratore del database di Sentinel (DBA). Corrisponde a esecdba, il proprietario degli oggetti di database.
 - j. Specificare le informazioni di autenticazione per l'utente del database dell'applicazione Sentinel. Corrisponde a esecapp, il nome utente dell'applicazione Sentinel utilizzato dai processi Sentinel per la connessione al database.
 - k. Specificare le informazioni di autenticazione per l'utente del database amministratore di Sentinel. Corrisponde a esecadm, l'utente amministratore di Sentinel.
 - l. Fare clic su *Avanti* nella finestra di riepilogo dell'installazione del database.
19. Se si è scelto di installare DAS ma di non installare il database di Sentinel, verrà richiesto di specificare le informazioni del database di Sentinel di Oracle seguenti. Queste informazioni saranno utilizzate per configurare DAS perché faccia riferimento al database di Sentinel.
- Nome host del database o indirizzo IP – Il nome o l'indirizzo IP del database di Sentinel di Oracle esistente per il quale si desidera configurare la connessione da parte del componente DAS.
 - Nome database – Il nome o dell'istanza di database vuoto Oracle esistente per il quale si desidera configurare la connessione da parte del componente DAS (il valore di default è ESEC).
 - Porta di database (il valore di default è 1521)
 - Per l'utente del database dell'applicazione Sentinel, specificare il login "esecapp" e immettere la password impostata per questo utente durante l'installazione del database di Sentinel.

Oracle Configuration

Select the Oracle JDBC driver (ojdbc14.jar):

Hostnam e:

Database Nam e:

Port:

Login: Password:

20. Se si è scelto di installare DAS, configurare il supporto e-mail di Sentinel. Specificare il server SMTP e l'indirizzo e-mail del mittente che dovrà essere utilizzato dal servizio di esecuzione per l'invio di messaggi (facoltativo – è possibile modificarlo manualmente dopo l'installazione [`$(ESEC_HOME)\sentinel\config\execution.properties`]):

SMTP Server:

From "EmailAddress":

21. Se si è scelto di installare Advisor, selezionare il tipo di installazione di Advisor (se l'opzione di Advisor prevedeva la scelta di un nome utente e una password)
- Download Internet diretto – Il computer che esegue Advisor è connesso direttamente a Internet. In questa configurazione, gli aggiornamenti vengono scaricati da Sentinel automaticamente e a scadenze regolari mediante Sentinel.
 - Autonomo - Advisor è configurato come sistema isolato che necessita di interventi manuali per ricevere aggiornamenti da Sentinel.
22. Se si è scelto di installare Advisor e si è selezionato di utilizzare l'opzione Download Internet diretto, specificare nome utente e password Advisor e la frequenza di aggiornamento dei dati di Advisor. Se non è possibile verificare nome utente o password, dopo aver fatto clic su *Avanti* verrà chiesto se si desidera continuare (non consigliabile). Se si sceglie di continuare, digitare di nuovo la password di Advisor nella finestra di conferma della password. In caso contrario correggere la password di Advisor.

Please enter the username and password to access the Advisor server and feed data:

Username:

Password:

Please select how often Advisor data needs to be updated:

6 Hours 12 Hours

23. Se si è scelto di installare Advisor, specificare:

- L'indirizzo del mittente, visualizzato nelle notifiche di e-mail.
- L'indirizzo del destinatario, per l'invio delle notifiche di e-mail.

NOTA: dopo l'installazione è possibile cambiare gli indirizzi e-mail di Advisor modificando i file `attackcontainer.xml` e `alertcontainer.xml` nella directory `$ESEC_HOME/sentinel/config`. Per ulteriori informazioni, vedere il *capitolo 7 – Scheda Advisor della Guida dell'utente di Sentinel*.

- Selezionare *Sì* o *No* a seconda che si desideri ricevere e-mail relative alla riuscita degli aggiornamenti di Advisor. Le notifiche di errori saranno inviate sempre.

Advisor Configuration

Enter the from address for sending the email notifications:

Enter the addresses to which email notifications should be sent (comma separated):

Do you want email notifications for successful Advisor updates (error notifications will always be sent)?

Yes No

24. Se si è scelto di installare HP Service Desk o Remedy Integration, verrà richiesto di specificare altre informazioni. Per ulteriori informazioni, vedere la *Guida all'integrazione con soluzioni di terze parti di Sentinel*.
25. Leggere le informazioni presenti nella schermata visualizzata e al termine fare clic su *Avanti*. Una volta completata l'installazione, verrà chiesto di riavviare il sistema. Fare clic su *Fine* per riavviare il sistema.
26. Il programma di installazione di Sentinel, per default, 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 per evitare che il database interrompa l'accettazione degli eventi.
27. Se si prevede un'elevata frequenza di eventi (superiore ai 500 eventi al secondo), sarà necessario seguire le istruzioni aggiuntive per la configurazione riportate nella sezione [Impostazione della strategia di inserimento di eventi OCI \(Oracle Call Interface\)](#).

Installazione di Sentinel Control Center e Generatore servizi di raccolta in Windows

Installazione di Sentinel Control Center e Generatore servizi di raccolta in Windows

1. Inserire il CD di installazione di Sentinel nell'unità CD-ROM.
2. Passare al CD e fare doppio clic su *setup.bat*.

NOTA: l'installazione in modalità console non è supportata in Windows.

3. Dopo aver letto la schermata introduttiva, fare clic su *Avanti*.
4. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
5. Accettare la directory di installazione di default o fare clic su *Sfogli* per specificare il percorso di installazione. Fare clic su *Avanti*.

Fare clic su *Avanti* per installare "Sentinel 5" in questa cartella oppure fare clic su *Sfogli* per installarlo in una cartella diversa.

Nome directory:

6. Selezionare le funzioni da installare.
7. Specificare l'indirizzo e la porta dell'host in cui è installato Communication Server.

Host (hostname or IP address):

Port (default = 10012):

8. Se si è scelto di installare Sentinel Control Center, verrà visualizzato un prompt JVM (Java Virtual Machine):
 - Dimensioni heap JVM (MB) – Per default, è impostato sulla metà della memoria fisica rilevata nel computer, con un limite massimo di 1024 MB. Si tratterà delle dimensioni heap JVM massime utilizzate solo da Sentinel Control Center.

JVM Heap Size (MB)

Fare clic su *Avanti*.

9. Fare clic su *Installa*
10. Leggere le informazioni presenti nella schermata visualizzata e al termine fare clic su *Avanti*. Fare clic su *Fine*.

Operazioni successive all'installazione di Sentinel 5 per Oracle

Aggiornamento di e-mail Sentinel per l'autenticazione SMTP

Se nel sistema è necessaria l'autenticazione SMTP, sarà necessario aggiornare il file `execution.properties`. Il file si trova nel computer in cui è installato DAS. Nella directory `$ESEC_HOME/sentinel/config`. Per configurare questo file, eseguire `mailconfig.sh` per modificare il file e `mailconfigtest.sh` per eseguire il test delle modifiche.

Per configurare il file `execution.properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
$ESEC_HOME/sentinel/config
```

2. Eseguire il comando `mailconfig` come indicato di seguito:

```
./mailconfig.sh -host <server SMTP> -from <indirizzo e-mail di origine> -user <utente autenticazione posta> -password
```

Esempio:

```
./mailconfig.sh -host 10.0.1.14 -from my_name@domain.com -user my_user_name -password
```

Dopo aver immesso questo comando verrà richiesto di specificare una nuova password.

```
Immettere la password:*****
```

```
Confermare la password:*****
```

NOTA: quando si utilizza l'opzione relativa alla password, deve trattarsi dell'ultimo argomento.

Per eseguire il test della configurazione del file `execution properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
$ESEC_HOME/sentinel/config
```

2. Eseguire il comando `mailconfigtest` come indicato di seguito:

```
./mailconfigtest.sh -to <indirizzo e-mail di destinazione>
```

Se l'invio del messaggio e-mail è riuscito correttamente, il messaggio sarà ricevuto all'indirizzo di destinazione e verrà visualizzato il messaggio seguente sullo schermo dell'utente.

```
Messaggio e-mail inviato.
```

Controllare la casella postale e-mail per confermare la ricezione del messaggio. La riga dell'oggetto e il contenuto dovrebbero essere:

```
Oggetto: Testing Sentinel mail property
```

This is a test for Sentinel mail property set up. If you see this message, your Sentinel mail property has been configured correctly to send emails

Database di Sentinel

Dopo aver installato il database di Sentinel, il database conterrà gli utenti di default seguenti:

- `esecdba` – Proprietario schema database. I privilegi DBA non sono concessi all'utente `esecdba` per motivi di sicurezza. Per utilizzare Enterprise Manager, 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 `esecadm` del sistema operativo.
- `esecrpt` – Utente rapporti database
- `SYS` – Utente database SYS
- `SYSTEM` – Utente database SYSTEM

Servizio di raccolta

Durante l'installazione del servizio di raccolta, saranno installati i servizi di raccolta seguenti per l'esecuzione di ognuno dei quali sarà impostata una porta del servizio di raccolta.

Prodotto	Nome servizio di raccolta
Servizi di raccolta dimostrativi	
Test per il caricamento di risorse, funziona con servizio di raccolta DemoEvents	DemoAssetUpload
Test degli eventi demo, funziona con servizi di raccolta DemoAssetUpload e DemoVulnerabilityUpload	DemoEvents
Test per il caricamento di vulnerabilità, funziona con servizio di raccolta DemoEvents	DemoVulnerabilityUpload
Test per l'invio di un evento	SendOneEvent
Test per l'invio di più eventi	SendMultipleEvents

NOTA: per ulteriori informazioni relative alla configurazione dei servizi di raccolta dimostrativi, vedere il *capitolo 12, Test dell'installazione*.

NOTA: per aggiungere ulteriori Servizi di raccolta, andare al portale per i clienti di Sentinel e scaricare il Service Pack più recente per la versione installata. Il Service Pack più recente per la versione in uso contiene il gruppo completo degli ultimi Servizi di raccolta disponibili per la versione di Sentinel in uso.

Per ulteriori informazioni (anche sulla configurazione) utilizzare la documentazione fornita per ogni servizio di raccolta in:

`$WORKBENCH_HOME/Elements/<nome servizio di raccolta>/Docs/`

Per installare altri servizi di raccolta, eseguire lo script del Service Pack sul CD del Service Pack. Lo script installerà i servizi di raccolta in locale.

In Windows:

```
.\service_pack.bat
```

In UNIX:

```
./service_pack.sh
```

Per istruzioni sull'installazione del Service Pack e l'elenco dei servizi di raccolta, vedere *le Note di rilascio del Service Pack*.

Aggiornamento del codice di licenza

Come aggiornare il codice di licenza (Linux)

1. Eseguire il login come utente esecadm.
2. Inserire e montare il CD di installazione di Sentinel.
3. Passare alla directory disk1/utilities/linux.
4. Immettere il comando seguente:

```
./softwarekey
```
5. Immettere il numero 1 per specificare la chiave primaria. Premere Invio.

Creazione di un'istanza Oracle per il database di Sentinel

NOTA: questa procedura viene riportata come esempio della creazione di spazi delle tabelle personali anziché utilizzare la funzione di creazione di spazi delle tabelle fornita nel CD di installazione. I valori relativi alle dimensioni possono essere diversi a seconda della configurazione e dei requisiti del sistema. Gli spazi delle tabelle devono essere denominati esattamente come segue.

Nell'istanza Oracle sarà necessario configurare:

- parametri
- spazi delle tabelle

Creazione di 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.

Parametri consigliati per la configurazione minima di Linux	
Parametri	Dimensioni (byte o specificato diversamente)
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608

Parametri consigliati per la configurazione minima di Linux	
Parametri	Dimensioni (byte o specificato diversamente)
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
optimizer_index_caching	50
optimizer_index_cost_adj	55

Dimensioni minime spazi delle tabelle di Linux		
Spazio delle tabelle	Dimensioni esempio	Note
REDO	3 x 100 M	Corrisponde al valore minimo. Nel caso di EPS elevato creare log di ripetizione di dimensioni maggiori.
SYSTEM	500 M	Valore minimo
TEMP	1 G	Valore minimo
UNDO	1 G	Valore minimo
ESENTD	5 G	Valore minimo Per i dati evento
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 evento
ESENTX2	500 M	Valore minimo Indice per configurazione, risorse, vulnerabilità e associazioni (estensione automatica abilitata)
SENT_ADVISORD	200 M	Valore minimo Per dati di Advisor (estensione automatica abilitata)
SENT_ADVISORX	100 M	Valore minimo Per indice di Advisor (estensione automatica abilitata)
SENT_LOBS	100 M	Valore minimo Per oggetti di database di grandi dimensioni (estensione automatica abilitata)
SENT_SMRYD	3 G	Valore minimo Per aggregazione, dati di riepilogo
SENT_SMRYX	2 G	Valore minimo Per aggregazione, indice di riepilogo

3. Eseguire lo script createEsecdba.sh presente 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.

Impostazione della strategia di inserimento eventi OCI (Oracle Call Interface)

Sentinel 5.1 fornisce un framework per l'utilizzo di strategie diverse per inserire eventi nel database. Sentinel 5.1 fornisce due strategie per inserire eventi nel database Oracle.

- JDBCLoadStrategy
- OCILoadStrategy

La strategia da utilizzare per l'inserimento di eventi è regolata dalla proprietà insert strategy del componente EventStoreService in das_binary.xml.

La strategia JDBC è la strategia di default configurata pronta per l'utilizzo.

La strategia OCI è una strategia di inserimento nativa per l'inserimento di eventi più rapido. Per questa strategia è necessario che le librerie OCI Oracle siano installate nel computer che esegue il componente DAS. La strategia OCI deve essere utilizzata in configurazioni in cui si prevede un'elevata frequenza di eventi.

Il numero di eventi da raggruppare per l'inserimento nel database è regolato dalla proprietà insert.batchsize. La proprietà insert.batchsize è utilizzata da tutte le strategie di inserimento di eventi.

Per cambiare la strategia di inserimento eventi di Sentinel da quella di default JDBC alla strategia OCI, è necessario eseguire alcune operazioni.

Modifica della strategia di inserimento di eventi da JDBC a OCI

1. Verificare che le librerie OCI Oracle siano installate nel computer che esegue il componente DAS di Sentinel. Sarà necessario conoscere il percorso di ORACLE_HOME nei passaggi seguenti.
2. Eseguire il login al computer come utente esecadm dal passaggio 1.
3. Creare un file “.bash_profile” nella home directory dell'utente esecadm. Inserirvi il testo seguente (modificare il percorso di ORACLE_HOME in modo che sia conforme all'installazione in uso):

```
ORACLE_HOME=/build/home/oracle/OraHome
export ORACLE_HOME
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

4. Aprire il file \$ESEC_HOME/sentinel/config/das_binary.xml per la modifica in qualsiasi editor di testo.
5. Eseguire una ricerca del testo seguente:

```
JDBCLoadStrategy
```

6. Modificare il testo in:

```
OCILoadStrategy
```

7. Salvare la modifica nel file `das_binary.xml`.
8. Riavviare l'applicazione DAS Binary. Il riavvio di DAS Binary può essere eseguito più facilmente eseguendo il comando `"ps -ef | grep DAS_Binary"` per ottenere l'ID del processo, interrompendo il processo e consentendo alla sorveglianza di Sentinel di riavviare automaticamente il processo.

Una volta riavviato DAS Binary, verrà caricata la libreria `$ESEC_HOME/sentinel/lib/libocievent.so` che sarà utilizzata per eseguire l'inserimento di eventi nel database tramite OCI.

Altre opzioni per l'inserimento di eventi OCI

Oltre a specificare `"OCILoadStrategy"` nel file `das_binary.xml`, è possibile configurare diverse altre opzioni relative a OCI.

- `insert.batchsize` – Questa impostazione consente di configurare il numero massimo di eventi da inserire nel database contemporaneamente.
- `insert.oci.workerCount` – Questa impostazione consente di configurare il numero di thread da utilizzare per inserire dati di eventi nel database.
- `insert.oci.queueWaitTime` – Questa impostazione consente di specificare il tempo massimo di attesa in secondi per l'inserimento dei dati dalla coda in entrata nel database. Quando si riceve un `"batchsize"` di eventi completo, viene inserito l'intero batch. Ma se il flusso di eventi in entrata è lento, il tempo di attesa della coda viene utilizzato per determinare quando eseguire l'inserimento nel database (anche se non è stato ancora ricevuto un batch completo di eventi).
- `insert.oci.highWatermark` – Il limite massimo della coda di eventi.
- `insert.oci.lowWatermark` – Il limite minimo della coda di eventi.
- `insert.oci.optimizationFlag` – Flag di ottimizzazione. "Attivo" o "Disattivo".

Suggerimenti per il debug di OCI

L'interfaccia OCI registra i messaggi nel file `$ESEC_HOME/sentinel/log/ocievent.log`. I messaggi iniziali scritti nel file di log devono includere messaggi relativi a corretta o non riuscita connessione al database... Si tratta di una buona occasione per verificare che la libreria OCI sia stata caricata e configurata correttamente.

L'interfaccia OCI registra anche gli errori nel file di log `das_binary` memorizzato nella directory `$ESEC_HOME/sentinel/log`. Gli errori registrati nel file di log `das_binary` comprendono errori di individuazione/caricamento della libreria `libocievent.so`, errori di connessione al database ed errori di inserimento eventi/ associazioni di eventi.

Se i messaggi di errore indicano che il file `"libocievent.so"` non è stato individuato o caricato, sarà necessario controllare tre cose:

1. Verificare che le librerie OCI Oracle siano installate.
2. Verificare che il file `"libocievent.so"` sia memorizzato nella directory `$ESEC_HOME/sentinel/lib`.
3. Verificare che la directory `$ESEC_HOME/sentinel/lib` sia in `"LD_LIBRARY_PATH"` dell'utente `"esecadm"`. In caso contrario sarà possibile aggiornare `LD_LIBRARY_PATH` nel profilo dell'utente `"esecadm"`.
4. Verificare che le variabili di ambiente `ORACLE_HOME` e `LD_LIBRARY_PATH` siano aggiornate correttamente nelle variabili di ambiente dell'utente `esecadm` come descritto nella sezione `"Modifica della strategia di inserimento di eventi da JDBC a OCI"`.

5

Installazione di Sentinel 5 per MS SQL

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo viene descritto come installare Sentinel Enterprise Security Management Sentinel 5 per MS SQL.

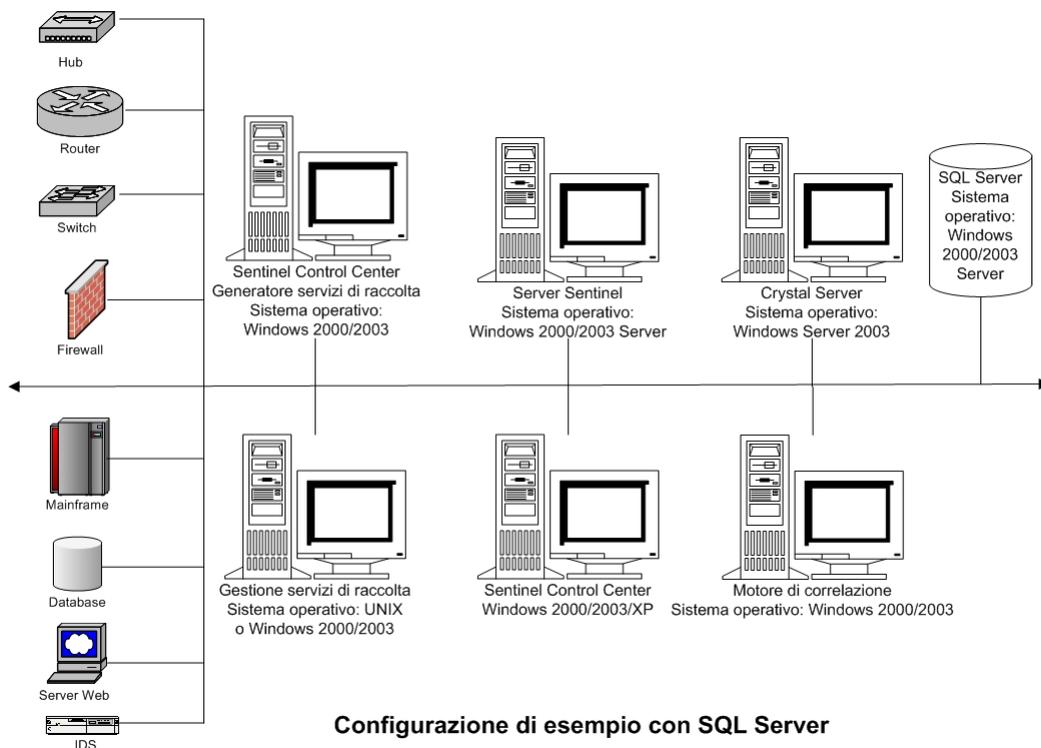
Operazioni preliminari all'installazione di Sentinel 5 MSSQL

NOTA: prima dell'installazione, verificare che il computer in uso soddisfi i requisiti minimi di sistema e che il sistema operativo sia stato ottimizzato utilizzando le procedure consigliate correnti per la sicurezza.

NOTA: Sentinel non supporta i cluster MS né la disponibilità elevata per Windows.

NOTA: quando si esegue un'installazione completa di Sentinel dopo averne rimosso una precedente, è necessario rimuovere alcuni file e impostazioni del sistema derivanti dall'installazione precedente. Se non si rimuovono tali file o impostazioni la nuova installazione completa potrebbe non riuscire. Questa operazione deve essere eseguita su ogni computer sul quale si sta eseguendo una nuova installazione. Per ulteriori informazioni, vedere *l'appendice E*.

Di seguito è illustrata una configurazione tipica di Sentinel. La configurazione dell'utente potrebbe essere diversa, a seconda dell'ambiente in uso. Indipendentemente dalla configurazione selezionata, è necessario installare prima il database.



NOTA: per ulteriori informazioni sui sistemi operativi supportati, vedere *la sezione sulle piattaforme supportate per il server Sentinel su Windows nel capitolo 1 "Introduzione"*.

Per ottenere un codice di licenza

Per l'installazione e l'esecuzione del servizio DAS (Database Access Service) del server Sentinel è necessario disporre di un codice di licenza valido. Tale codice di licenza è bloccato per il computer nel quale si sta installando DAS. Il codice di licenza emesso per un computer non funzionerà su un computer diverso.

Per ottenere il codice di licenza, è necessario determinare l'ID host e fornire tali informazioni a Novell che provvederà all'assegnazione di un codice di licenza.

Per determinare l'ID dell'host

1. Inserire il CD di installazione di Sentinel nell'unità CD-ROM.
2. Passare alla directory delle utility sul CD.
3. Eseguire il file:

```
hostid.exe
```

4. Inviare l'ID host al Supporto tecnico Novell. Il Supporto clienti fornirà il codice di licenza richiesto.

Database di Sentinel

Prima di installare il server Sentinel, sarà necessario accertarsi di disporre di quanto segue:

- Per i requisiti hardware, vedere il *capitolo 1 e 2*
- Windows 2000 Server con Service Pack 4 o Windows Server 2003 con Service Pack 1

- SQL Server 2000 Enterprise Edition Service Pack 3a o SQL Server 2005 Enterprise Addition (Sentinel v5.1.1 SP1 e versioni successive) installato e in esecuzione.

NOTA: per motivi connessi alle prestazioni, a seconda che si stia eseguendo l'installazione in RAID e che l'ambiente RAID lo consenta, il log delle transazioni dovrebbe fare riferimento al disco con scrittura più veloce disponibile.

NOTA: se si è installato SQL Server con modalità di autenticazione mista, è possibile accedere con l'account di Windows o mediante l'autenticazione di SQL Server. Per la modalità non mista, è necessario utilizzare l'autenticazione di Windows.

Per modificare le impostazioni della modalità di autenticazione, in SQL Enterprise Manager, fare clic con il pulsante destro del mouse sul server di cui si desidera modificare le impostazioni (per default: (locale) (Windows NT)), scegliere *Proprietà*, fare clic sulla scheda *Protezione* e selezionare *SQL Server e Windows* oppure *Solo Windows* per Autenticazione. L'account del servizio di avvio deve essere impostato su *System*.

- Nome dell'istanza di SQL Server di destinazione (default consigliata).

NOTA: se l'istanza è stata denominata durante l'installazione di SQL Server, utilizzare tale nome quando richiesto durante l'installazione del database e/o dei componenti DAS. Se non si conosce il nome dell'istanza, lasciarlo vuoto durante l'installazione, ovvero non aggiungere \

- Numero di porta dell'istanza di SQL Server di destinazione (default: 1433).
- Se si prevede di utilizzare l'autenticazione di Windows per uno o più utenti di Sentinel, è necessario creare l'utente di dominio di Windows corrispondente prima di installare il database di Sentinel. È possibile designare come utenti di dominio di Windows gli utenti Sentinel seguenti:
 - Amministratore del database di Sentinel - Proprietario dello schema del database (ad esempio esecdba)
 - Utente dell'applicazione Sentinel – Utilizzato dalle applicazioni Sentinel per connettersi al database (ad esempio esecapp)
 - Amministratore di Sentinel – Amministratore per il login a Sentinel Control Center (ad esempio esecadm)
 - Utente dei rapporti di Sentinel – Utilizzato per la creazione di rapporti (ad esempio esecrpt)

Server Sentinel

NOTA: se non si intende installare il database di Sentinel contemporaneamente al server Sentinel, è necessario installare prima il database di Sentinel.

Prima di installare il server Sentinel, sarà necessario accertarsi di disporre di quanto segue:

- Per i requisiti hardware, vedere il *capitolo 1 e 2*
- Windows 2000 Server con Service Pack 4 o Windows Server 2003 con Service Pack 1
- Numero di serie e codice licenza per Novell Sentinel 5 (per DAS). Per ulteriori informazioni, vedere [Per ottenere un codice di licenza](#).
- Se si installa DAS e si utilizza un account utente di dominio di Windows per l'utente dell'applicazione Sentinel, è necessario assegnare a tale utente il privilegio di accesso come servizio. A tale scopo, aprire Criteri di protezione locali nel Pannello di controllo del computer in cui si installerà DAS (*Start > Impostazioni > Pannello di controllo > Strumenti di amministrazione > Criteri di protezione locali*). Nella finestra di Criteri di

protezione locali, passare a *Criteri locali > Assegnazione diritti utente*. Aprire il criterio *Accesso come servizio* e aggiungere l'utente.



- Server SMTP – Necessario per l'invio di e-mail da Sentinel.

Sentinel Control Center e Wizard

Prima di installare il server Sentinel, sarà necessario accertarsi di disporre di quanto segue:

- Per i requisiti hardware, vedere i *capitoli 1 e 2*
- Windows 2000 Server con Service Pack 4 o Windows Server 2003 con Service Pack 1

Advisor

Per installare Advisor, sarà necessario ottenere un ID Advisor e una password da Novell. Download Internet diretto utilizza la porta 443.

NOTA: se si intende utilizzare Advisor solo per il rilevamento dell'utilizzo, non sarà necessario installare il software Crystal Enterprise. È infatti necessario solo se si intende eseguire Crystal Reports per Sentinel. Per ulteriori informazioni, vedere il *capitolo 10, Configurazione di Advisor*.

Installazione di Sentinel 5 per MS SQL

Sentinel 5 supporta due tipi di installazione, ovvero:

- Semplice – L'opzione di installazione integrata. Servizi Sentinel, Servizio di raccolta e applicazioni con MS SQL nello stesso computer. Supporta solo l'autenticazione di SQL Server. Questo tipo di installazione è eseguita solo a scopo dimostrativo.
- Personalizzata – Consente un'installazione completamente distribuita.

NOTA: per default, il programma di installazione imposta i filegroup seguenti perché le dimensioni NON aumentino automaticamente: ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX. Tutti gli altri filegroup sono impostati per l'aumento automatico delle dimensioni. Il motivo per il quale non viene consentito l'aumento automatico di ESENTD, ESENTX, SENT_SMRYD e SENT_SMRYX è che contengono dati di eventi e dati di eventi di riepilogo. L'utilizzo dello spazio per gli eventi e i riepiloghi può essere notevolmente dinamico. È necessario monitorare ed estendere questi filegroup degli eventi in maniera controllata, in base alla configurazione del file system e tenendo in considerazione il bilanciamento IO e le attività di backup e recupero del database.

La gestione della partizione SDM (archiviazione, eliminazione e aggiunta di partizioni) dovrebbe essere pianificata per mantenere dimensioni controllate per gli eventi.

Installazione semplice

Questa installazione installa tutti i componenti (incluso il database) in un'unica piattaforma e supporta esclusivamente l'autenticazione di SQL Server. Questa operazione è eseguita principalmente a scopo dimostrativo. Non è consigliabile eseguirla per ambienti di test e produzione.

NOTA: con l'installazione semplice non è supportata l'autenticazione con password di Gestione servizi di raccolta.

Installazione semplice di Sentinel

1. Verificare di aver raccolto le informazioni, eseguito i task e soddisfatto i requisiti specificati nella sezione [Operazioni preliminari all'installazione di Sentinel 5 per MSSQL](#) per i componenti da installare.
2. Inserire il CD di installazione di Sentinel nell'unità CD-ROM.
3. Passare al CD e fare doppio clic su *setup.bat*.

NOTA: l'installazione in modalità console non è supportata in Windows.

4. Nel riquadro successivo, fare clic sulla freccia giù e selezionare una delle lingue seguenti.
 - English (Inglese)
 - French (Francese)
 - German (Tedesco)
 - Italiano
 - Portuguese (Portoghese)
 - Spanish (Spagnolo)
5. Dopo aver letto la schermata introduttiva, fare clic su *Avanti*.
6. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
7. Accettare la directory di installazione di default o fare clic su *Sfoggia* per specificare il percorso di installazione. Fare clic su *Avanti*.

Fare clic su *Avanti* per installare "Sentinel 5" in questa cartella oppure fare clic su *Sfoggia* per installarlo in una cartella diversa.

Nome directory:

8. Selezionare Semplice. Fare clic su *Avanti*.

Simple
 All-In-One easy installation.

Custom
 Allows the user to configure a custom installation.

9. Immettere le informazioni di configurazione

- Numero di serie e codice licenza
- Server SMTP (nome DNS o indirizzo IP) – se si desidera avere la possibilità di inviare e-mail in Sentinel
- E-mail – Specificare un indirizzo di e-mail valido al quale vengano inviate le e-mail di notifica di Advisor (ad esempio Sent_Server@myserver.com).
- Password di sistema globale – specificare una password e la password di conferma corrispondente. Questa diventerà la password per tutti gli utenti di default. Sono inclusi sia gli utenti esecadm del sistema operativo che gli utenti del database. Per l'elenco degli utenti del database di default creato durante l'installazione vedere [Database di Sentinel](#) nella sezione [Operazioni successive all'installazione di Sentinel 5 per MSSQL](#).
- Directory dati - l'ubicazione di tutti i file di dati per il database e Advisor. Per modificare il percorso di default, fare clic sul pulsante ... e selezionare un'ubicazione. L'ubicazione di default è %ESEC_HOME%\data.

NOTA: se si sta installando Advisor, l'installazione Semplice consentirà di configurare Advisor per l'uso di Download Internet diretto con un intervallo di aggiornamento di 12 ore e tutte le notifiche via e-mail abilitate.

- Per installare Advisor, selezionare *Installa Advisor*. Specificare nome utente e password. Se non è possibile verificare nome utente o password, dopo aver fatto clic su *Avanti* verrà chiesto se si desidera continuare (non consigliabile). Se si sceglie di continuare, digitare di nuovo la password di Advisor nella finestra di conferma della password. In caso contrario correggere la password di Advisor.

Fare clic su *Avanti*.

Numero di serie: Codice di licenza:

Server SMTP: E-mail:

Password di sistema globale (utilizzata per tutti gli utenti Sentinel e per Gestione servizi di raccolta)

Password: Conferma password:

Directory dati:

Installa Advisor (è necessario specificare nome utente e password nei campi sotto...)

Nome utente: Password:

10. Per la configurazione dell'installazione del database, immettere:

- nome utente e password sa
- Se l'istanza di SQL Server è denominata, immetterne il nome

Database Installation Configuration

Database Name: SQL Server Instance:

Login:

Password:

11. Leggere le informazioni presenti nella schermata visualizzata e al termine fare clic su *Avanti*. Una volta completata l'installazione, sarà necessario riavviare il sistema.

NOTA: se si desidera installare software di integrazione di terze parti (HP Service Desk o Remedy Integration), dopo aver riavviato il computer, eseguire di nuovo il programma di installazione e selezionare il software di integrazione di terze parti che si desidera installare. Per ulteriori informazioni, vedere la *Guida all'integrazione con soluzioni di terze parti*.

Installazione personalizzata

Installazione personalizzata di Sentinel

1. Verificare di aver raccolto le informazioni, eseguito i task e soddisfatto i requisiti specificati nella sezione [Operazioni preliminari all'installazione di Sentinel 5 per MSSQL](#) per i componenti da installare.
2. Inserire il CD di installazione di Sentinel nell'unità CD-ROM.
3. Passare al CD e fare doppio clic su *setup.bat*.

NOTA: l'installazione in modalità console non è supportata in Windows.

4. Nel riquadro successivo, fare clic sulla freccia giù e selezionare una delle lingue seguenti.
 - English (Inglese)
 - French (Francese)
 - German (Tedesco)
 - Italiano
 - Portuguese (Portoghese)
 - Spanish (Spagnolo)
5. Dopo aver letto la schermata introduttiva, fare clic su *Avanti*.
6. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
7. Accettare la directory di installazione di default o fare clic su *Sfoggia* per specificare il percorso di installazione. Fare clic su *Avanti*.

Fare clic su *Avanti* per installare "Sentinel 5" in questa cartella oppure fare clic su *Sfoggia* per installarlo in una cartella diversa.

Nome directory:

C:\Programmi\sentinel5.1.3.0

Sfoggia

8. Selezionare *Personalizzata* (default). Fare clic su *Avanti*.
9. Selezionare le funzioni da installare.

NOTA: per ulteriori informazioni su quali componenti è possibile installare e in quale posizione per configurazioni diverse, vedere il *capitolo 1, Requisiti di sistema*.

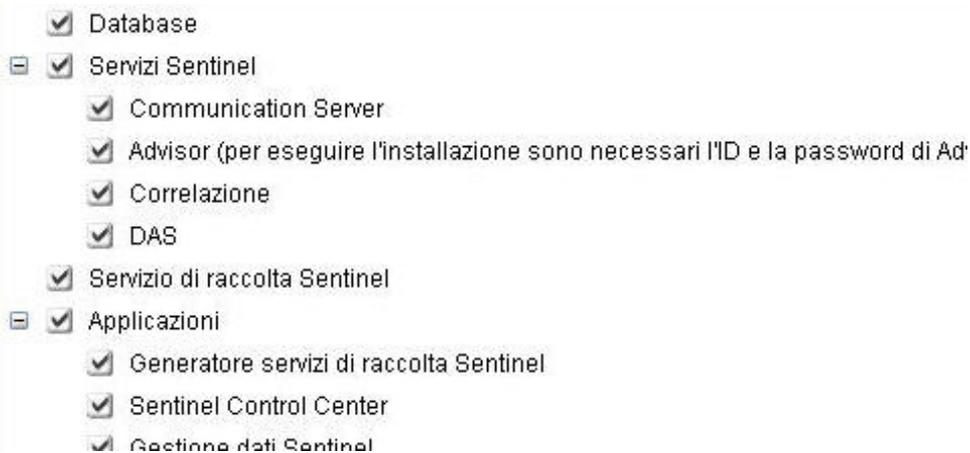
È possibile installare i componenti seguenti:

- Database – Consente di installare il database di Sentinel
- Communication Server – Consente di installare il bus di messaggi (iSCALE)
- Advisor
- Motore di correlazione
- DAS
- Servizio di raccolta
- Generatore servizi di raccolta
- Sentinel Control Center
- Gestione dati Sentinel
- HP OpenView Service Desk
- Remedy Integration

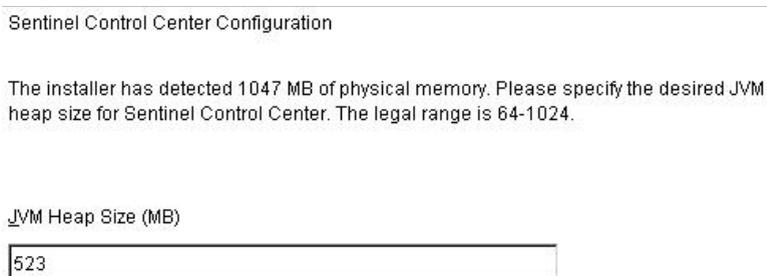
NOTA: per informazioni sull'installazione di HP OpenView Service Desk o Remedy Integration, vedere la *Guida all'integrazione con soluzioni di terze parti*.

NOTA: se nessuna delle funzioni secondarie dei "Servizi Sentinel" è selezionata, deselegionare anche la funzione "Servizi Sentinel". Verrà visualizzata in grigio con un segno di spunta bianco se è ancora selezionata ma tutte le relative funzioni secondarie sono state deselegionate.

NOTA: come parte dell'installazione del componente del database di Sentinel, il programma di installazione inserirà i file nella cartella %ESEC_HOME%\utilities\cartella db.



- Se si è scelto di installare DAS, verrà richiesto di specificare:
 - Numero di serie
 - Codice di licenza
- Se si è scelto di installare componenti di integrazione di terze parti, verrà richiesto di specificare una password per sbloccare i componenti di terze parti selezionati. Per ulteriori informazioni, vedere la *Guida all'integrazione con soluzioni di terze parti*.
- Se si è scelto di installare Sentinel Control Center, verrà visualizzato un prompt JVM (Java Virtual Machine):
 - Dimensioni heap JVM (MB) – Per default, è impostato sulla metà della memoria fisica rilevata nel computer, con un limite massimo di 1024 MB. Si tratterà delle dimensioni heap JVM massime utilizzate solo da Sentinel Control Center.



- Se si sceglie di installare il servizio di raccolta, sarà possibile decidere di proteggere o meno Gestione servizi di raccolta di Wizard con una password. Se si sceglie di proteggere Gestione servizi di raccolta di Wizard, verrà chiesto di creare un'apposita password.

NOTA: la protezione del servizio di raccolta di Wizard con una password richiederà di specificare la password per il caricamento, lo scaricamento o il debug di raccolte in Gestione servizi di raccolta di Wizard. Questa password va aggiunta al nome utente e alla password di Sentinel necessari per eseguire il login a Gestione servizi di raccolta di Wizard.

NOTA: per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, Sentinel richiede una password con le caratteristiche seguenti:

1. Scegliere password composte da non meno di 8 caratteri, di cui almeno un carattere MAIUSCOLO, un carattere minuscolo, un carattere speciale (!@#\$%^&*()_+) e un carattere numerico (0-9).
 2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.
 3. La password non deve essere una parola "comune", ovvero una parola inclusa nel dizionario o di uso gergale.
 4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione delle password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.
 5. Scegliere una password memorizzabile seppure complessa. Ad esempio, Mfhq5!ao (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#3a (Vivo a Napoli Da Quasi 3 anni).
-

Opzioni di protezione con password di Gestione servizi di raccolta:

- Non proteggere Gestione servizi di raccolta con password
- Proteggi Gestione servizi di raccolta tramite password**

Password:

Conferma password:

14. Se si è scelto di installare DAS, selezionare la quantità di RAM del sistema che si desidera allocare per Data Access Service. Per gli ambienti distribuiti, è consigliabile selezionare la quantità massima di memoria (4 GB). Per gli ambienti indipendenti, è consigliabile selezionare metà della memoria RAM.

Selezionare la quantità di memoria (RAM) da allocare ai processi del server di accesso ai dati di Sentinel. Per ottenere prestazioni ottimali, allocare la massima quantità di memoria possibile.

15. Per l'installazione del database, saranno visualizzati i prompt seguenti

- a. Selezionare la piattaforma del server di database di destinazione, ovvero Microsoft SQL Server 2000 o 2005 e selezionare una delle opzioni seguenti:
 - Creare un nuovo database con oggetti di database – Consente di creare una nuova istanza di database MS SQL e di inserire automaticamente nel nuovo database i relativi oggetti.
 - Aggiungi oggetti di database a un database vuoto esistente - Consente solo di aggiungere il database a un'istanza di database MS SQL esistente. Il database esistente deve essere vuoto.
- b. Specificare la directory dei log di installazione del database (default: %ESEC_HOME%\logs\db). Accettare la directory dei log di installazione del database di default o fare clic su *Sfoggia* per specificare un'ubicazione diversa.

Selezionare la piattaforma server del database di destinazione:

- Creare un nuovo database con oggetti di database.
- Aggiungi oggetti di database a un database vuoto esistente.

Directory log di installazione database:

- c. Immettere le informazioni di configurazione per SQL Server:
 - (1) Nome host del database o indirizzo IP – Per default, sarà visualizzato il computer host locale, se SQL Server è installato in locale. Se la versione di SQL Server che si desidera installare non è visualizzata nell'elenco a discesa, selezionare *'Altro'* nell'elenco. Verrà visualizzata una casella di testo nella quale sarà possibile digitare il nome host. Il nome host specificato deve essere completo (ovvero 'sqlserver.sentinel.net' anziché solo 'sqlserver'). Se si è specificato il nome di un'istanza durante l'installazione di SQL Server, sarà necessario aggiungere '\<nome_istanza>' alla fine del nome host, dove <nome_istanza> è il nome assegnato all'istanza durante l'installazione di SQL Server.
 - (2) Nome database (nuovo database) - Il nome da assegnare al nuovo database SQL Server. Oltre al database di cui si specifica il nome verrà creato un altro database con il nome <nome_db>_WF per l'utilizzo con iTRAC.
 - (2) Nome database (database esistente) – Il nome del database di SQL Server esistente al quale si desidera aggiungere gli oggetti. Utilizzare il nome del database che non contiene il suffisso "_WF".
 - (3) Porta di database (il valore di default è 1433)
 - Per l'amministratore del database di sistema, selezionare:

- (4) Autenticazione di Windows (viene utilizzato il nome utente con cui viene eseguito il programma di installazione)
- (5) Autenticazione di SQL Server (è necessario immettere la password dell'utente sa)

Microsoft SQL Server Configuration

Hostname[<InstanceName>]: (1) <Hostname>[<InstanceName>] (3) Port: 1433

Database: ESEC (2)

Please enter the authentication information for the database System Administrator user or choose "Windows Authentication" to use current user.

Windows Authentication (4)

SQL Server Authentication

Autenticazione di Windows

Microsoft SQL Server Configuration

Hostname[<InstanceName>]: (1) <Hostname>[<InstanceName>] (3) Port: 1433

Database: ESEC (2)

Please enter the authentication information for the database System Administrator user or choose "Windows Authentication" to use current user.

Windows Authentication

SQL Server Authentication (5)

Login: sa

Password:

Autenticazione di SQL Server

- d. Se si è scelto di creare un nuovo database, specificare l'ubicazione per i file seguenti:

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

- File di dati
- File di indice
- File di dati di riepilogo
- File di indice di riepilogo
- File di log

Specificare l'ubicazione di memorizzazione dei file di database seguenti:

Directory dati:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>
Directory indice:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>
Directory dati di riepilogo:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>
Directory indice di riepilogo:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>
Directory di log:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>

- e. Se si è scelto di installare un nuovo database, specificarne le dimensioni:
- Standard (20.000 MB, capacità 30 giorni per 500.000 eventi al giorno)
 - Grandi (400.000 MB, capacità 30 giorni a 10.000.000 di eventi al giorno)
 - Personalizzate (specificare le dimensioni manualmente). Se si seleziona questa opzione verrà richiesto di specificare:
 - (1) dimensione del database in MB (10.000 – 2.000.000)
 - (2) dimensione di ogni file di log in MB (100 – 100.000)
 - (3) dimensione massima di ogni file di database in MB (2.000 – 100.000)

Please select Standard, Large, or Custom database size.

Standard (20,000MB, 30 day capacity @ 500,000 events per day)

Large (400,000MB, 30 day capacity @ 10,000,000 events per day)

Custom (specify database sizing manually)

- f. Per l'amministratore del database di Sentinel (DBA), selezionare:
- Autenticazione di Windows, immettere <nome dominio>\<nome utente>
 - Autenticazione di SQL Server (esecdba), password e conferma password

NOTA: se si seleziona "Autenticazione di SQL Server", non sarà possibile modificare il nome di login di default.

Specificare le informazioni di autenticazione per l'utente (DBA) amministratore del database di Sentinel.

- Autenticazione di Windows
- Autenticazione di SQL Server

Login:

Autenticazione di Windows

Specificare le informazioni di autenticazione per l'utente (DBA) amministratore del database di Sentinel.

Autenticazione di Windows

Autenticazione di SQL Server

Login:

Password:

Conferma password:

Autenticazione di SQL Server

g. Per l'amministratore del database dell'applicazione Sentinel, selezionare:

NOTA: se si utilizza un login di dominio Windows per l'utente di database dell'applicazione Sentinel, sarà necessario concedere all'utente il privilegio "Accesso come servizio" nel computer come specificato nella sezione [Server Sentinel](#), all'interno della sezione [Operazioni preliminari all'installazione di Sentinel 5 per MSSQL](#).

- Autenticazione di Windows, specificare <nome dominio>\<nome utente>, password e conferma password
- Autenticazione di SQL Server (esecapp), immettere password e conferma password

NOTA: se si seleziona "Autenticazione di SQL Server", non sarà possibile modificare il nome di login di default.

Specificare le informazioni di autenticazione per l'utente di database dell'applicazione Sentinel.

Autenticazione di Windows

Autenticazione di SQL Server

Login:

Password:

Conferma password:

Autenticazione di Windows

Specificare le informazioni di autenticazione per l'utente di database dell'applicazione Sentinel.

Autenticazione di Windows

Autenticazione di SQL Server

Login:

Password:

Conferma password:

Autenticazione di SQL Server

- h. Per l'utente amministratore di Sentinel, selezionare:
- Autenticazione di Windows, immettere <nome dominio>\<nome utente>
 - Autenticazione di SQL, immettere il nome utente per l'amministratore Sentinel (valore di default: esecadm), password e conferma password

NOTA: se si seleziona "Autenticazione di SQL Server", non sarà possibile modificare il nome di login di default.

Specificare le informazioni di autenticazione per l'utente amministratore di Sentinel.

- Autenticazione di Windows
 Autenticazione di SQL Server

Login:

Autenticazione di Windows

Specificare le informazioni di autenticazione per l'utente amministratore di Sentinel.

- Autenticazione di Windows
 Autenticazione di SQL Server

Login:

Password:

Conferma password:

Autenticazione di SQL Server

- i. Per l'utente dei rapporti di Sentinel, selezionare:
- Autenticazione di Windows, immettere <nome dominio>\<nome utente>
 - Autenticazione di SQL Server (esecrpt), immettere password e conferma password

NOTA: se si seleziona "Autenticazione di SQL Server", non sarà possibile modificare il nome di login di default.

Specificare le informazioni di autenticazione per l'utente amministratore di Sentinel.

- Autenticazione di Windows
 Autenticazione di SQL Server

Login:

Autenticazione di Windows

Specificare le informazioni di autenticazione per l'utente dei rapporti di Sentinel.

Autenticazione di Windows

Autenticazione di SQL Server

Login:

Password:

Conferma password:

Autenticazione di SQL Server

- j. Fare clic su *Avanti* nella finestra di riepilogo dell'installazione del database.
16. Se si è scelto di installare DAS ma di non installare il database di Sentinel, verrà richiesto di specificare le informazioni del database di Sentinel di SQL Server seguenti. Queste informazioni saranno utilizzate per configurare DAS perché faccia riferimento al database di Sentinel.
- Nome host del database o indirizzo IP – Per default, sarà visualizzato il computer host locale, se il database di Sentinel per SQL Server è installato in locale. Se la versione del database di Sentinel per SQL Server che si desidera configurare per la connessione con DAS non è visualizzata nell'elenco a discesa, selezionare *Altro* nell'elenco. Verrà visualizzata una casella di testo nella quale sarà possibile digitare il nome host. Il nome host specificato deve essere completo (ovvero 'sqlserver.sentinel.net' anziché solo 'sqlserver'). Se si è specificato il nome di un'istanza durante l'installazione di SQL Server, sarà necessario aggiungere '\<nome_istanza>' alla fine del nome host, dove <nome_istanza> è il nome assegnato all'istanza durante l'installazione di SQL Server.
 - Nome database – Il nome del database di Sentinel per SQL Server che si desidera configurare per la connessione tramite DAS. Utilizzare il nome del database che non contiene il suffisso "_WF".
 - Porta di database (il valore di default è 1433)
 - Per l'utente del database dell'applicazione di Sentinel, selezionare:

NOTA: se si utilizza un login di dominio Windows per l'utente di database dell'applicazione Sentinel, sarà necessario concedere all'utente il privilegio "Accesso come servizio" nel computer come specificato nella sezione [Server Sentinel](#), all'interno della sezione [Operazioni preliminari all'installazione di Sentinel 5 per MSSQL](#).

- Autenticazione di Windows – Specificare l'account di accesso al dominio di Windows per tale utente durante l'installazione del database di Sentinel e specificarne la password. La password è necessaria per configurare il servizio Sentinel per Windows su "Accesso come servizio" come account di accesso al dominio di Windows.
- Autenticazione di SQL Server – Specificare l'account di accesso "esecpp" e immettere la password per tale utente durante l'installazione del database di Sentinel.

Microsoft SQL Server Configuration

Hostname[<InstanceName>]:
 <Hostname>[<InstanceName>] Port: 1433
 Database: ESEC

Please enter the authentication information for the e-Security Application Database User.

Windows Authentication
 SQL Server Authentication

Login:
 Password:

Autenticazione di Windows

Microsoft SQL Server Configuration

Hostname[<InstanceName>]:
 <Hostname>[<InstanceName>] Port: 1433
 Database: ESEC

Please enter the authentication information for the e-Security Application Database User.

Windows Authentication
 SQL Server Authentication

Login: esecapp
 Password:

Autenticazione di SQL Server

17. Se si è scelto di installare DAS, configurare il supporto e-mail di Sentinel. Specificare il server SMTP e l'indirizzo e-mail del mittente che dovrà essere utilizzato dal servizio di esecuzione per l'invio di messaggi (facoltativo – è possibile modificarlo manualmente dopo l'installazione [[%ESEC_HOME%\sentinel\config\execution.properties]):

The Execution Service (a component of DAS) will perform actions triggered by the Correlation Engine and Sentinel Console. One action it can perform is sending email. Please specify the SMTP server and the "From" email address Execution Service should use for all email it sends.

SMTP Server:
 localhost

"From" Email Address:
 email@VING

18. Se si sceglie di installare Advisor, verrà visualizzata la richiesta seguente relativa al tipo di installazione:
- Download Internet diretto – Il computer che esegue Advisor è connesso direttamente a Internet. In questa configurazione, gli aggiornamenti vengono scaricati da Novell automaticamente e a scadenze regolari mediante Internet.

- Autonomo - Advisor è configurato come sistema isolato che necessita di interventi manuali per ricevere aggiornamenti da Sentinel.

Please select the type of Advisor Installation

Direct Internet Download

StandAlone

19. Se si è scelto di installare Advisor e si è selezionato di utilizzare l'opzione Download Internet diretto, specificare nome utente e password Advisor e la frequenza di aggiornamento dei dati di Advisor. Se non è possibile verificare nome utente o password, dopo aver fatto clic su *Avanti* verrà chiesto se si desidera continuare (non consigliabile). Se si sceglie di continuare, digitare di nuovo la password di Advisor nella finestra di conferma della password. In caso contrario correggere la password di Advisor.

Please enter the username and password to access the Advisor server and feed data:

Username:

Password:

Please select how often Advisor data needs to be updated:

6 Hours 12 Hours

20. Se si è scelto di installare Advisor, specificare:

- La directory in cui saranno memorizzati i file di feed di dati di Advisor. Si tratta dell'ubicazione in cui vengono salvati i file di attacchi e di feed scaricati.
- L'indirizzo del destinatario, per l'invio delle notifiche di e-mail.
- Selezionare Sì o No a seconda che si desideri ricevere e-mail relative alla riuscita degli aggiornamenti di Advisor. Le notifiche di errori saranno inviate sempre.

Please enter the directory where Advisor data feed files are to be stored:

Enter the from address for sending the email notifications:

Enter the addresses to which email notifications should be sent (comma separated):

Do you want email notifications for successful Advisor updates (error notifications will always be sent)?

Yes No

NOTA: dopo l'installazione è possibile cambiare gli indirizzi e-mail di Advisor modificando i file `attackcontainer.xml` e `alertcontainer.xml` nella directory `$ESEC_HOME/sentinel/config`. Per ulteriori informazioni vedere il *capitolo 9 "Scheda Advisor" della Guida dell'utente di Sentinel*.

21. Se si è scelto di installare HP Service Desk o Remedy Integration, verrà richiesto di specificare altre informazioni. Per ulteriori informazioni, vedere la *Guida all'integrazione con soluzioni di terze parti di Sentinel*.

22. Leggere le informazioni presenti nella schermata visualizzata e al termine fare clic su *Avanti*. Una volta completata l'installazione, verrà chiesto di riavviare il sistema.
23. Fare clic su *Fine* per riavviare il sistema.
24. Se si prevede un'elevata frequenza di eventi (superiore ai 800 eventi al secondo), sarà necessario seguire le istruzioni aggiuntive per la configurazione riportate nella sezione [Impostazione della strategia di inserimento di eventi ADO \(Active Data Objects\)](#).

Operazioni successive all'installazione di Sentinel 5 per MS SQL

Aggiornamento di e-mail Sentinel per l'autenticazione SMTP

Se nel sistema è necessaria l'autenticazione SMTP, sarà necessario aggiornare il file `execution.properties`. Il file si trova nel computer in cui è installato DAS. Nella directory `%ESEC_HOME%\sentinel\config`. Per configurare questo file, eseguire `mailconfig.bat` per modificare il file e `mailconfigtest.bat` per eseguire il test delle modifiche.

Per configurare il file `execution.properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
%ESEC_HOME%\sentinel\config
```

2. Eseguire il comando `mailconfig` come nell'esempio seguente:

```
./mailconfig.sh -host <Server SMTP> -from <indirizzo e-mail di origine> -user <utente autenticazione posta> -password
```

Esempio:

```
./mailconfig.sh -host 10.0.1.14 -from my_name@domain.com -user my_user_name -password
```

Dopo aver immesso questo comando verrà richiesto di specificare una nuova password.

```
Immettere la password:*****
```

```
Confermare la password:*****
```

NOTA: quando si utilizza l'opzione relativa alla password, deve trattarsi dell'ultimo argomento.

Per eseguire il test della configurazione del file `execution.properties`

1. Nel computer in cui è installato DAS, passare alla directory seguente:

```
%ESEC_HOME%\sentinel\config
```

2. Eseguire il comando `mailconfigtest` come indicato di seguito:

```
mailconfigtest.bat -to <indirizzo e-mail di destinazione>
```

Se l'invio della e-mail è riuscito correttamente, l'e-mail sarà ricevuta all'indirizzo di destinazione e verrà visualizzato il messaggio seguente sullo schermo dell'utente.

```
Email has been sent successfully!
```

Controllare la casella postale e-mail per confermare la ricezione del messaggio. La riga dell'oggetto e il contenuto dovrebbero essere:

Subject: Testing Sentinel mail property

This is a test for Sentinel mail property set up. If you see this message, your Sentinel mail property has been configured correctly to send emails

Database di Sentinel

Dopo aver installato il database di Sentinel, il database conterrà gli utenti di default seguenti:

- esecdba – proprietario dello schema (se si utilizza l'utente di dominio di Windows, configurabile in fase di installazione)
- esecapp – nome utente utilizzato dalle applicazioni di Sentinel per connettersi al database (se si utilizza l'utente di dominio di Windows, configurabile in fase di installazione)
- esecadm – amministratore di Sentinel (se si utilizza l'utente di dominio di Windows, configurabile in fase di installazione)
- esecrpt – utente dei rapporti (se si utilizza l'utente di dominio di Windows, configurabile in fase di installazione)

Servizio di raccolta

Durante l'installazione del servizio di raccolta, saranno installati i servizi di raccolta seguenti per l'esecuzione di ognuno dei quali sarà impostata una porta del servizio di raccolta.

Prodotto	Nome servizio di raccolta
Servizi di raccolta dimostrativi	
Test per il caricamento di risorse, funziona con il servizio di raccolta DemoEvents	DemoAssetUpload
Test degli eventi demo, funziona con i servizi di raccolta DemoAssetUpload e DemoVulnerabilityUpload	DemoEvents
Test per il caricamento di vulnerabilità, funziona con il servizio di raccolta DemoEvents	DemoVulnerabilityUpload
Test per l'invio di un evento	SendOneEvent
Test per l'invio di più eventi	SendMultipleEvents

NOTA: per ulteriori informazioni relative alla configurazione del servizio di raccolta dimostrativi, vedere il *capitolo 12, Test dell'installazione*.

NOTA: per servizi di raccolta aggiuntivi, visitare il portale del servizio clienti Sentinel. Per ulteriori informazioni (anche sulla configurazione) utilizzare la documentazione fornita per ogni servizio di raccolta in:

`%WORKBENCH_HOME%\Elements\`

Per installare altri servizi di raccolta, eseguire lo script del Service Pack sul CD del Service Pack. Lo script installerà i servizi di raccolta in locale.

In Windows:

```
.\service_pack.bat
```

In UNIX:

```
./service_pack.sh
```

Per istruzioni sull'installazione del Service Pack e per un elenco dei servizi di raccolta, vedere le *Note di rilascio del Service Pack*.

Aggiornamento del codice di licenza

Se il codice di licenza di Sentinel è scaduto e Novell ne ha fornito uno nuovo, eseguire il programma dei codici software per aggiornare la licenza.

Aggiornamento del codice di licenza

1. Eseguire l'accesso come utente con diritti di amministrazione.
2. Aprire %ESEC_HOME%\utilities.
3. Immettere il comando seguente:

```
softwarekey.exe
```

4. Immettere il numero 1 per specificare la chiave primaria. Premere Invio.

Istruzioni di configurazione per l'utilizzo dell'autenticazione di Windows di SQL Server con il driver JDBC DataDirect

NOTA: le informazioni seguenti sono tratte dalla Guida all'installazione di DataDirect Connect[®] per JDBC[®]. È consigliabile che le operazioni illustrate di seguito vengano effettuate dall'amministratore di sistema.

Dopo l'installazione di Connect per JDBC, è necessario eseguire alcune operazioni di configurazione sui componenti seguenti allo scopo di utilizzare l'autenticazione di Windows su SQL Server:

- Server di database SQL Server
- Controller di dominio
- Workstation client

Per ulteriori informazioni sull'autenticazione di Windows e il driver SQL Server Connect per JDBC, fare riferimento alle *guide dell'utente e di riferimento del driver DataDirect Connect per JDBC*.

Server di database SQL Server

In questa sezione viene descritta la configurazione necessaria per il server di database SQL Server ai fini dell'utilizzo dell'autenticazione di Windows con il driver SQL Server Connect per JDBC.

Nome entità servizio

Per utilizzare il protocollo di autenticazione Kerberos, è necessario registrare un nome di entità servizio per ogni istanza di SQL Server. Si tratta di un nome univoco che mappa il server SQL Server di un determinato computer e la relativa porta a un nome di conto utilizzato per avviare il servizio stesso (conto di avvio del servizio). Il nome di entità servizio è costituito dagli elementi seguenti:

- Il nome di classe del servizio per SQL Server è sempre MSSQLSvc
- Il nome host corrisponde al nome DNS completo del computer che esegue SQL Server
- Il numero di porta corrisponde a quello su cui l'istanza di SQL Server è in ascolto

Ad esempio: MSSQLSvc/DBServer.test:1433 è un nome di entità servizio per un'istanza di SQL Server in esecuzione su un computer denominato DBServer nel dominio test e in ascolto sulla porta 1433.

Elenco di nomi di entità servizio

Rivolgersi all'amministratore di dominio o del database per accertarsi di utilizzare i nomi di entità servizio appropriati registrati per ogni istanza di SQL Server. L'amministratore di dominio o database può utilizzare il comando `ldifde` di Windows per elencare i nomi registrati.

Registrazione di nomi di entità servizio

Se necessario, l'amministratore di dominio o database può registrare nomi di entità servizio mediante lo strumento `Setspn` disponibile in Windows Resource Kit. Ad esempio:

```
setspn -A MSSQLSvc/DBServer.test:1433 sqlsvc
```

consente di registrare un nome di entità servizio che mappa il conto di avvio del servizio denominato `sqlsvc` a un'istanza di SQL Server in esecuzione su un computer denominato `DBServer` nel dominio `test` e in ascolto sulla porta 1433.

Lo strumento `Setspn` è disponibile nel sito Web seguente:

<http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/setspn-o.asp>.

Fare riferimento alla documentazione Microsoft fornita con lo strumento `Setspn` per istruzioni sul suo utilizzo.

NOTA: se il conto di avvio per SQL Server viene modificato, i nomi di entità servizio per SQL Server devono essere eliminati e registrati nuovamente.

Modalità di autenticazione

Per utilizzare l'autenticazione di Windows, la modalità di autenticazione di SQL Server deve essere imposta su una delle opzioni seguenti:

- Solo Windows
- Mista

Se oltre all'autenticazione di Windows verrà utilizzata l'autenticazione di SQL Server, la modalità da utilizzare è Mista.

Controller di dominio

Il driver di SQL Server supporta l'autenticazione di Windows quando il centro distribuzione chiavi di Kerberos è in esecuzione su un controller di dominio di Windows 2000. Durante la comunicazione con il centro distribuzione chiavi, i messaggi passati tra quest'ultimo e SQL Server vengono cifrati.

Poiché SQL Server è solo in grado di utilizzare l'algoritmo di cifratura DES-CBC-MD5, il conto di avvio del servizio SQL Server nel controller di dominio deve contenere la proprietà di Active Directory "Utilizza crittografia DES per questo account". Rivolgersi all'amministratore del dominio per verificare che la proprietà sia imposta per il conto di avvio del servizio SQL Server. Tale conto non può essere utilizzato per l'accesso client.

Computer client

In questa sezione viene descritta la configurazione necessaria per il computer client ai fini dell'utilizzo dell'autenticazione di Windows con il driver SQL Server Connect per JDBC.

File di configurazione di Kerberos

Il modulo di login di Kerberos richiede il nome dell'area di autenticazione Kerberos (il nome del dominio di Windows) e il nome del relativo centro distribuzione chiavi (nome del controller di dominio di Windows). Quando si installa Connect per JDBC, viene installato un file di configurazione che specifica un'area di autenticazione Kerberos e un nome del centro distribuzione chiavi generici. Il file è denominato `krb5.conf` e viene installato nella directory `/lib` della directory di installazione di Connect per JDBC.

È necessario modificare tale file per specificare il nome dell'area di autenticazione e quello del centro distribuzione chiavi per l'ambiente in uso. Se il file non viene modificato in modo da includere tali dati, verrà generato l'errore seguente:

```
Message:[DataDirect][SQLServer JDBC Driver]Could not
    establish a connection using integrated security:
    No valid credentials provided
```

Il driver SQL Server Connect per JDBC configura automaticamente il modulo di login di Kerberos in modo da caricare il file di configurazione `krb5.conf` a meno che la proprietà di sistema `java.security.krb5.conf` non sia già impostata in modo da fare riferimento a un altro file di configurazione. Non è possibile ignorare il nome dell'area di autenticazione di Kerberos e del centro distribuzione chiavi specificati nel file `krb5.conf` mediante le proprietà di sistema seguenti: `java.security.krb5.realm` e `java.security.krb5.kdc`.

Impostazione della strategia di inserimento eventi ADO (Active Data Objects)

Sentinel 5.1 fornisce un framework per l'utilizzo di strategie diverse per inserire eventi nel database. Sentinel 5.1 fornisce due strategie per inserire eventi nel database di MS SQL:

- `JDBCLoadStrategy`
- `ADOLoadStrategy`

La strategia da utilizzare per l'inserimento di eventi è regolata dalla proprietà `insert.strategy` del componente `EventStoreService` in `das_binary.xml`.

La strategia JDBC è la strategia di default configurata pronta per l'utilizzo.

La strategia ADO è una strategia nativa per l'inserimento di eventi più rapido. Per questa strategia è necessario che i pacchetti aggiuntivi di Windows siano installati nel computer che esegue il componente DAS. Vedere la sezione seguente per informazioni sui pacchetti che è necessario installare. La strategia ADO deve essere utilizzata in configurazioni in cui si prevede un'elevata frequenza di eventi.

Il numero di eventi da raggruppare per l'inserimento nel database è regolato dalla proprietà `insert.batchsize`. La proprietà `insert.batchsize` è utilizzata da tutte le strategie di inserimento di eventi.

Le sezioni seguenti descrivono come passare alle strategie di caricamento ADO.

Prerequisiti per la strategia di caricamento ADO

Il connettore nativo ADO richiede l'installazione di .NET Framework e del pacchetto ridistribuibile J# sul computer che esegue `DAS_Binary`.

NOTA: sarà necessario disinstallare eventuali versioni precedenti di .NET Framework e del pacchetto ridistribuibile J# per poter installare le versioni elencate nell'ordine seguente.

- .NET Framework 2.0 Beta 2 disponibile all'indirizzo <http://www.microsoft.com/downloads/details.aspx?FamilyID=7ABD8C8F-287E-4C7E-9A4A-A4ECFF40FC8E&displaylang=en>
- visual J# versione 2.0 Beta 2 disponibile all'indirizzo <http://www.microsoft.com/downloads/details.aspx?FamilyId=A2788A92-76AB-4BF4-893A-FA9FD5031F14&displaylang=en>

Impostazione della strategia di inserimento degli eventi di caricamento ADO

Per cambiare la strategia di inserimento eventi di Sentinel da quella di default JDBC alla strategia ADO, è necessario eseguire alcune operazioni.

Passaggio dalla strategia di inserimento JDB alla strategia di inserimento ADO

1. In un editor di testo, aprire `%ESEC_HOME%\sentinel\config\das_binary.xml`.
2. Eseguire una ricerca del testo seguente:

```
JDBCLoadStrategy
```

3. Modificare il testo in:

```
ADOLoadStrategy
```

4. Salvare la modifica nel file `das_binary.xml`.
5. Riavviare l'applicazione `DAS_Binary`.

Una volta riavviato `DAS Binary`, verranno caricate le librerie `%ESEC_HOME%\Sun-1.4.2\bin\EventInsert.dll` e `EventJNICLIBridge.dll` che saranno utilizzate per eseguire l'inserimento di eventi nel database tramite ADO.

Suggerimenti per il debug di ADO

L'interfaccia di ADO registrerà i messaggi di errore nel file `the %ESEC_HOME%\sentinel\log\ADOEventStoreError.log`. I messaggi di errore iniziali scritti nel file di log possono includere errori di connessione al database. In questo file verranno inoltre registrate le eccezioni verificatesi durante l'inserimento di eventi nel database. Si noti che: in questo file vengono registrati solo gli errori.

Per verificare che ADO sia connesso e caricato in modo corretto, controllare il file di log `das_binary` che si trova in `%ESEC_HOME%\sentinel\directory` di log.

L'interfaccia ADO registra inoltre gli errori nel file di log `das_binary` memorizzato nella directory `%ESEC_HOME%\sentinel\` directory di log. Gli errori registrati nel file di log `das_binary` comprendono errori di individuazione/caricamento della libreria `EventJNICLIBridge.dll`, errori di connessione al database ed errori di inserimento eventi/ associazioni di eventi.

Se i messaggi di errore indicano che i connettori nativi non sono stati caricati correttamente, verificare quanto segue:

- Accertarsi che nel computer siano installate le versioni corrette di .NET Framework e del pacchetto ridistribuibile J#.
- Accertarsi che i file “`EventJNICLIBridge.dll`” e “`EventInsert.dll`” si trovino nella directory `%ESEC_HOME%\Sun-1.4.2\bin\` directory.

6

Migrazione di dati e patch per Oracle in Solaris

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo vengono trattati gli argomenti seguenti:

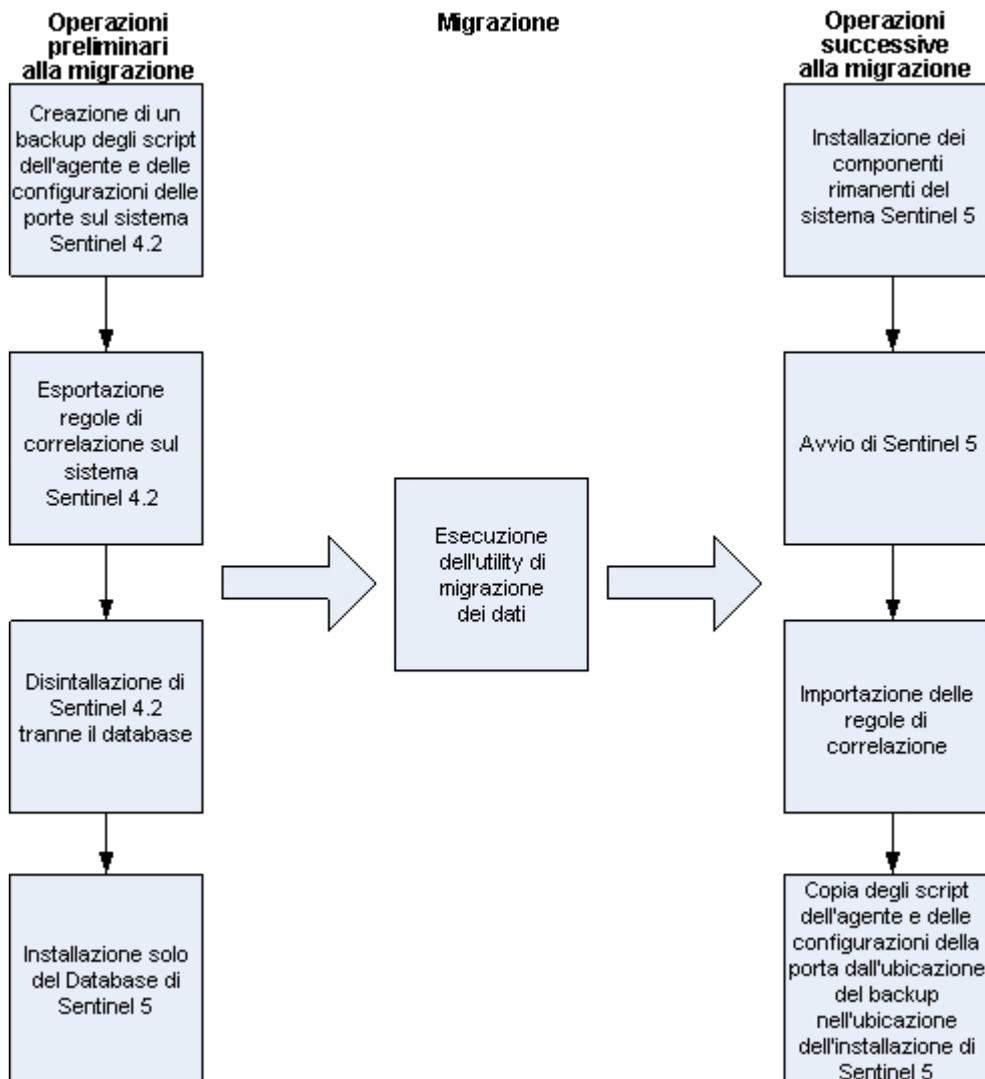
- [Migrazione e upgrade dei dati da v4.2.0 a v5.1.3](#)
- [Patch da v5.x.x a v5.1.3](#)

Migrazione di dati e upgrade da v4.2 a v5.1.3

Il processo di upgrade a Sentinel 5 con migrazione dati da v4.2.0 è composto da:

- Operazioni preliminari alla migrazione
 - Backup di un'istanza del database di Sentinel. Ciò consentirà di recuperare il database v4.2 in caso di errori imprevisti.
 - Eseguire il backup di tutti i comandi di scelta rapida del sistema o degli script eventualmente inclusi nella directory \$ESEC_HOME
 - Esportare le regole di correlazione di Sentinel v4.2 eventualmente esistenti. Per istruzioni, vedere la sezione [Operazioni preliminari alla migrazione – Esportazione di regole di correlazione](#).
 - Eseguire il backup degli script e delle configurazioni delle porte dei servizi di raccolta. Per istruzioni vedere la sezione [Operazioni preliminari alla migrazione – Backup degli script e della configurazione delle porte dei servizi di raccolta](#).
 - Con l'eccezione del componente Database, disinstallare Sentinel v4.2. Per istruzioni vedere [Operazioni preliminari all'installazione – Disinstallazione di v4.2](#).
 - Installare solo il database di Sentinel 5. Per istruzioni, vedere la sezione [Operazioni preliminari all'installazione – Installazione del database di Sentinel 5](#).
- Migrazione
 - Eseguire l'utility di migrazione dei dati. Per istruzioni vedere la sezione [Migrazione](#).
- Operazioni successive alla migrazione
 - Installare i componenti di Sentinel 5 rimanenti. Per istruzioni, vedere la sezione [Operazioni successive alla migrazione – Installazione di Sentinel 5](#).
 - Installare il Sentinel Service Pack più recente.
 - Avviare Sentinel 5.
 - Importare le regole di correlazione eventualmente esistenti. Per istruzioni, vedere la sezione [Operazioni successive alla migrazione – Installazione di Sentinel 5](#).
 - Copiare gli script e le configurazioni delle porte dei servizi di raccolta dall'ubicazione di backup all'ubicazione di installazione di Sentinel 5. Per istruzioni vedere la sezione [Operazioni successive alla migrazione – Riconfigurazione degli script e delle configurazioni delle porte dei servizi di raccolta](#).
 - Riconfigurare le impostazioni di Crystal Reporting correlate a Oracle 9i Client in modo che facciano riferimento al database di Sentinel 5 e importare i modelli di

Crystal Report per Sentinel 5. Per istruzioni, vedere la sezione [Operazioni successive alla migrazione – Configurazione di Sentinel 5 per Crystal Reporting](#).



Server Sentinel

Prima di aggiungere i componenti del server di Sentinel 5 è necessario che la versione precedente del software sia disinstallata. Non disinstallare la versione precedente, ovvero la versione 4.2 del Database, perché necessaria per eseguire la migrazione dei dati da v4.2 a Sentinel 5. Prima di procedere con la disinstallazione, eseguire il backup dei dati contenuti nel computer che esegue il server Sentinel (directory di installazione \$ESEC_HOME e unità radice). Ciò consentirà di recuperare la versione v4.2 in caso di errori imprevisti.

Di seguito sono riportate istruzioni dettagliate per la migrazione e per le operazioni preliminari e successive all'installazione.

Gestione servizi di raccolta

Prima di installare il software di Gestione servizi di raccolta di Sentinel 5 è necessario disinstallare tutte le istanze della versione 4.2 di tale componente. Prima di procedere con la disinstallazione, eseguire il backup dei dati contenuti nel computer che esegue Gestione servizi di raccolta v4.2 (directory di installazione \$ESEC_HOME e unità radice).

Per ogni computer che esegue Gestione servizi di raccolta v4.2 con almeno una porta configurata, salvare una copia del contenuto delle directory seguenti in un'ubicazione facilmente accessibile. Il contenuto di queste directory verrà utilizzato durante le operazioni successive alla migrazione per riconfigurare rapidamente l'impostazione delle porte dei servizi di raccolta nell'installazione v4.2:

- \$WORKBENCH_HOME/Agents: contiene i file di configurazione delle porte.
- \$WORKBENCH_HOME/Elements: contiene gli script del Servizio di raccolta.
- Se non si crea una copia del contenuto delle directory indicate, sarà necessario riconfigurare completamente tutti gli script e le porte dei servizi di raccolta.

NOTA: il Generatore servizi di raccolta e Gestione servizi di raccolta della versione 4.2 non sono compatibili con i componenti v5.

Di seguito sono riportate istruzioni dettagliate per la migrazione e per le operazioni preliminari e successive all'installazione.

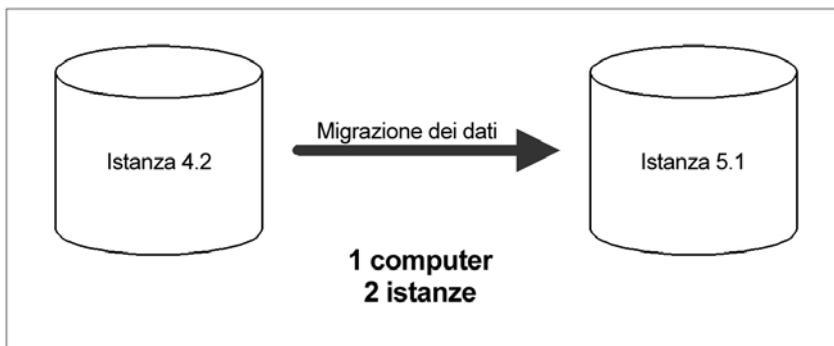
Server Crystal Reporting

È necessario utilizzare i rapporti più recenti del Service Pack più recente dopo aver eseguito l'upgrade a Sentinel 5. I nuovi rapporti sono scritti per funzionare con il nuovo schema di database. Per ottenere il Service Pack più recente, contattare il supporto tecnico Novell.

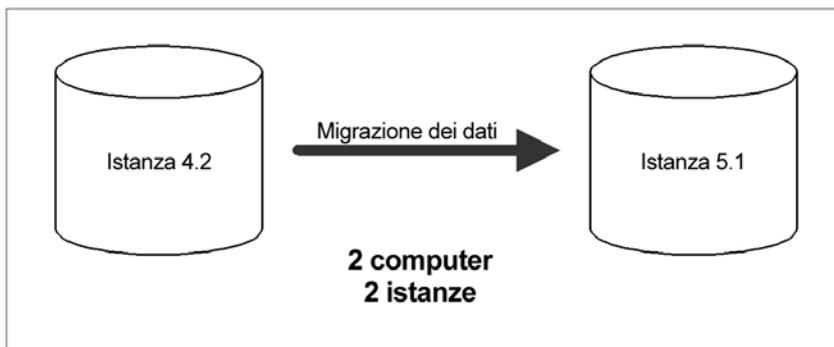
Server di database

Viene fornita una utility per la migrazione dei dati di Sentinel 5 allo scopo di copiare i dati da un database Sentinel 4.2.0 in Solaris 8/9 a un database Sentinel 5.1.3 in Solaris 9. L'utility di migrazione dei dati supporta la migrazione in:

- 1 computer con due istanze del database



- 2 computer con 1 istanza del database per ognuno



L'utility supporta la migrazione dei dati seguenti:

- Utenti e autorizzazioni assegnate
- Gestione filtri
- Opzioni di configurazione dei menu accessibili tramite il pulsante destro del mouse
- Tag CV rinominati
- Configurazioni di partizioni e archivi
- I casi v4.2 vengono copiati in v5 come casi
- Casi ed eventi correlati ai casi

NOTA: l'utility di migrazione dei dati NON eseguirà la migrazione dei dati di eventi, ad eccezione dei dati di eventi associati ai casi. Sarà eseguita la migrazione solo dei dati di eventi associati ai casi.

NOTA: non è possibile visualizzare i dati degli eventi dei casi in Sentinel Control Center. I dati di eventi di casi possono essere visualizzati mediante Crystal Reporting o le query SQL.

Di seguito sono riportate istruzioni dettagliate per la migrazione e per le operazioni preliminari e successive all'installazione.

Operazioni preliminari alla migrazione – Esportazione delle regole di correlazione

Esportazione di un set di regole di correlazione

1. Nella console Sentinel v4.2, nella scheda Amministratore, aprire la finestra Regole di correlazione.
2. Selezionare un gruppo di regole.
3. Fare clic su *Esporta*. Verrà avviato un browser di file. Passare al dispositivo di destinazione sul quale scrivere la regola e fare clic su *OK*. Il gruppo di regole verrà esportato come file xml.

Operazioni preliminari alla migrazione – Backup degli script e delle configurazioni delle porte dei servizi di raccolta.

Backup degli script e delle configurazioni delle porte dei Servizio di raccolta

1. In tutti i computer Sentinel v4.2 che eseguono Gestione servizi di raccolta, creare una directory in cui memorizzare tutti gli script e le configurazioni delle porte dei servizi di raccolta per il computer specifico.

2. Nella directory appena creata, creare un file di testo con l'elenco dei nomi di tutti i servizi di raccolta utilizzati dalla configurazione di una porta in Gestione servizi di raccolta. Utilizzare Generatore servizi di raccolta per determinare i servizi di raccolta utilizzati da Gestione servizi di raccolta. Se Gestione servizi di raccolta è in esecuzione in Solaris, sarà necessario utilizzare Generatore servizi di raccolta in un computer Windows (Generatore servizi di raccolta non è supportato in Solaris).
3. Copiare le directory seguenti nella directory appena creata:
 - \$WORKBENCH_HOME/Agents
 - \$WORKBENCH_HOME/Elements

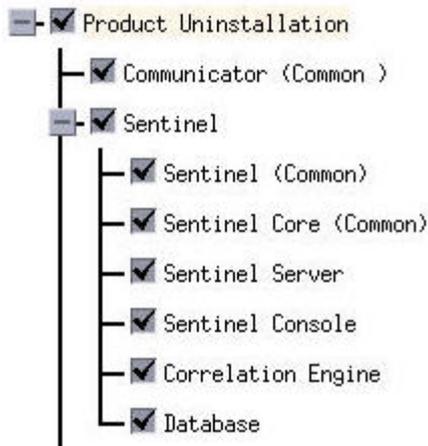
Operazioni preliminari alla migrazione – Disinstallazione della versione v4.2

Disinstallazione della versione v4.2

1. Nel computer che esegue v4.2 e in tutti i computer client, chiudere tutte le console Sentinel e tutti i Generatori di servizi di raccolta.
2. Eseguire il login come utente radice.
3. Arrestare il server Sentinel.
4. Passare alla directory:


```
$ESEC_HOME/_uninst
```
5. Immettere:


```
./uninstall.bin
```
6. Seguire i prompt visualizzati. Selezionare le applicazioni da disinstallare. Selezionare tutte le funzioni.



NOTA: se nel computer è installato software di terze parti, disinstallarlo.

7. Procedere con i prompt visualizzati fino alla finestra di disinstallazione del database.

8. Nella finestra di disinstallazione del database, selezionare *Non eliminare alcun elemento*.

Do you want to delete the database?

Delete the entire database instance.

Delete only the database objects.

Delete nothing.

9. Continuare la disinstallazione utilizzando le altre finestre visualizzate.
10. Riavviare il sistema.

Operazioni preliminari alla migrazione – Installazione del database di Sentinel 5

Installazione del database di Sentinel 5

1. Verificare di aver raccolto le informazioni, eseguito i task e soddisfatto i requisiti specificati nella sezione relativa al database di Sentinel nel *capitolo 3: Installazione di Sentinel per Oracle*, nella sezione relativa alle operazioni preliminari all'installazione.
2. Verificare che Oracle sia configurato come illustrato nella relativa sezione sulla configurazione di Oracle inclusa nel *capitolo 3. Installazione di Sentinel 5 per Oracle*, nella sezione relativa alle operazioni preliminari all'installazione.
3. Eseguire il login come utente radice.
4. Inserire e montare il CD di installazione di Sentinel.
5. Individuare il percorso di directory completo sul CD.
6. Avviare il programma di installazione passando alla directory di installazione sul CD-ROM e digitare:
Per la modalità GUI:

```
./setup.sh
```


oppure
Per la modalità testuale ("headless"):

```
./setup.sh -console
```
7. Dopo aver letto la schermata introduttiva, fare clic su *Avanti*.
8. Accettare il contratto di licenza con l'utente finale e fare clic su *Avanti*.
9. Accettare la directory di installazione di default o fare clic su *Sfoglia* per specificare il percorso di installazione. Fare clic su *Avanti*.

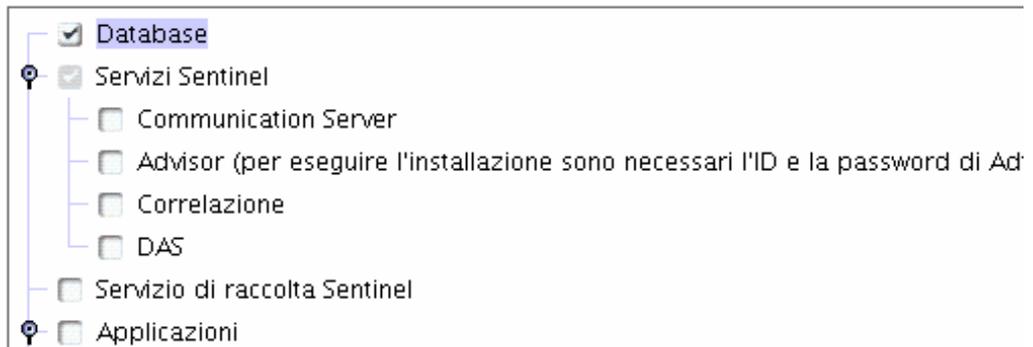
Fare clic su *Avanti* per installare "Sentinel 5" in questa cartella oppure fare clic su *Sfoglia* per installarlo in una cartella diversa.

Nome directory:

10. Selezionare *Personalizzata* (default). Fare clic su *Avanti*.
11. Per le funzioni da installare, deselezionare tutte le funzioni e selezionare *solo Database*. Fare clic su *Avanti*.

NOTA: accertarsi di deselezionare la caratteristica *Servizi Sentinel* di livello superiore. Verrà visualizzata in grigio con un segno di spunta bianco se è ancora selezionata ma tutte le relative funzioni secondarie sono state deselezionate.

Selezionare le funzioni di "Sentinel 5" che si desidera installare:



12. 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 sistema operativo – Il valore di default è `esecadm`
 - Home directory utente amministratore 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: se viene creato un nuovo utente, sarà necessario impostare la relativa password in modo manuale, non nel programma di installazione. È consigliabile eseguire questa operazione direttamente eseguendo il login al sistema dopo l'installazione del prodotto.

NOTA: per soddisfare le rigorose configurazioni di sicurezza necessarie per la certificazione dei criteri comuni, Sentinel richiede una password con le caratteristiche seguenti:

1. Scegliere password composte da non meno di 8 caratteri, di cui almeno un carattere MAIUSCOLO, un carattere minuscolo, un carattere speciale (`#$_`) e un carattere numerico (0-9). Non utilizzare spazi.
 2. Non è possibile includere nella password l'indirizzo di e-mail o una parte qualsiasi del nome completo.
-

-
3. La password non deve essere una parola "comune", ovvero una parola inclusa nel dizionario o di uso gergale.
 4. È necessario che nella password non siano incluse parole di alcuna lingua poiché esistono numerosi programmi per la violazione di password in grado di elaborare milioni di possibili combinazioni di parole in pochi secondi.
 5. È consigliabile scegliere una password facile da ricordare e allo stesso tempo complessa. Ad esempio, Mfhq5#ao (Mio Figlio Ha Quasi 5 Anni Ormai) oppure VaNdq#5a (Vivo a Napoli Da Quasi 5 anni).
-

13. Immettere il nome host (o IP) e il numero di porta (valore di default: 10012) per Communication Server. Fare clic su *Avanti*.
14. Selezionare Oracle come piattaforma del server di database di destinazione, quindi selezionare una delle opzioni seguenti:
 - Creare un nuovo database con oggetti di database – Consente di creare una nuova istanza di database Oracle e di inserire automaticamente nella nuova istanza gli oggetti di database.
 - Aggiungo oggetti di database a un database vuoto esistente - Consente solo di aggiungere il database a un'istanza di database Oracle esistente. L'istanza di database esistente deve essere vuota con l'eccezione della presenza dell'utente esecdba
15. Specificare la directory dei log di installazione del database (default: \$ESEC_HOME/logs/db). Accettare la directory dei log di installazione del database di default o fare clic su *Sfoglia* per specificare un'ubicazione diversa.

Selezionare la piattaforma server del database di destinazione:

Oracle 9i

- Creare un nuovo database con oggetti di database.
- Aggiungo oggetti di database a un database vuoto esistente.

Directory log di installazione database:

/opt/sentinel5.1.3.0/logs/db

Sfoglia

16. Fare clic su *OK* per il nome utente oracle di default.

Please enter the Oracle Username:

oracle

17. Se si è scelto di creare un nuovo database, specificare gli elementi seguenti:
 - Il percorso per il file del driver JDBC Oracle (in genere il nome del file jar è ojdbc14.jar). Percorso completo del file jar, in genere \$ORACLE_HOME/jdbc/lib/ojdbc14.jar (in questo campo non è possibile utilizzare variabili di ambiente).
 - Nome host – Il nome host del computer in cui installare il database. Questo campo non è configurabile se si sta creando una nuova istanza del database.
 - Nome database – Il nome dell'istanza di database da installare.

NOTA: è necessario assegnare al database un nome diverso da quello specificato per l'installazione della versione 4.2.

Oracle Configuration

Select the Oracle JDBC driver (ojdbc14.jar):

Host name:

Database Name:

18. Se si è scelto di aggiungere oggetti di database a un database Oracle esistente vuoto, verrà richiesto di specificare le informazioni seguenti.
- Il percorso per il file del driver JDBC Oracle (in genere il nome del file jar è ojdbc14.jar). Percorso completo del file jar, in genere \$ORACLE_HOME/jdbc/lib/ojdbc14.jar (in questo campo non è possibile utilizzare variabili di ambiente).
 - Nome database o indirizzo IP – Il nome o l'indirizzo IP dell'host in cui si trova il database di Oracle al quale si desidera aggiungere oggetti di database. Può essere il nome host locale o un nome host remoto.
 - Nome database – Il nome dell'istanza di database Oracle vuoto esistente al quale si desidera aggiungere oggetti di database (il valore di default è ESEC). È necessario assegnare al database un nome diverso da quello specificato per l'installazione della versione 4.2. Questo nome di database deve essere visualizzato come nome di servizio nel file tnsnames.ora (nella directory \$ORACLE_HOME/network/admin/) del computer dal quale si sta eseguendo il programma di installazione.

NOTA: se il nome del database non è presente nel file tnsnames.ora, il programma di installazione non visualizzerà un errore a questo punto dell'installazione (poiché verifica la connessione utilizzando una connessione JDBC diretta), ma l'installazione del database non riuscirà quando il programma di installazione tenterà di connettersi al database via sqlplus. Se l'installazione del database si interrompe a questo punto, senza uscire dal programma di installazione modificare il Service Name (Nome servizio) per il database nel file tnsnames.ora presente nel computer, quindi tornare al programma di installazione e riprendere l'installazione. In questo modo verrà ritentata l'installazione del database con i nuovi valori presenti nel file tnsnames.ora.

- Porta di database (il valore di default è 1521)
- Per l'utente amministratore del database di Sentinel (DBA), specificare la password per l'utente "esecdba". La password esecdba deve essere uguale a quella dell'installazione di v4.2. Il campo nome utente in questo prompt non è modificabile.

Oracle Configuration

Select the Oracle JDBC driver (ojdbc14.jar):

Host Name:

Database Name:

Port:

Login: Password:

19. Se si è scelto di creare un nuovo database, verrà visualizzato il prompt seguente:
- Memoria Oracle (MB) – La quantità di RAM da allocare a questa istanza del database di Oracle.
 - Porta listener – La porta sulla quale creare un listener Oracle (il valore di default è 1521).
 - Password utente SYS e conferma password – SYS è un utente Oracle di default che verrà creato nella nuova istanza del database. La password utente verrà impostata sul valore specificato in questo campo.
 - Password utente SYSTEM e conferma password – SYSTEM è un utente Oracle di default che verrà creato nella nuova istanza del database. La password utente verrà impostata sul valore specificato in questo campo.

Oracle Configuration

Oracle Memory (MB):

Listener Port:

SYS User Credentials SYSTEM User Credentials

Password: Password:

Confirm Password: Confirm Password:

20. Se si è scelto di creare un nuovo database, verrà richiesto di specificare le dimensioni del database: Sono disponibili le opzioni seguenti:
- Standard (20 GB)
 - Grandi (400 GB)
 - Personalizzate (specificare le dimensioni manualmente). Se si seleziona questa opzione verrà richiesto di specificare:
 - dimensione iniziale di ogni file di database in MB (100 – 10.000)
 - dimensione massima di ogni file di database in MB (2.000 – 100.000)
 - dimensione di tutti i file di database in MB (7.000 – 2.000.000)
 - dimensione di ogni file di log in MB (100 – 100.000)

Please select Standard, Large, or Custom database size.

Standard (20,000MB, 30 day capacity @ 500,000 events per day)

Large (400,000MB, 30 day capacity @ 10,000,000 events per day)

Custom (specify database sizing manually)

21. Se si è scelto di creare un nuovo database, verrà richiesto di specificare l'ubicazione di memorizzazione per i file di database seguenti.

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

Il programma di installazione non creerà tali directory, per cui è necessario crearle esternamente prima di continuare.

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>
```

presumendo che "oracle" sia il nome utente Oracle e "dba" il nome gruppo Oracle.

- Directory dati
- Directory indice
- Directory dati di riepilogo
- Directory indice di riepilogo
- Directory dei file temporanei e dello spazio delle tabelle di annullamento
- Directory log di ripetizione membro A
- Directory log di ripetizione membro B

Please enter the storage location for the following database files.

Data Directory: /u01/home/oracle

Index Directory: /u01/home/oracle

Summary Data Directory: /u01/home/oracle

Summary Index Directory: /u01/home/oracle

Temp and Undo Directory: /u01/home/oracle

Redo Log Member A Directory: /u01/home/oracle

Redo Log Member B Directory: /u01/home/oracle

22. Se si è scelto di creare un nuovo database, specificare le informazioni di autenticazione per l'amministratore del database di Sentinel (DBA). Corrisponde a esecdba, il proprietario degli oggetti di database.
23. Specificare le informazioni di autenticazione per l'utente del database dell'applicazione Sentinel. Corrisponde a esecapp, il nome utente dell'applicazione Sentinel utilizzato dai processi Sentinel per la connessione al database.
24. Specificare le informazioni di autenticazione per l'utente del database amministratore di Sentinel. Corrisponde a esecadm, l'utente amministratore di Sentinel.
25. Fare clic su *Avanti* nella finestra di riepilogo dell'installazione del database.

26. Una volta completata l'installazione, verrà chiesto di riavviare il sistema. Fare clic su *Fine* per riavviare il sistema.

Migrazione

L'utility di migrazione dei dati eseguirà la migrazione solo degli elementi seguenti:

- Utenti e autorizzazioni assegnate
- Gestione filtri
- Opzioni di configurazione dei menu accessibili tramite il pulsante destro del mouse
- Tag CV rinominati
- Configurazioni di partizioni e archivi
- I casi v4.2 vengono copiati in v5 come casi
- Casi ed eventi correlati ai casi

NOTA: l'utility di migrazione dei dati NON eseguirà la migrazione dei dati di eventi, ad eccezione dei dati di eventi associati ai casi. Sarà eseguita la migrazione solo dei dati di eventi associati ai casi.

NOTA: non è possibile visualizzare tramite Sentinel Control Center i dati degli eventi dei casi. I dati di eventi di casi possono essere visualizzati mediante Crystal Reporting o le query SQL.

Per i database di Sentinel 4.2 che non utilizzano la password `esecdba` per il proprietario dello schema del database di Sentinel.

NOTA: con questa procedura viene aggiunto l'id di `esecdba` al database v4.2 per consentire la migrazione dei dati da v4.2 a v5.

1. Per Solaris eseguire il login come proprietario del software Oracle.
2. Passare alla directory:

```
$ESEC_HOME/utilities/db/scripts/ddl/oracle/Migration
```

3. Mediante SQL*Plus, connettersi al database v4.2 come SYSDBA.
4. Al prompt SQL (SQL>), digitare:

```
@import_add_esecdba.sql
```

5. Uscire da SQL*Plus.

NOTA: dopo aver eseguito la migrazione dei dati, è possibile eliminare l'utente `esecdba` dal database Sentinel 4.2 utilizzando Oracle Enterprise Manager.

Migrazione dati

NOTA: in Solaris l'utility di migrazione dati utilizza Oracle*Net per effettuare la connessione al database Sentinel 5 e tra i database di Sentinel 5 e 4.2. Assicurarsi che il file `tnsnames.ora` in cui si esegue l'utility di migrazione dati contenga le voci per i database Sentinel sia 4.2 che 5 in modo da poter stabilire le connessioni Oracle*Net.

1. Eseguire il login come utente radice.
2. Verificare nelle variabili di ambiente che `java` (versione 1.4.2) sia nel `PATH`. È possibile eseguire questa verifica mediante il comando seguente sulla riga di comando:

```
java -version
```

Se il comando indicato non riesce, individuare l'ubicazione di installazione di java nel sistema o scaricare e installare java. Aggiornare quindi la variabile di ambiente PATH perché includa l'eseguibile java. Se ad esempio java è installato nella directory:

```
/opt/sentinel5.1.3.0/Sun-1.4.2
```

Aggiungere quanto segue all'inizio della variabile di ambiente PATH:

```
/opt/sentinel5.1.3.0/Sun-1.4.2/bin:
```

3. Montare il CD di installazione del software Sentinel 5 nel server di database che contiene il database si Sentinel 5.

4. Passare alla directory seguente nel CD di installazione del software Sentinel 5:

```
sentinel/dbsetup/bin
```

5. Eseguire il comando:

```
./MigrateDb.sh
```

6. Verrà richiesto quanto segue:

- nome host del database che esegue il database di Sentinel 5 al quale si sta eseguendo la migrazione
- nome del database di destinazione (del database Sentinel 5 al quale si sta eseguendo la migrazione)
- password esecdba (la password deve essere la stessa per l'utente esecdba nei database Sentinel v4.2 e v5)
- nome del database di origine (nome del database v4.2)
- directory di log (in cui saranno memorizzati i file di log di migrazione dei dati)
- opzione di migrazione:
 - (1) Impostazioni di sistema
 - (2) Casi
 - (3) entrambi
 - (4) fatto

NOTA: è necessario che la migrazione delle impostazioni di sistema venga eseguita correttamente prima di continuare con la migrazione dei casi.

NOTA: se la migrazione delle impostazioni di sistema non riesce, disinstallare il database di Sentinel 5 selezionando l'opzione che consente di eliminare solo gli oggetti di database. Reinstallare quindi il database di Sentinel 5 selezionando l'opzione che consente di aggiungere gli oggetti di database a un database vuoto esistente. Riprovare quindi ad eseguire la migrazione dei dati attenendosi alle istruzioni fornite.

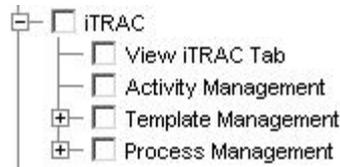
NOTA: se la migrazione dei casi non riesce, eseguirla di nuovo. L'utility di migrazione ricomincerà dal punto di errore. Non sono necessari altri task di pulizia.

NOTA: dopo aver eseguito la migrazione dei dati, è possibile eliminare l'utente esecdba dal database Sentinel 4.2 utilizzando Oracle Enterprise Manager qualora fosse necessario aggiungerlo per l'utility di migrazione dati.

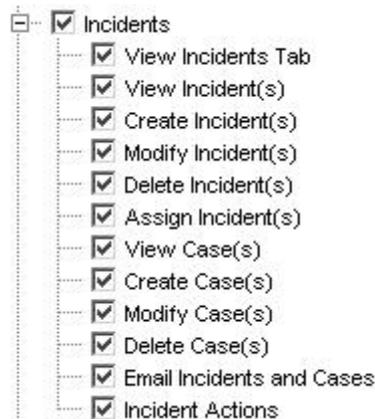
Operazioni successive alla migrazione – Installazione di Sentinel 5

In Sentinel 5, le funzioni seguenti sono nuove, diversi o sono state rimosse.

- iTRAC: nuova funzione. Le autorizzazioni utente associate sono:



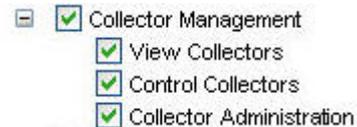
- Casi – aggiunta di Amministrazione casi La funzione relativa a tutti i casi è stata rimossa. Le autorizzazioni utente associate sono:



Casi di Sentinel v4.2

Casi di Sentinel v5

- Gestione servizi di raccolta – in v4.2 corrisponde a Wizard Monitoring. Alla scheda 'View Wizards' è stata sostituita la scheda 'Visualizza servizi di raccolta. 'Control Wizards and Collector' sono stati sostituiti con 'Controllo servizi di raccolta' e 'Amministrazione servizi di raccolta. Le autorizzazioni utente associate sono:



Sentinel v4.2 Wizard Monitoring

Gestione servizi di raccolta di Sentinel v5

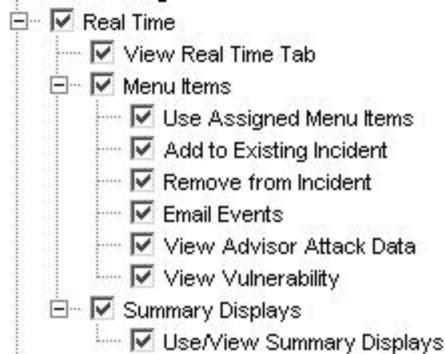
- Amministrazione – Aggiunta di statistiche DAS, gestione della sessione utente e gestione dei ruoli iTRAC. Le 'Regole di correlazione' sono state rinominate come 'Correlazione'. La funzione di configurazione degli eventi è stata spostata in Gestione dati Sentinel. La 'Configurazione utente' è stata rinominata in 'Gestione utenti'. Le autorizzazioni utente associate sono:



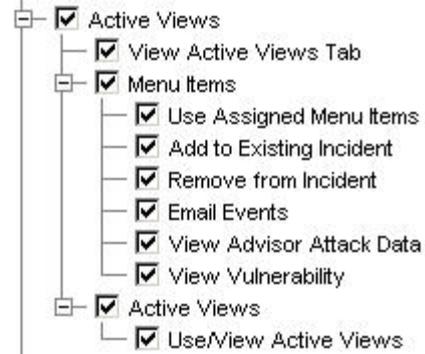
Sentinel v4.2 Administration

Amministrazione di Sentinel v5

- ActiveViews™ - Nella versione v4.2 era denominato Real Time. 'Summary Displays' è stato rinominato in Active Views. Le autorizzazioni utente associate sono:



Sentinel v4.2 Real Time



Sentinel v5 Active Views™

- La funzionalità di panoramica del sistema non è disponibile in Sentinel 5.

Installazione di Sentinel 5

1. Installare Sentinel 5, vedere il capitolo 3 relativo all'installazione: 'Installazione di Sentinel 5 per Oracle'.
2. Installare il Service Pack di Sentinel più recente.
3. Se si desidera aggiungere nuove funzionalità agli utenti esistenti della versione v4.2, eseguire la procedura seguente:
 - a. Verificare che il server Sentinel sia in esecuzione.
 - b. Eseguire il login a Sentinel Control Center come utente con autorizzazioni di amministrazione/gestione utenti (ovvero esecadm).
 - c. In Sentinel Control Center fare clic sulla scheda Amministratore. Espandere Configurazione utente nel riquadro di navigazione o dalla barra di navigazione fare clic su *Amministrazione > Configurazione utente*.
 - d. Fare clic con il pulsante destro del mouse sull'utente al quale si desidera aggiungere la funzionalità (ovvero esecadm) e selezionare *Dettagli utente*. Fare clic sulla scheda *Autorizzazioni*.
 - e. Espandere iTRAC e assegnare le necessarie autorizzazioni.
 - f. Espandere Casi e assegnare 'Amministrazione casi in base alle necessità.
 - g. Espandere Gestione servizi di raccolta e assegnare 'Amministrazione servizi di raccolta' in base alle necessità.
 - h. Espandere Amministrazione e assegnare Statistiche DAS, 'Gestione sessioni utente e 'Gestione ruoli iTRAC in base alle necessità.
 - i. Fare clic sulla scheda *Ruoli* e assegnare il ruolo di amministratore o workflow di analisi in base alle necessità.
 - j. Fare clic su *OK*.
4. Se applicabile, importare le regole di correlazione. I gruppi di regole esportati da Sentinel 4.2 saranno visualizzati come cartelle delle regole se importati in Sentinel 5.
5. Copiare dal backup gli script dei servizi di raccolta e le configurazioni delle porte attenendosi alle istruzioni riportate nella sezione [Operazioni successive alla migrazione – Riconfigurazione degli script e delle configurazioni delle porte dei servizi di raccolta](#)

Operazioni successive alla migrazione – Riconfigurazione degli script e delle configurazioni delle porte dei servizi di raccolta.

In ogni computer in cui sono installati i servizi di raccolta di Sentinel 5 (Gestione servizi di raccolta), eseguire la procedura seguente per riapplicare gli script e le configurazioni delle porte dei servizi di raccolta utilizzati nell'installazione di Sentinel v4.2.

Per riapplicare gli script e le configurazioni delle porte dei servizi di raccolta

1. Arrestare Gestione servizi di raccolta eseguendo il comando seguente come utente esecadm:

```
$ESEC_HOME/wizard/agent-manager.sh stop
```

2. Copiare i file seguenti dall'ubicazione in cui è stata archiviata una copia di backup della directory \$WORKBENCH_HOME/Agents relativa all'installazione di Sentinel v4.2 nella directory \$WORKBENCH_HOME/Agents dell'installazione attuale di Sentinel 5 (sovrascrivere i file se necessario):

- localhost_portcfg.dat
- localhost_snmpcfg.dat

3. Leggere il file di testo creato durante le operazioni preliminari alla migrazione con l'elenco dei servizi di raccolta utilizzati dall'installazione di Sentinel v4.2 Gestione servizi di raccolta nel computer. Per eseguire questo passaggio sarà necessario conoscere i nomi dei servizi di raccolta.
4. Copiare le directory i cui nomi equivalgono a quelli del servizio di raccolta nel file di testo dall'ubicazione in cui è stata archiviata la copia di backup della directory \$WORKBENCH_HOME/Elements relativa all'installazione di Sentinel v4.2 alla directory \$WORKBENCH_HOME/Elements dell'installazione attuale di Sentinel 5 (sovrascrivere i file e/o le directory se necessario).
5. Scaricare l'utility UpgradePortCfgFile dal sito Web del supporto tecnico di Sentinel ([download](#)).
6. Estrarre il file ZIP UpgradePortCfgFile.
7. Aprire un prompt dei comandi e passare alla directory dell'utility UpgradePortCfgFile estratta. Da questa directory, eseguire il comando:

```
./UpgradePortCfgFile.sh
```

8. Eseguire il comando seguente come utente radice per garantire che le impostazioni di proprietà dei file appena copiati siano impostate correttamente:

```
chown -R esecadm:esec $ESEC_HOME/wizard
```

9. Avviare Gestione servizi di raccolta eseguendo il comando seguente come utente esecadm:

```
$ESEC_HOME/wizard/agent-manager.sh start
```

Operazioni successive alla migrazione – Configurazione di Sentinel 5 per Crystal Reporting

Se si desidera passare dall'esecuzione di Crystal Reporting per v4.2 all'esecuzione di Crystal Reporting in Sentinel 5, è necessario eseguire le operazioni seguenti:

- Modificare le impostazioni del client Oracle 9i correlate a Crystal Reporting affinché puntino al database di Sentinel 5.

- Importare i modelli di Crystal Report (inclusi i modelli di migrazione dei dati) dal Service Pack più recente.

Per ulteriori informazioni, vedere il capitolo relativo all'installazione di Crystal Reports.

Patch da v5.x.x a v5.1.3

Eeguire questa procedura su tutti i computer nei quali sono installati i componenti di Sentinel.

Se si sta eseguendo il programma di installazione delle patch dal computer in cui si è originariamente installato il componente Database, sarà necessario conoscere la password dell'utente amministratore del database di Sentinel (esecdba).

Upgrade da v5.x.x a v5.1.3 per Solaris

1. Eseguire il login come utente radice.
2. Se applicabile, creare una copia di backup del file `syslog.conf`.

NOTA: se si esegue v5.1.1 sp1 o successive e si apportano modifiche al file `syslog.conf`, sarà necessario creare una copia del file. Il programma di installazione delle patch sovrascriverà il file `syslog.conf`. Dopo aver applicato la patch, modificare o sovrascrivere il nuovo file `syslog.conf` affinché corrisponda a quello originale.

3. Inserire e montare il CD di installazione delle patch di Sentinel.
4. Avviare il programma di installazione passando alla directory delle patch appropriata sul CD-ROM ed eseguendo il comando:

Per la modalità GUI:

```
./setup.sh
```

oppure

Per la modalità testuale ("headless"):

```
./setup.sh -console
```

5. Fare clic su *Avanti* nella schermata introduttiva.
6. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
7. Fare clic su *Avanti* fino a visualizzare la finestra delle informazioni sul database.
8. Verificare che il tipo di database sia corretto. Selezionare l'ubicazione della directory dei log di installazione del database. Fare clic su *Avanti*.
9. Verificare che le informazioni per il server Oracle siano corrette. Immettere la password `esecdba`. Seguire i prompt rimanenti del programma di installazione.

Aggiornamento del connettore syslog

Se si utilizzano gli script del connettore `syslog` di una versione di Sentinel precedente alla 5.1.1.1, ovvero 5.0, 5.01.0, 5.1.0.0 o 5.1.1.0, è necessario iniziare a utilizzare gli script aggiornati del connettore inclusi nella patch. Per passare ai nuovi script del connettore `syslog`, installarli dopo aver rimosso quelli precedenti.

Il connettore syslog viene ora installato con script eseguibili su Windows e UNIX, nonché con file di configurazione migliorati. L'installazione del server proxy syslog come servizio è stata inoltre semplificata.

Per rimuovere il connettore syslog

1. Eseguire il login come utente radice.
2. Eseguire `cd $ESEC_HOME/wizard/syslog`
3. `./syslog-server.sh remove`

Per installare il connettore syslog

1. Eseguire il login come utente radice.
2. Eseguire `cd $ESEC_HOME/wizard/syslog`
3. Eseguire `./syslog-server.sh install`
4. Se si apportano modifiche al file `syslog.conf` dell'installazione originale, sarà necessario modificare o sovrascrivere il nuovo file affinché rifletta quello originale. Il file `syslog.conf` si trova in:

`$ESEC_HOME/wizard/syslog/config`

Ulteriore aggiornamento da v5.0.x a v5.1.3

Dopo aver eseguito l'upgrade da v5.0.x a v5.1.3, è necessario aggiornare le opzioni relative alle autorizzazioni di gestione degli utenti e alla configurazione dei menu. Facoltativamente, è possibile aggiornare l'autorizzazione di visualizzazione server.

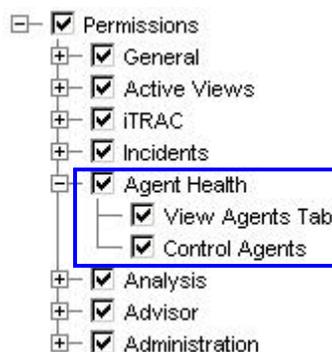
Aggiornamento delle autorizzazioni di gestione degli utenti per v5.0.x a v5.1.3

Quando si esegue l'upgrade da v5.0.x a v5.1.3, Collector Health viene modificato in Gestione servizi di raccolta con l'aggiunta di un'altra funzionalità di Amministrazione servizi di raccolta.

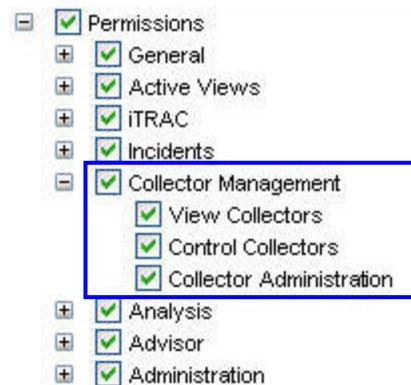
Aggiornamento delle autorizzazioni di gestione utenti

1. Eseguire il login a Sentinel Control Center come utente con autorizzazioni di amministrazione/gestione utenti.

In v5.1, Stato servizio di raccolta in Autorizzazioni è stato modificato in 'Gestione servizi di raccolta' con l'aggiunta di un'altra autorizzazione.



Autorizzazioni utente di Sentinel v5.0



Autorizzazioni utente di Sentinel v5.1.x

2. In Sentinel Control Center fare clic sulla scheda Amministratore. Espandere Configurazione utente nel riquadro di navigazione o dalla barra di navigazione fare clic su *Amministrazione > Configurazione utente*.
3. Fare clic con il pulsante destro del mouse su un utente Amministratore (ovvero esecadm o un altro utente amministratore) e scegliere *Dettagli utente*. Fare clic sulla scheda *Autorizzazioni*.
4. Espandere *Gestione servizi di raccolta* e assegnare *'Amministrazione servizi di raccolta'*. Fare clic su *OK*.

Aggiornamento delle opzioni di configurazione menu da v5.0.x a v5.1.3

Se prima dell'upgrade a v5.1 sono state create voci aggiuntive nella configurazione dei menu, sarà necessario aggiornare i percorsi dei comandi. Come per la versione 5.1.0.0 in Solaris, il comando da eseguire nella configurazione dei menu deve risiedere nella directory \$ESEC_HOME/sentinel/exec. Come per la versione 5.1.0.0 in Solaris, il comando da eseguire nella configurazione dei menu deve risiedere nella directory \$ESEC_HOME/sentinel/exec. Se è necessario eseguire un comando altrove nel filesystem, creare un collegamento simbolico da un'ubicazione in \$ESEC_HOME/sentinel/exec al comando da eseguire.

Per il corretto funzionamento della configurazione dei menu con traceroute è necessario modificare manualmente 'tracert' in 'traceroute'.

Per aggiungere un'opzione al menu di configurazione dei menu

1. Eseguire il login a Sentinel Control Center come utente con autorizzazioni di amministrazione/gestione utenti.
2. Fare clic sulla scheda *Amministratore*.
3. Nella barra di spostamento fare clic su *Amministratore > Configurazione menu*.
4. Nella finestra Configurazione menu fare clic su *Modifica* quindi evidenziare l'elemento di menu da aggiornare. Fare clic su *Dettagli*.
5. Nella finestra di dialogo Configurazione menu eseguire le operazioni necessarie in:
 - Riga di comando/URL
 - Parametri: devono essere racchiusi dal segno di percentuale, ad esempio %EbentName%

NOTA: per un elenco dei tag disponibili che è possibile utilizzare durante la definizione dei parametri, fare clic su ? nella finestra di dialogo Configurazione menu oppure vedere il capitolo relativo al tag Meta nella Guida di riferimento dell'utente di Sentinel.

6. Fare clic su *OK*.
7. Fare clic su *Salva*.

Aggiornamento dell'opzione di visualizzazione server da v5.0.x a v5.1.3

Per utilizzare la schermata Visualizzazione server dopo l'installazione della patch, è necessario concedere l'apposita autorizzazione all'utente Sentinel che utilizza Gestione utenti. Gestione utenti si trova nella scheda Amministratore di Sentinel Control Center.

ALL GROUP BY SERVER HOSTNAME						
	Starts	AutoRestarts	StartTime	State	UpTime	Version
Processes Health						
localhost.localdomain						
Communication Server	1	0	01/20/2006 19:47:09 EST	Running	11:01s	5.1.1.1
Correlation Engine	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
DAS_Binary	2	0	01/20/2006 19:51:59 EST	Running	6:11s	5.1.1.1
DAS_Query	3	1	01/20/2006 19:48:04 EST	Running	10:06s	5.1.1.1
DAS_RT	2	0	01/20/2006 19:47:54 EST	Running	10:16s	5.1.1.1
DAS_ITRAC	2	0	01/20/2006 19:47:54 EST	Running	10:16s	5.1.1.1
Query Manager	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
RuleG Checker	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
Sonic Lock Remover	0	0		NOT_INITIALIZED		5.1.1.1

Ready Refresh Options Refreshed At: Fri Jan 20 19:57:26 EST 2006

Server Crystal Reporting

Dopo aver eseguito l'upgrade a Sentinel 5.1.3, inclusa l'applicazione del Service Pack più recente, è necessario importare i rapporti dall'ultimo Service Pack. Per ulteriori informazioni, vedere il capitolo relativo a *Crystal Reports* nella *Guida all'installazione di Sentinel*.

Aggiornamento di e-mail Sentinel per l'autenticazione SMTP

Se nel sistema è necessaria l'autenticazione SMTP, sarà necessario aggiornare il file `execution.properties`. Il file si trova nel computer in cui è installato DAS. Nella directory `$ESEC_HOME/sentinel/config`. Per configurare questo file, eseguire `mailconfig.sh` per modificare il file e `mailconfigtest.sh` per eseguire il test delle modifiche.

Per configurare il file `execution.properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
$ESEC_HOME/sentinel/config
```

2. Eseguire il comando `mailconfig` come indicato di seguito:

```
./mailconfig.sh -host <server SMTP> -from <indirizzo e-mail di origine> -user <utente autenticazione posta> -password
```

Esempio:

```
./mailconfig.sh -host 192.0.2.14 -from my_name@domain.com -user my_user_name -password
```

Dopo aver immesso questo comando verrà richiesto di specificare una nuova password.

```
Immettere la password:*****
```

```
Confermare la password:*****
```

NOTA: quando si utilizza l'opzione relativa alla password, deve trattarsi dell'ultimo argomento.

Per eseguire il test della configurazione del file `execution.properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
$ESEC_HOME/sentinel/config
```

2. Eseguire il comando `mailconfigtest` come indicato di seguito:

```
./mailconfigtest.sh -to <indirizzo e-mail di  
destinazione>
```

Se l'invio del messaggio e-mail è riuscito correttamente, il messaggio sarà ricevuto all'indirizzo di destinazione e verrà visualizzato il messaggio seguente sullo schermo dell'utente.

```
Messaggio e-mail inviato.
```

Controllare la casella postale e-mail per confermare la ricezione del messaggio. La riga dell'oggetto e il contenuto dovrebbero essere:

```
Oggetto: Testing Sentinel mail property
```

```
This is a test for Sentinel mail property set up.
```

```
If you see this message, your Sentinel mail property  
has been configured correctly to send emails
```


7

Migrazione di dati e patch per MS SQL

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

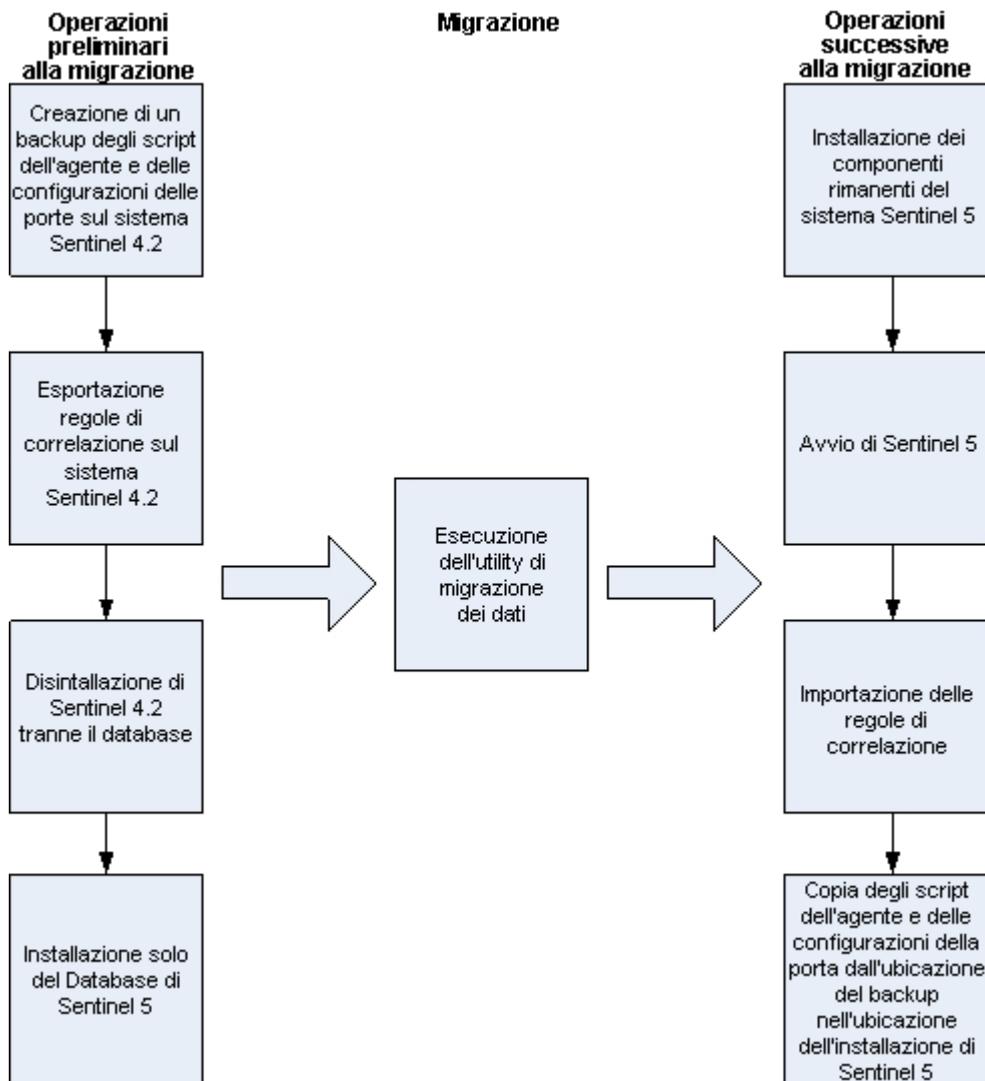
In questo capitolo vengono trattate le operazioni relative alla migrazione dei dati e all'upgrade per:

- [Migrazione e upgrade dei dati da v4.2.1 a v5.1.3](#)
- [Patch da v5.x.x a v5.1.1](#)

Migrazione di dati e upgrade da v4.2 a v5.1.3

Il processo di upgrade a Sentinel 5 con migrazione dati da v4.2.0 è composto da:

- Operazioni preliminari alla migrazione
 - Backup di un'istanza del database del server Sentinel. Ciò consentirà di recuperare il database v4.2 in caso di errori imprevisti.
 - Eseguire il backup di tutti i comandi di scelta rapida del sistema o degli script eventualmente inclusi nella directory %ESEC_HOME%
 - Esportare le regole di correlazione di Sentinel v4.2 eventualmente esistenti. Per istruzioni, vedere la sezione [Operazioni preliminari alla migrazione – Esportazione di regole di correlazione](#).
 - Eseguire il backup degli script e delle configurazioni delle porte dei servizi di raccolta. Per istruzioni vedere la sezione [Operazioni preliminari alla migrazione – Backup degli script e della configurazione delle porte dei servizi di raccolta](#).
 - Con l'eccezione del componente Database, disinstallare Sentinel v4.2. Per istruzioni vedere [Operazioni preliminari all'installazione – Disinstallazione di v4.2](#).
 - Installare solo il database di Sentinel 5. Per istruzioni, vedere la sezione [Operazioni preliminari all'installazione – Installazione del database di Sentinel 5](#).
- Migrazione
 - Eseguire l'utility di migrazione dei dati. Per istruzioni vedere la sezione [Migrazione](#).
- Operazioni successive alla migrazione
 - Installare i componenti di Sentinel 5 rimanenti. Per istruzioni, vedere la sezione [Operazioni successive alla migrazione – Installazione di Sentinel 5](#).
 - Installare il Sentinel Service Pack più recente.
 - Avviare Sentinel 5.
 - Importare le regole di correlazione eventualmente esistenti. Per istruzioni, vedere la sezione [Operazioni successive alla migrazione – Installazione di Sentinel 5](#).
 - Copiare gli script e le configurazioni delle porte dei servizi di raccolta dall'ubicazione di backup all'ubicazione di installazione di Sentinel 5. Per istruzioni vedere la sezione [Operazioni successive alla migrazione – Riconfigurazione degli script e delle configurazioni delle porte dei servizi di raccolta](#).
 - Se si esegue il server Crystal con Sentinel, importare i modelli di Crystal Report di Sentinel 5. Per istruzioni, vedere la sezione [Operazioni successive alla migrazione – Configurazione di Sentinel 5 per Crystal Reporting](#).



Server Sentinel

Prima di aggiungere i componenti del server di Sentinel 5 è necessario che la versione precedente del software sia disinstallata. Non disinstallare la versione precedente, ovvero la versione 4.2 del Database, perché necessaria per eseguire la migrazione dei dati da v4.2 a Sentinel 5. Prima di procedere con la disinstallazione, eseguire il backup dei dati contenuti nel computer che esegue il server Sentinel (directory di installazione %ESEC_HOME% e unità radice). Ciò consentirà di recuperare la versione v4.2 in caso di errori imprevisti.

Di seguito sono riportate istruzioni dettagliate per la migrazione e per le operazioni preliminari e successive all'installazione.

Gestione servizi di raccolta

Prima di installare il software di Gestione servizi di raccolta di Sentinel 5 è necessario disinstallare tutte le istanze della versione 4.2 di tale componente. Prima di procedere con la disinstallazione, eseguire il backup dei dati contenuti nel computer che esegue Gestione servizi di raccolta v4.2 (directory di installazione %ESEC_HOME% e unità radice).

Per ogni computer che esegue Gestione servizi di raccolta v4.2 con almeno una porta configurata, salvare una copia del contenuto delle directory seguenti in un'ubicazione facilmente accessibile. Il contenuto di queste directory verrà utilizzato durante le operazioni successive alla migrazione per riconfigurare rapidamente l'impostazione delle porte dei servizi di raccolta nell'installazione v4.2:

- %WORKBENCH_HOME%/Agents: contiene i file di configurazione delle porte.
- %WORKBENCH_HOME%/Elements: contiene gli script dei Servizi di raccolta.
- Se non si crea una copia del contenuto delle directory indicate, sarà necessario riconfigurare completamente tutti gli script e le porte dei servizi di raccolta.

NOTA: il Generatore servizi di raccolta e Gestione servizi di raccolta della versione 4.2 non sono compatibili con i componenti v5.

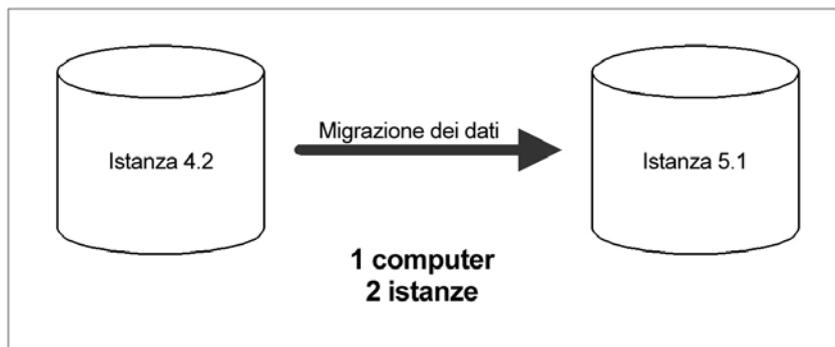
Di seguito sono riportate istruzioni dettagliate per la migrazione e per le operazioni preliminari e successive all'installazione.

Server Crystal Reporting

È necessario utilizzare i rapporti più recenti del Service Pack più recente dopo aver eseguito l'upgrade a Sentinel 5. I nuovi rapporti sono scritti per funzionare con il nuovo schema di database. Per ottenere il Service Pack più recente, contattare il supporto tecnico di Sentinel.

Server di database

Viene fornita una utility per la migrazione dei dati di Sentinel 5 allo scopo di copiare i dati da un database Sentinel 4.2.1 in Sentinel v5.1.2. L'utility di migrazione dei dati supporta la migrazione solo con il database sia Sentinel 4.2.1 che Sentinel 5.1.3 nello stesso computer e nella stessa istanza di SQL Server, ma ognuno in un diverso database.



Vengono migrati i dati seguenti:

- Utenti e autorizzazioni assegnate
- Gestione filtri
- Opzioni di configurazione dei menu accessibili tramite il pulsante destro del mouse
- Tag CV rinominati
- Configurazioni di partizioni e archivi
- I casi v4.2 vengono copiati in v5 come casi
- Casi ed eventi correlati ai casi

NOTA: l'utility di migrazione dei dati NON eseguirà la migrazione dei dati di eventi, ad eccezione dei dati di eventi associati ai casi. Sarà eseguita la migrazione solo dei dati di eventi associati ai casi.

NOTA: non è possibile visualizzare tramite Sentinel Control Center i dati degli eventi dei casi. I dati di eventi di casi possono essere visualizzati mediante Crystal Reporting o le query SQL.

Operazioni preliminari alla migrazione – Esportazione delle regole di correlazione

Importazione di un set di regole di correlazione

1. Nella console Sentinel v4.2, nella scheda Amministratore, aprire la finestra Regole di correlazione.
2. Selezionare un gruppo di regole.
3. Fare clic su *Esporta*. Verrà avviato un browser di file. Passare al dispositivo di destinazione sul quale scrivere la regola e fare clic su *OK*. Il gruppo di regole verrà esportato come file xml.

Operazioni preliminari alla migrazione – Backup degli script e delle configurazioni delle porte dei servizi di raccolta.

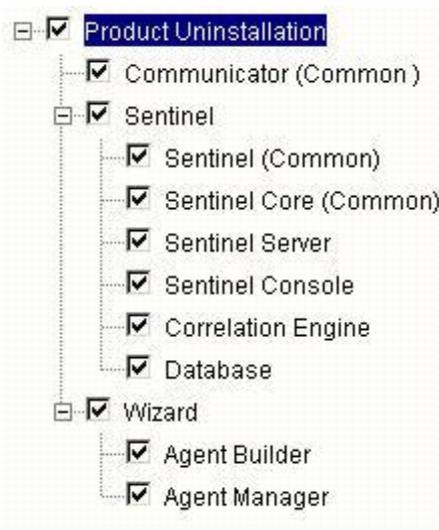
Backup degli script e delle configurazioni delle porte dei Servizio di raccolta

1. In tutti i computer Sentinel v4.2 che eseguono Gestione servizi di raccolta, creare una directory in cui memorizzare tutti gli script e le configurazioni delle porte dei servizi di raccolta per il computer specifico.
2. Nella directory appena creata, creare un file di testo con l'elenco dei nomi di tutti i servizi di raccolta utilizzati dalla configurazione di una porta in Gestione servizi di raccolta. Utilizzare Generatore servizi di raccolta per determinare i servizi di raccolta utilizzati da Gestione servizi di raccolta. Se Gestione servizi di raccolta è in esecuzione in UNIX, sarà necessario utilizzare Generatore servizi di raccolta in un computer Windows (Generatore servizi di raccolta non è supportato in UNIX).
3. Copiare le directory seguenti nella directory appena creata:
 - %WORKBENCH_HOME%\Agents
 - %WORKBENCH_HOME%\Elements

Operazioni preliminari alla migrazione – Disinstallazione della versione v4.2

Disinstallazione della versione v4.2

1. nel computer che esegue Sentinel v4.2:
 - Chiudere tutte le console di Sentinel e tutte le istanze dei Generatori servizi di raccolta
 - Fare clic su *Start > Programmi > Sentinel > Disinstalla Sentinel 4.2.1.x*
2. Procedere con i prompt visualizzati fino alla finestra di disinstallazione del database. Selezionare tutte le funzioni.



NOTA: nell'esempio precedente non è visualizzata la funzionalità relativa al software di integrazione di terze parti. Se nel computer è installato software di terze parti, disinstallarlo.

Procedere con i prompt visualizzati fino alla finestra di disinstallazione del database.

3. Nella finestra di disinstallazione del database, selezionare *Non eseguire alcuna azione sul database*.

Please select which database uninstall action to perform:

- Delete the entire database instance.
- Delete only the database objects.
- Perform no action on the database.

4. Continuare la disinstallazione utilizzando le altre finestre visualizzate.

Operazioni preliminari alla migrazione – Installazione del database di Sentinel 5

Installazione del database di Sentinel 5

1. Verificare che la variabile di ambiente non faccia riferimento a 4.2. In caso affermativo, eliminarla. Le variabili di ambiente seguenti non devono essere presenti:
 - ESEC_HOME
 - ESEC_VERSION
 - ESEC_JAVA_HOME
 - ESEC_CONF_FILE
 - WORKBENCH_HOME
2. Verificare di aver raccolto le informazioni, eseguito i task e soddisfatto i requisiti specificati nella sezione relativa al database di Sentinel nel *capitolo 4: Installazione di Sentinel 5 per MS SQL*, nella sezione relativa alle operazioni preliminari all'installazione.
3. Inserire il CD di installazione di Sentinel nell'unità CD-ROM.

4. Passare al CD e fare doppio clic su *setup.bat*.

NOTA: l'installazione in modalità console non è supportata in Windows.

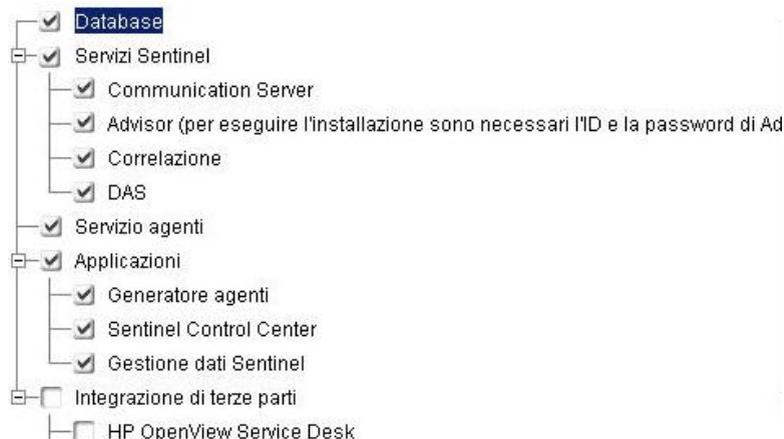
5. Nel riquadro successivo, fare clic sulla freccia giù e selezionare una delle lingue seguenti.
 - English (Inglese)
 - French (Francese)
 - German (Tedesco)
 - Italiano
 - Portoghese (Portoghese)
 - Spanish (Spagnolo)
6. Dopo aver letto la schermata introduttiva, fare clic su *Avanti*.
7. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
8. Accettare la directory di installazione di default o fare clic su *Sfoggia* per specificare un altro percorso di installazione. Fare clic su *Avanti*.

Fare clic su *Avanti* per installare "Sentinel 5" in questa cartella oppure fare clic su *Sfoggia* per installarlo in una cartella diversa.

Nome directory:

9. Per il tipo di installazione, selezionare *Personalizzata* (default). Fare clic su *Avanti*.
10. Per le funzioni da installare, deselezionare tutte le funzioni e selezionare *solo Database*. Fare clic su *Avanti*.

NOTA: verificare di aver deselezionato la funzione superiore "Servizi Sentinel". Verrà visualizzata in grigio con un segno di spunta bianco se è ancora selezionata ma tutte le relative funzioni secondarie sono state deselezionate.



11. Immettere il nome host (o IP) e il numero di porta (valore di default: 10012) per Communication Server. Fare clic su *Avanti*.
12. Selezionare *Microsoft SQL Server* come piattaforma di destinazione del database, quindi scegliere '*Crea un nuovo database con gli oggetti del database*'. Specificare inoltre la directory dei log di installazione del database (default: %ESEC_HOME%\logs\db). Accettare la *directory dei log di installazione del*

database di default o fare clic su *Sfoggia* per specificare un'ubicazione diversa. Fare clic su *Avanti*.

Selezionare la piattaforma server del database di destinazione:

Microsoft SQL Server 2000

- Creare un nuovo database con oggetti di database.
- Aggiungi oggetti di database a un database vuoto esistente.

Directory log di installazione database:

C:\Programmi\sentinel5.1.3.0\logs\db

Sfoggia

13. Immettere le informazioni di configurazione per SQL Server:

- (1) Nome host del database o indirizzo IP – Per default, sarà visualizzato il computer host locale, se SQL Server è installato in locale. Se la versione di SQL Server che si desidera installare non è visualizzata nell'elenco a discesa, selezionare '*Altro*' nell'elenco. Verrà visualizzata una casella di testo nella quale sarà possibile digitare il nome host. Il nome host specificato deve essere completo (ovvero 'sqlserver.sentinel.net' anziché solo 'sqlserver'). Se si è specificato il nome di un'istanza durante l'installazione di SQL Server, sarà necessario aggiungere '\<nome_istanza>' alla fine del nome host, dove <nome_istanza> è il nome assegnato all'istanza durante l'installazione di SQL Server.
- (2) Il nome da assegnare al nuovo database SQL Server. Oltre al database di cui si specifica il nome verrà creato un altro database con il nome <nome_db>_WF per l'utilizzo con iTRAC.

NOTA: è necessario assegnare al database un nome diverso da quello specificato per l'installazione della versione 4.2.

- (3) Porta di database (il valore di default è 1433)
- Per l'amministratore del database di sistema, selezionare:
 - (4) Autenticazione di Windows (viene utilizzato il nome utente con cui viene eseguito il programma di installazione)
 - (5) Autenticazione di SQL Server e immettere la password dell'utente sa

Microsoft SQL Server Configuration

Hostname[<InstanceName>]: (1)
<Hostname>[<InstanceName>]

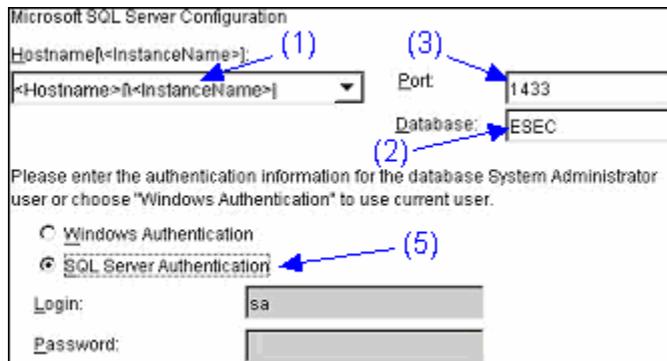
Port: (3) 1433

Database: (2) ESEC

Please enter the authentication information for the database System Administrator user or choose "Windows Authentication" to use current user.

Windows Authentication (4)
 SQL Server Authentication

Windows Authentication



Autenticazione di SQL Server

14. Immettere il percorso dei file di database seguenti:

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

- File di dati
- File di indice
- File di dati di riepilogo
- File di indice di riepilogo
- File di log

Specificare l'ubicazione di memorizzazione dei file di database seguenti:

Directory dati:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>
Directory indice:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>
Directory dati di riepilogo:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>
Directory indice di riepilogo:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>
Directory di log:	<input type="text" value="C:\Programmi\esecdata"/>	<input type="button" value="..."/>

15. Immettere le dimensioni del database:

- Standard (20.000 MB, capacità 30 giorni per 500.000 eventi al giorno)
- Grandi (400.000 MB, capacità 30 giorni a 10.000.000 di eventi al giorno)
- Personalizzate (specificare le dimensioni manualmente). Se si sceglie questa opzione, verranno chieste le informazioni seguenti:
 - (1) dimensioni del database in MB (10.000 – 2.000.000)
 - (2) dimensioni di ogni file di log in MB (100 – 100.000)
 - (3) dimensioni massime di ogni file di database in MB (2.000 – 100.000)

16. Per l'amministratore del database di Sentinel (DBA), selezionare:

- Autenticazione di SQL Server (esecdba), password e conferma password
- Autenticazione di Windows, immettere <nome dominio>\<nome utente>

NOTA: se si seleziona "Autenticazione di SQL Server", non sarà possibile modificare il nome di login di default.

Specificare le informazioni di autenticazione per l'utente (DBA) amministratore del database di Sentinel.

- Autenticazione di Windows
- Autenticazione di SQL Server

Login:

Autenticazione di Windows

Specificare le informazioni di autenticazione per l'utente (DBA) amministratore del database di Sentinel.

- Autenticazione di Windows
- Autenticazione di SQL Server

Login:

Password:

Conferma password:

Autenticazione di SQL Server

NOTA: per l'autenticazione di SQL, il programma di installazione procede solo se la password dell'utente esecdba corrisponde a quella dell'utente esecdba della versione 4.2.

17. Per l'utente del database dell'applicazione Sentinel. Selezionare:

- *Autenticazione di SQL Server* (esecapp), immettere password e conferma password
- *Autenticazione di Windows*, specificare <nome dominio>\<nome utente>, password e conferma password

NOTA: se si seleziona "*Autenticazione di SQL Server*", non sarà possibile modificare il nome di login di default.

Specificare le informazioni di autenticazione per l'utente di database dell'applicazione Sentinel.

- Autenticazione di Windows
- Autenticazione di SQL Server

Login:

Password:

Conferma password:

Autenticazione di Windows

Specificare le informazioni di autenticazione per l'utente di database dell'applicazione Sentinel.

Autenticazione di Windows

Autenticazione di SQL Server

Login:
Password:
Conferma password:

Autenticazione di SQL Server

18. Per l'utente amministratore di Sentinel. Selezionare:

- *Autenticazione di SQL*, immettere il nome utente per l'amministratore Sentinel (valore di default: esecadm), password e conferma password
- *Autenticazione di Windows*, immettere <nome dominio>\<nome utente>

NOTA: se si seleziona "*Autenticazione di SQL Server*", non sarà possibile modificare il nome di login di default.

Specificare le informazioni di autenticazione per l'utente amministratore di Sentinel.

Autenticazione di Windows

Autenticazione di SQL Server

Login:
Password:
Conferma password:

Autenticazione di Windows

Specificare le informazioni di autenticazione per l'utente amministratore di Sentinel.

Autenticazione di Windows

Autenticazione di SQL Server

Login:
Password:
Conferma password:

Autenticazione di SQL Server

19. Per l'utente di Sentinel Reporting. Selezionare:

NOTA: per effettuare l'Autenticazione di Windows in Sentinel Reporting è necessario che Crystal Enterprise Professional sia in esecuzione. Professional consente di creare diversi conti e mappature, in base alle proprie esigenze. Se si utilizza la versione Standard, selezionare *Autenticazione di SQL*.

- *Autenticazione di SQL Server* (esecrpt), immettere password e conferma password
- *Autenticazione di Windows*, immettere <nome dominio>\<nome utente>

NOTA: se si seleziona "*Autenticazione di SQL Server*", non sarà possibile modificare il nome di login di default.

Specificare le informazioni di autenticazione per l'utente dei rapporti di Sentinel.

- Autenticazione di Windows
 Autenticazione di SQL Server

Login:

Autenticazione di Windows

Specificare le informazioni di autenticazione per l'utente dei rapporti di Sentinel.

- Autenticazione di Windows
 Autenticazione di SQL Server

Login:

Password:

Conferma password:

Autenticazione di SQL Server

20. Fare clic su *Avanti* nella finestra di riepilogo dell'installazione del database.
21. Una volta completata l'installazione, verrà chiesto di riavviare il sistema. Fare clic su *Fine* per riavviare il sistema.

Migrazione

L'utility di migrazione dei dati eseguirà la migrazione solo degli elementi seguenti:

- Utenti e autorizzazioni assegnate
- Gestione filtri
- Opzioni di configurazione dei menu accessibili tramite il pulsante destro del mouse.
- Tag CV rinominati
- Configurazioni di partizioni e archivi
- I casi v4.2 vengono copiati in v5 come casi
- Casi ed eventi correlati ai casi

NOTA: l'utility di migrazione dei dati NON eseguirà la migrazione dei dati di eventi, ad eccezione dei dati di eventi associati ai casi. Sarà eseguita la migrazione solo dei dati di eventi associati ai casi.

NOTA: non è possibile visualizzare tramite Sentinel Control Center i dati degli eventi dei casi. I dati di eventi di casi possono essere visualizzati mediante Crystal Reporting o le query SQL.

Migrazione di dati per i database Sentinel 5 in cui l'utente amministratore del database di Sentinel dispone dell'autenticazione di Windows.

NOTA: questa procedura è valida per le installazioni del database di Sentinel 5 in cui l'amministratore del database di Sentinel (equivalente all'utente esecdba) dispone dell'Autenticazione di Windows. Con questa procedura viene aggiunto un utente esecdba con autenticazione SQL nel database di Sentinel 5 in modo da poter migrare i dati dalla versione 4.2 alla versione 5.

1. Eseguire il login come utente con diritti di amministrazione.
2. Avviare MS SQL Server Query Analyzer. Eseguire il login come utente sa o equivalente con autenticazione di Windows.
3. Fare clic su *File > Apri*. Individuare:

```
%ESEC_HOME%\utilities\db\scripts\ddl\mssql\Migration
```
4. Selezionare `import_add_esecdba.sql`.
5. Fare clic su *Apri*.
6. Fare clic su *Interrogazione > Esegui*.
7. Al termine dello script, uscire da Query Analyzer.

NOTA: dopo aver eseguito la migrazione dei dati, è possibile utilizzare MS SQL Server Enterprise Manager per eliminare l'utente esecdba con autenticazione SQL dal database di Sentinel 5.

Migrazione dati

1. Eseguire il login come utente con diritti di amministrazione.
2. Verificare nelle variabili di ambiente che java (versione 1.4.2) sia nel PATH. È possibile eseguire questa verifica mediante il comando seguente sulla riga di comando:

```
java -version
```

Se il comando indicato non riesce, individuare l'ubicazione di installazione di java nel sistema o scaricare e installare java. Aggiornare quindi la variabile di ambiente PATH perché includa l'eseguibile java. Se ad esempio java è installato nella directory:

```
C:\Programmi\sentinel5.1.3.0\Sun-1.4.2
```

Aggiungere quanto segue all'inizio della variabile di ambiente PATH:

```
C:\Programmi\sentinel5.1.3.0\Sun-1.4.2\bin;
```

3. Al prompt dei comandi, passare alla directory seguente del CD di installazione di Sentinel 5:

```
sentinel\dbsetup\bin
```

4. Eseguire il comando:

```
.\MigrateDb.bat
```
5. Verrà richiesto quanto segue:
 - nome host del database che esegue i database di Sentinel 4.2 e 5
 - nome del database di destinazione (del database Sentinel 5 al quale si sta eseguendo la migrazione)

- password esecdba (la password deve essere la stessa per l'utente esecdba nei database Sentinel v4.2 e v5)
- nome del database di origine (nome del database v4.2)
- directory di log (in cui saranno memorizzati i file di log di migrazione dei dati)
- opzione di migrazione:
 - (1) Impostazioni di sistema
 - (2) Casi
 - (3) entrambi
 - (4) fatto

NOTA: è necessario che la migrazione delle impostazioni di sistema venga eseguita correttamente prima di continuare con la migrazione dei casi.

NOTA: se la migrazione delle impostazioni di sistema ha esito negativo, disinstallare il database di Sentinel 5 selezionando l'opzione per *l'eliminazione dei soli oggetti di database*. Reinstallare quindi il database di Sentinel 5 selezionando l'opzione per *aggiungere oggetti a un database vuoto esistente*. Riprovare quindi ad eseguire la migrazione dei dati attenendosi alle istruzioni fornite.

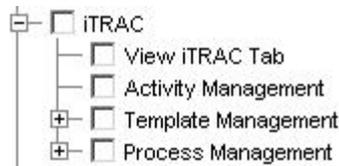
NOTA: se la migrazione dei casi non riesce, eseguirla di nuovo. L'utility di migrazione ricomincerà dal punto di errore. Non sono necessari altri task di pulizia.

NOTA: dopo aver eseguito la migrazione dei dati, è possibile eliminare l'utente esecdba con autenticazione SQL dal database Sentinel 5 utilizzando MS SQL Server, qualora fosse necessario aggiungerlo per l'utility di migrazione dei dati.

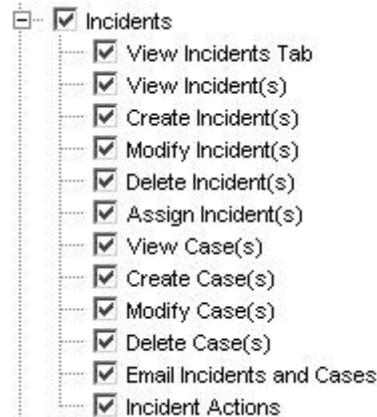
Operazioni successive alla migrazione – Installazione di Sentinel 5

In Sentinel 5, le funzioni seguenti sono nuove, diversi o sono state rimosse.

- iTRAC: nuova funzione. Le autorizzazioni utente associate sono:



- Casi – aggiunta di Amministrazione casi La funzione relativa a tutti i casi è stata rimossa. Le autorizzazioni utente associate sono:



Casi di Sentinel v4.2

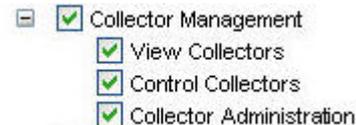


Casi di Sentinel v5

- Gestione servizi di raccolta – in v4.2 corrisponde a Wizard Monitoring. Alla *scheda 'View Wizards'* è stata sostituita la scheda *'Visualizza servizi di raccolta'*. *'Control Wizards and Collector'* sono stati sostituiti con *'Controllo servizi di raccolta'* e *'Amministrazione servizi di raccolta'*. Le autorizzazioni utente associate sono:



Sentinel v4.2 Wizard Monitoring



Gestione servizi di raccolta di Sentinel v5

- Amministrazione – Aggiunta di statistiche DAS, gestione della sessione utente e gestione dei ruoli iTRAC. *Le regole di correzione sono state ridenominate come Correlazione*. La funzione di configurazione degli eventi è stata spostata in Gestione dati Sentinel. *Configurazione* utente è stata ridenominata *Gestione utente*. Le autorizzazioni utente associate sono:



Sentinel v4.2 Administration

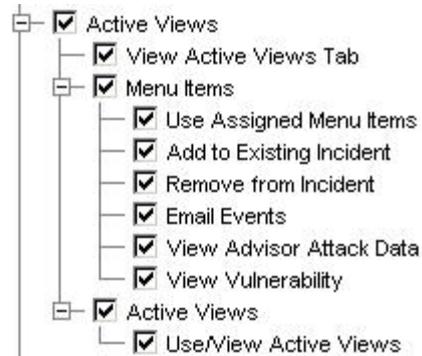


Amministrazione di Sentinel v5

- ActiveViews™ - Nella versione v4.2 era denominato Real Time. 'Summary Displays' è stato rinominato in *Active Views*. Le autorizzazioni utente associate sono:



Sentinel v4.2 Real Time



Sentinel v5 Active Views™

- La funzionalità di panoramica del sistema non è disponibile in Sentinel 5.

Installazione di Sentinel 5

1. Installare Sentinel 5, vedere il capitolo relativo all'installazione: *'Installazione di Sentinel 5 per Windows'*.
2. Installare il Service Pack di Sentinel più recente.
3. Se si desidera aggiungere nuove funzionalità agli utenti esistenti della versione v4.2, eseguire la procedura seguente:
 - a. Verificare che il *server Sentinel* sia in esecuzione.
 - b. Eseguire il login a Sentinel Control Center come utente con autorizzazioni di amministrazione/gestione utenti (ovvero *esecadm*).
 - c. In Sentinel Control Center fare clic sulla scheda Amministratore. Espandere Configurazione utente nel riquadro di navigazione o dalla barra di navigazione fare clic su *Amministrazione > Configurazione utente*.
 - d. Fare clic con il pulsante destro del mouse sull'utente al quale si desidera aggiungere la funzionalità (ovvero *esecadm*) e selezionare *Dettagli utente*. Fare clic sulla scheda *Autorizzazioni*.
 - e. Espandere *iTRAC* e assegnare le necessarie autorizzazioni.
 - f. Espandere *Casi* e assegnare *'Amministrazione casi* in base alle necessità.
 - g. Espandere *Gestione servizi di raccolta* e assegnare *'Amministrazione servizi di raccolta'* in base alle necessità.
 - h. Espandere *Amministrazione* e assegnare *Statistiche DAS*, *'Gestione sessioni utente* e *'Gestione ruoli iTRAC* in base alle necessità.
 - i. Fare clic sulla scheda *Ruoli* e assegnare il *ruolo di amministratore o workflow di analisi* in base alle necessità.
 - j. Fare clic su *OK*.
4. Se applicabile, importare le regole di correlazione. I gruppi di regole esportati da Sentinel 4.2 saranno visualizzati come cartelle delle regole se importati in Sentinel 5.
5. Copiare dal backup gli script dei servizi di raccolta e le configurazioni delle porte attenendosi alle istruzioni riportate nella sezione [Operazioni successive alla migrazione – Riconfigurazione degli script e delle configurazioni delle porte dei servizi di raccolta](#).

Operazioni successive alla migrazione – Riconfigurazione degli script e delle configurazioni delle porte dei servizi di raccolta.

In ogni computer in cui sono installati i servizi di raccolta di Sentinel 5 (Gestione servizi di raccolta), eseguire la procedura seguente per riapplicare gli script e le configurazioni delle porte dei servizi di raccolta utilizzati nell'installazione di Sentinel v4.2.

Per riapplicare gli script e le configurazioni delle porte dei servizi di raccolta

1. Arresto di Gestione servizi di raccolta in Windows.
2. Copiare i file seguenti dall'ubicazione in cui è stata archiviata una copia di backup della directory %WORKBENCH_HOME%\Agents relativa all'installazione di Sentinel v4.2 nella directory %WORKBENCH_HOME%\Agents dell'installazione attuale di Sentinel 5 (sovrascrivere i file se necessario):
 - localhost_portcfg.dat
 - localhost_snmpcfg.dat
3. Leggere il file di testo creato durante le operazioni preliminari alla migrazione con l'elenco dei servizi di raccolta utilizzati dall'installazione di Sentinel v4.2 Gestione servizi di raccolta nel computer. Per eseguire questo passaggio sarà necessario conoscere i nomi dei servizi di raccolta.
4. Copiare le directory i cui nomi equivalgono a quelli del servizio di raccolta nel file di testo dall'ubicazione in cui è stata archiviata la copia di backup della directory %WORKBENCH_HOME%\Elements relativa all'installazione di Sentinel v4.2 alla directory %WORKBENCH_HOME%\Elements dell'installazione attuale di Sentinel 5 (sovrascrivere i file e/o le directory se necessario).
5. Scaricare l'utility UpgradePortCfgFile dal sito Web del supporto tecnico di Sentinel ([download](#)).
6. Estrarre il file ZIP UpgradePortCfgFile.
7. Aprire un prompt dei comandi e passare alla directory dell'utility UpgradePortCfgFile estratta. Da questa directory, eseguire il comando:

```
.\UpgradePortCfgFile.bat
```
8. Avvio di *Gestione servizi di raccolta*

Operazioni successive alla migrazione – Configurazione di Sentinel 5 per Crystal Reporting

Se si desidera passare dall'esecuzione di Crystal Reporting per Sentinel v4.2 all'esecuzione di Crystal Reporting in Sentinel 5, è necessario eseguire le operazioni seguenti:

- Modificare le impostazioni ODBC correlate a Crystal Reporting affinché puntino al database di Sentinel ODBC.
- Importare i modelli di Crystal Report (inclusi i modelli di migrazione dei dati) dal Service Pack più recente.

Per ulteriori informazioni, vedere il capitolo relativo all'installazione di *Crystal Reports*.

Patch da v5.x.x a v5.1.3

Eseguire questa procedura su tutti i computer nei quali sono installati i componenti di Sentinel.

Applicazione di patch a Sentinel da v5.x.x a v5.1.3 quando l'amministratore del database di Sentinel (esecdba) esegue il login con autenticazione di SQL Server

Upgrade da v5.x.x a v5.1.3 per l'autenticazione di SQL Server

NOTA: se si esegue v5.1.1 sp1 o successive e si apportano modifiche al file `syslog.conf`, sarà necessario creare una copia del file. Il programma di installazione delle patch sovrascriverà il file `syslog.conf`. Dopo aver applicato la patch, modificare o sovrascrivere il nuovo file `syslog.conf` affinché corrisponda a quello originale.

1. Chiudere tutte le istanze aperte di *Sentinel Control Center*, *Gestione dati Sentinel* e *Generatore servizi di raccolta*.
2. Inserire il CD di installazione delle patch di Sentinel nell'unità CD-ROM.
3. Passare alla directory di patch appropriata.
4. Fare doppio clic su `setup.bat` in questa directory.

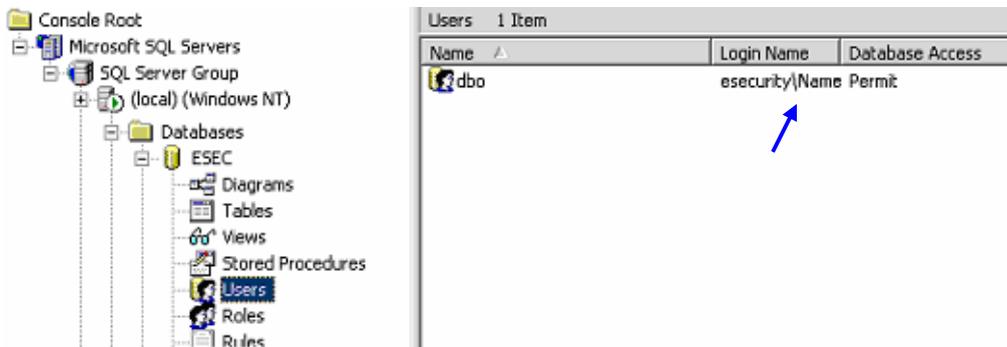
NOTA: l'installazione in modalità console non è attualmente supportata in Windows.

5. Fare clic su *Avanti* nella schermata introduttiva.
6. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
7. Fare clic su *Avanti* fino a visualizzare la finestra delle informazioni sul database.
8. Verificare che il tipo di database sia corretto. Selezionare l'ubicazione della directory dei log di installazione del database. Fare clic su *Avanti*.
9. Verificare che le informazioni per il server MS SQL siano corrette. Selezionare *Autenticazione di SQL Server*. Specificare il nome utente e la password `esecdba`. Fare clic su *Avanti*.
10. Fare clic su *Installa*. È possibile che venga richiesto di riavviare il computer. In caso contrario, riavviare servizi Sentinel (*Gestione servizi di raccolta*, *Sentinel e comunicazioni Sentinel*).

Applicazione di patch a Sentinel da v5.x.x a v5.1.3 quando l'amministratore del database di Sentinel (esecdba) esegue il login con autenticazione di Windows

Per l'autenticazione di Windows, la patch InstallShield non applicherà la patch del database. Il programma di installazione delle patch del database deve essere eseguito come utente 'esecdba' del dominio Windows per il database di Sentinel.

Se si sta eseguendo il programma di installazione delle patch nel computer in cui si è originariamente installato il componente Database, sarà necessario conoscere il nome utente e la password dell'utente amministratore del database di Sentinel (`esecdba`). È possibile determinare quale è l'utente `esecdba` cercando il nome di login per l'utente `dbo` del database di Sentinel mediante SQL Server Enterprise Manager, come segue.



Durante l'applicazione della patch, verrà visualizzato un messaggio che avvisa che la patch del database deve essere applicata mediante la riga di comando come illustrato di seguito.

Applicazione di patch da v5.x.x a v5.1.3 per l'autenticazione di Windows

NOTA: se si esegue v5.1.1 sp1 o successive e si apportano modifiche al file `syslog.conf`, sarà necessario creare una copia del file. Il programma di installazione delle patch sovrascriverà il file `syslog.conf`. Dopo aver applicato la patch, modificare o sovrascrivere il nuovo file `syslog.conf` affinché corrisponda a quello originale.

1. Chiudere tutte le istanze aperte di *Sentinel Control Center*, *Gestione dati Sentinel* e *Generatore servizi di raccolta*.
2. Inserire il CD di installazione delle patch di Sentinel nell'unità CD-ROM.
3. Passare alla directory di patch appropriata.
4. Fare doppio clic su `setup.bat` in questa directory.

NOTA: l'installazione in modalità console non è attualmente supportata in Windows.

5. Fare clic su *Avanti* nella schermata introduttiva.
6. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
7. Fare clic su *Avanti* fino a visualizzare la finestra delle informazioni sul database.
8. Verificare che il tipo e il nome di database siano corretti. Selezionare l'ubicazione della directory dei log di installazione del database. Fare clic su *Avanti*.

Verrà visualizzato il messaggio seguente. Leggerlo e fare clic su *OK* per continuare.



9. Verificare che le informazioni per il server MS SQL siano corrette. Selezione di *Autenticazione di Windows*. Immettere il nome utente e la password dell'utente dell'applicazione Sentinel. Fare clic su *Avanti*.

ATTENZIONE: per il computer del database, NON RIAVVIARE AL TERMINE DELL'INSTALLAZIONE.

10. Quando viene visualizzata la finestra di riepilogo, fare clic su *Installa*.
11. Sul computer del database, senza eseguire il riavvio, uscire da InstallShield.
12. Sul computer del database eseguire il login come utente 'esecdba' del dominio Windows se non lo si è già fatto.
13. Aprire un prompt dei comandi.
14. Verificare nelle variabili di ambiente che java (versione 1.4.2) sia nel PATH.
È possibile eseguire questa verifica mediante il comando seguente sulla riga di comando:

```
java -version
```

Se il comando indicato non riesce, individuare l'ubicazione di installazione di java nel sistema o scaricare e installare java. Aggiornare quindi la variabile di ambiente PATH perché includa l'eseguibile java. Se ad esempio java è installato nella directory:

```
C:\Programmi\sentinel5.1.3.0\Sun-1.4.2
```

Aggiungere quanto segue all'inizio della variabile di ambiente PATH:

```
C:\Programmi\sentinel5.1.3.0\Sun-1.4.2\bin;
```

15. Al prompt dei comandi, passare alla directory seguente del CD di installazione di Sentinel:

```
<Directory di patch>\sentinel\dbsetup\bin
```

16. Immettere il comando seguente:

```
.\PatchDb.bat
```

17. Al prompt digitare il nome host o l'indirizzo IP statico server SQL Server del database di Sentinel al quale si desidera applicare la patch.
18. Al prompt, digitare il nome del database di Sentinel SQL Server cui applicare la patch.
19. Al prompt, digitare option 1 per l'autenticazione di Windows. Lo script verificherà le informazioni specificate e inizierà ad applicare la patch al database.
20. Una volta completata l'applicazione della patch, riavviare i servizi.

Aggiornamento del connettore syslog

Se si utilizzano gli script del connettore syslog di una versione di Sentinel precedente alla 5.1.1.1, ovvero 5.0, 5.01.0, 5.1.0.0 o 5.1.1.0, è necessario iniziare a utilizzare gli script aggiornati del connettore inclusi nella patch. Per passare ai nuovi script del connettore syslog, installarli dopo aver rimosso quelli precedenti.

Il connettore syslog viene ora installato con script eseguibili su Windows e UNIX, nonché con file di configurazione migliorati. L'installazione del server proxy syslog come servizio è stata inoltre semplificata.

Per rimuovere il connettore syslog

1. Eseguire l'accesso come utente Administrator.
2. Eseguire `cd d/ %ESEC_HOME%\wizard\syslog`
3. Immettere:

```
.\syslog-server.bat remove
```

Per installare il connettore syslog

1. Eseguire l'accesso come utente Administrator.
2. Eseguire `cd d/ %ESEC_HOME\wizard\syslog`
3. Eseguire `.\syslog-server.bat install`
4. Se si apportano modifiche al file `syslog.conf` dell'installazione originale, sarà necessario modificare o sovrascrivere il nuovo file affinché rifletta quello originale. Il file `syslog.conf` si trova in:

`%ESEC_HOME%\wizard\syslog\config`

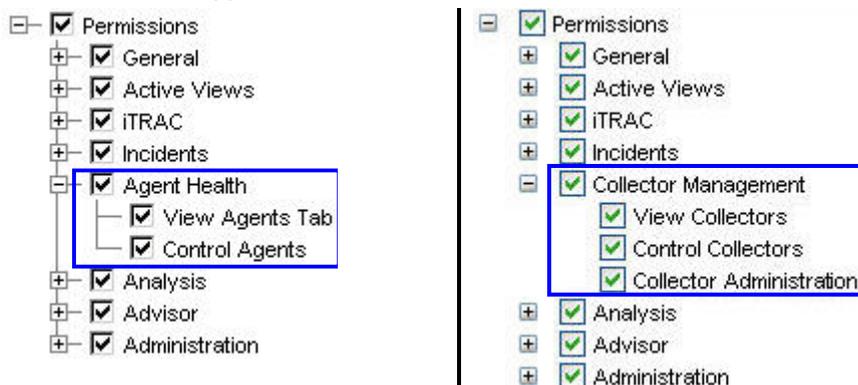
Aggiornamento delle autorizzazioni di gestione degli utenti per v5.0.x a v5.1.3

Quando si esegue l'upgrade da v5 o v5.0.1 a v5.1.3, Stato servizi di raccolta viene modificato in 'Gestione servizi di raccolta' con l'aggiunta di un'altra funzionalità di Amministrazione servizi di raccolta. Inoltre, è stata aggiunta la funzionalità di visualizzazione del server. Facoltativamente, è possibile concedere questa autorizzazione.

Aggiornamento delle autorizzazioni di gestione utenti

1. Eseguire il login a Sentinel Control Center come utente con autorizzazioni di amministrazione/gestione utenti.

In v5.1, Stato servizio di raccolta in Autorizzazioni è stato modificato in '*Gestione servizi di raccolta*' con l'aggiunta di un'altra autorizzazione.



Autorizzazioni utente di Sentinel v5.0 | Autorizzazioni utente di Sentinel v5.1

2. In Sentinel Control Center fare clic sulla scheda *Amministratore*. Espandere Configurazione utente nel riquadro di navigazione o dalla barra di navigazione fare clic su *Amministrazione > Configurazione utente*.
3. Fare clic con il pulsante destro del mouse su un utente Amministratore (ovvero `esecadm` o un altro utente amministratore) e scegliere *Dettagli utente*. Fare clic sulla scheda *Autorizzazioni*.
4. Espandere *Gestione servizi di raccolta* e assegnare '*Amministrazione servizi di raccolta*'. Fare clic su *OK*.

Aggiornamento delle autorizzazioni di visualizzazione server

Per utilizzare la schermata *Visualizzazione server* dopo l'installazione della patch, è necessario concedere l'apposita autorizzazione all'utente Sentinel che utilizza Gestione utenti. Gestione utenti si trova nella scheda Amministratore di Sentinel Control Center.

ALL GROUP BY SERVER HOSTNAME						
	Starts	AutoRestarts	StartTime	State	UpTime	Version
Processes Health						
localhost.localdomain						
Communication Server	1	0	01/20/2006 19:47:09 EST	Running	11:01s	5.1.1.1
Correlation Engine	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
DAS_Binary	2	0	01/20/2006 19:51:59 EST	Running	6:11s	5.1.1.1
DAS_Query	3	1	01/20/2006 19:48:04 EST	Running	10:06s	5.1.1.1
DAS_RT	2	0	01/20/2006 19:47:54 EST	Running	10:16s	5.1.1.1
DAS_JTRAC	2	0	01/20/2006 19:47:54 EST	Running	10:16s	5.1.1.1
Query Manager	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
RuleLg Checker	1	0	01/20/2006 19:48:14 EST	Running	9:56s	5.1.1.1
Sonic Lock Remover	0	0		NOT_INITIALIZED		5.1.1.1

Ready Refresh Options Refreshed At: Fri Jan 20 19:57:26 EST 2006

Server Crystal Reporting

Dopo aver eseguito l'upgrade a Sentinel v5.1.3, inclusa l'applicazione del Service Pack più recente, è necessario importare i rapporti dall'ultimo Service Pack. Per ulteriori informazioni, vedere il capitolo relativo a Crystal Reports nella Guida all'installazione.

Aggiornamento di e-mail Sentinel per l'autenticazione SMTP

Se nel sistema è necessaria l'autenticazione SMTP, sarà necessario aggiornare il file `execution.properties`. Il file si trova nel computer in cui è installato DAS. Nella directory `%ESEC_HOME%\sentinel\config`. Per configurare questo file, eseguire `mailconfig.bat` per modificare il file e `mailconfigtest.bat` per eseguire il test delle modifiche.

Per configurare il file `execution.properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
%ESEC_HOME%\sentinel\config
```

2. Eseguire il comando `mailconfig` come indicato di seguito:

```
./mailconfig.sh -host <Server SMTP> -from <indirizzo e-mail di origine> -user <utente autenticazione posta> -password
```

Esempio:

```
./mailconfig.sh -host 10.0.1.14 -from my_name@domain.com -user my_user_name -password
```

Dopo aver immesso questo comando verrà richiesto di specificare una nuova password.

```
Immettere la password:*****
```

```
Confermare la password:*****
```

NOTA: quando si utilizza l'opzione relativa alla password, deve trattarsi dell'ultimo argomento.

Per eseguire il test della configurazione del file `execution.properties`

1. Nel computer in cui è installato DAS, passare alla directory seguente:

```
%ESEC_HOME%\sentinel\config
```

2. Eseguire il comando `mailconfigtest` come indicato di seguito:

```
mailconfigtest.bat -to <indirizzo e-mail di destinazione>
```

Se l'invio del messaggio e-mail è riuscito correttamente, il messaggio sarà ricevuto all'indirizzo di destinazione e verrà visualizzato il messaggio seguente sullo schermo dell'utente.

```
Messaggio e-mail inviato.
```

Controllare la casella postale e-mail per confermare la ricezione del messaggio. La riga dell'oggetto e il contenuto dovrebbero essere:

```
Oggetto: Testing Sentinel mail property
```

```
This is a test for Sentinel mail property set up. If you  
see this message, your Sentinel mail property has been  
configured correctly to send emails
```

8

Patch per Oracle in Linux

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

In questo capitolo viene illustrato come applicare le patch da v5.1.1 a v5.1.3.

Patch da v5.1.1.1 a v5.1.3

Eseguire questa procedura su tutti i computer nei quali sono installati i componenti di Sentinel.

Se si sta eseguendo il programma di installazione delle patch dal computer in cui si è originariamente installato il componente Database, sarà necessario conoscere la password dell'utente amministratore del database di Sentinel (esecdba).

Upgrade da v5.1.1.1 a v5.1.3 per Linux

1. Eseguire il login come utente radice.

NOTA: se si apportano modifiche al file `syslog.conf` nell'installazione della versione 5.1.1.1, sarà necessario creare una copia del file. Il programma di installazione delle patch sovrascriverà il file `syslog.conf`. Dopo aver applicato la patch, modificare o sovrascrivere il nuovo file `syslog.conf` affinché corrisponda a quello originale.

2. Inserire e montare il CD di installazione delle patch di Sentinel.
3. Avviare il programma di installazione passando alla directory delle patch appropriata sul CD-ROM ed eseguendo il comando:

Per la modalità GUI:

```
./setup.sh
```

oppure

Per la modalità testuale ("headless"):

```
./setup.sh -console
```

4. Fare clic su *Avanti* nella schermata introduttiva.
5. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
6. Fare clic su *Avanti* fino a visualizzare la finestra delle informazioni sul database.
7. Verificare che il tipo di database sia corretto. Selezionare l'ubicazione della directory dei log di installazione del database. Fare clic su *Avanti*.
8. Verificare che le informazioni per il server Oracle siano corrette. Immettere la password `esecdba`. Seguire i prompt rimanenti del programma di installazione.

Aggiornamento del connettore syslog

Se si utilizzano gli script del connettore syslog di una versione di Sentinel precedente alla 5.1.1.1, ovvero 5.0, 5.01.0, 5.1.0.0 o 5.1.1.0, è necessario iniziare a utilizzare gli script aggiornati del connettore inclusi nella patch. Per passare ai nuovi script del connettore syslog, installarli dopo aver rimosso quelli precedenti.

Il connettore syslog viene ora installato con script eseguibili su Windows e UNIX, nonché con file di configurazione migliorati. L'installazione del server proxy syslog come servizio è stata inoltre semplificata.

Per rimuovere il connettore syslog

1. Eseguire il login come utente radice
2. Eseguire `cd $ESEC_HOME/wizard/syslog`
3. `./syslog-server.sh remove`

Per installare il connettore syslog

1. Eseguire il login come utente radice.
2. Eseguire `cd $ESEC_HOME/wizard/syslog`
3. Eseguire `./syslog-server.sh install`
4. Se si apportano modifiche al file `syslog.conf` dell'installazione originale, sarà necessario modificare o sovrascrivere il nuovo file affinché rifletta quello originale. Il file `syslog.conf` si trova in:

```
$ESEC_HOME/wizard/syslog/config
```

Server Crystal Reporting

Dopo aver eseguito l'upgrade a Sentinel 5.1.3, inclusa l'applicazione del Service Pack più recente, è necessario importare i rapporti dall'ultimo Service Pack. Per ulteriori informazioni, vedere il capitolo relativo a Crystal Reports nella Guida all'installazione.

Aggiornamento di e-mail Sentinel per l'autenticazione SMTP

Se nel sistema è necessaria l'autenticazione SMTP, sarà necessario aggiornare il file `execution.properties`. Il file si trova nel computer in cui è installato DAS. Nella directory `$ESEC_HOME/sentinel/config`. Per configurare questo file, eseguire `mailconfig.sh` per modificare il file e `mailconfigtest.sh` per eseguire il test delle modifiche.

Per configurare il file `execution.properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
$ESEC_HOME/sentinel/config
```

2. Eseguire il comando `mailconfig` come indicato di seguito:

```
./mailconfig.sh -host <server SMTP> -from <indirizzo  
e-mail di origine> -user <utente autenticazione  
posta> -password
```

Esempio:

```
./mailconfig.sh -host 192.0.2.14 -from  
my_name@domain.com -user my_user_name -password
```

Dopo aver immesso questo comando verrà richiesto di specificare una nuova password.

```
Immettere la password:*****
```

```
Confermare la password:*****
```

NOTA: quando si utilizza l'opzione relativa alla password, deve trattarsi dell'ultimo argomento.

Per eseguire il test della configurazione del file `execution.properties`

1. Nel computer in cui è installato DAS, eseguire il login come `esecadm` e passare alla directory seguente:

```
$ESEC_HOME/sentinel/config
```

2. Eseguire il comando `mailconfigtest` come indicato di seguito:

```
./mailconfigtest.sh -to <indirizzo e-mail di  
destinazione>
```

Se l'invio del messaggio e-mail è riuscito correttamente, il messaggio sarà ricevuto all'indirizzo di destinazione e verrà visualizzato il messaggio seguente sullo schermo dell'utente.

```
Messaggio e-mail inviato.
```

Controllare la casella postale e-mail per confermare la ricezione del messaggio. La riga dell'oggetto e il contenuto dovrebbero essere:

```
Oggetto: Testing Sentinel mail property
```

```
This is a test for Sentinel mail property set up.
```

```
If you see this message, your Sentinel mail property  
has been configured correctly to send emails
```


9

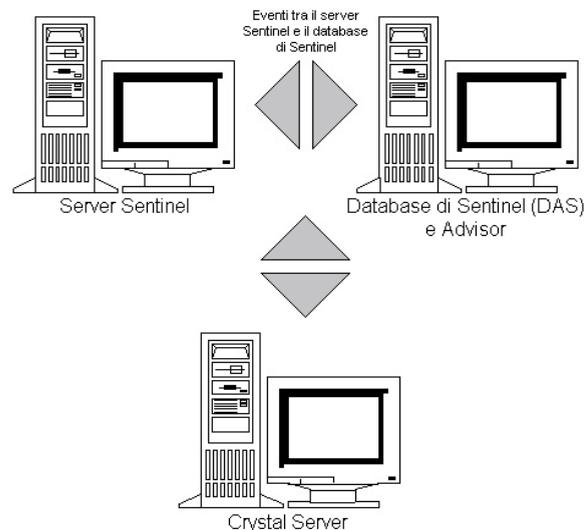
Crystal Reports per Windows e Solaris

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Crystal BusinessObjects Enterprise™ 11 è uno strumento per la generazione di rapporti.

In questo capitolo vengono trattate le operazioni relative all'installazione e alla configurazione del server Crystal Reports per Sentinel. È necessario eseguire l'installazione nell'ordine indicato.

- Installare Microsoft IIS e ASP.NET
- Installare MS SQL in base alla configurazione: come autenticazione di Windows o di SQL Server.
- Installare il server di Crystal
 - Configurazione di ODBC (Open Database Connectivity) per l'autenticazione di SQL oppure
 - Installazione e configurazione del software Oracle 9i Client
- Configurare inetmgr
- Applicare la patch di Crystal Reports
- Pubblicazione (Importazione) di Crystal Reports
- Impostazione di un conto 'utente denominato'
- Test della connettività al server Web
- Abilitazione dei primi 10 rapporti (facoltativo)
- Ottimizzazione della creazione di rapporti su eventi (consigliato)
- Configurazione di Sentinel sul server Crystal Enterprise Server



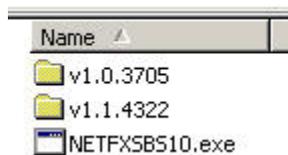
Panoramica

Il server Crystal Reports Server 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.

È necessario configurare un database CMS al di sopra di un database locale di MS SQL 2000. Il programma di installazione del server Crystal Reports consente di installare il database CMS nel database MSDE solo se non è installato alcun server MS SQL 2000 locale. Sentinel 5 non supporta le configurazioni MSDE.

Requisiti del sistema

- Windows® 2003 Server SP1, una partizione NTFS con IIS (Microsoft Internet Information Services) e NET.ASP. Sentinel 5 non supporta Crystal XI in Windows® 2000 Server.
- .NET Framework 1.1 (installato per default in Windows 2003. BusinessObjects Enterprise™ 11 non supporta .NET Framework 2.0). Per determinare la versione di .NET Framework installata sul computer in uso, spostarsi in %SystemRoot%\Microsoft.NET\Framework. La cartella con il numero maggiore non deve superare il valore v.1.1.xxxx. Ad esempio:

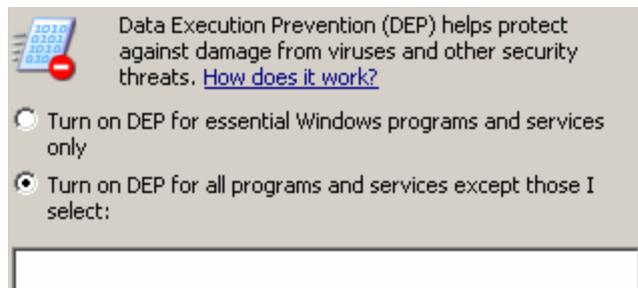


Requisiti di configurazione

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

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

Selezionare *Attiva protezione esecuzione programmi per tutti i programmi e i servizi tranne quelli selezionati*.



3. Se si prevede di utilizzare i rapporti di Sentinel utilizzando l'autenticazione di Windows NT, accertarsi che nel database Sentinel esista già il conto il conto di dominio Windows per l'utente dei rapporti Sentinel. Questa operazione viene eseguita durante l'installazione di Sentinel selezionando *Autenticazione di Windows* per l'impostazione del *metodo di autenticazione dell'utente dei rapporti Sentinel*, come nell'illustrazione seguente.

Specificare le informazioni di autenticazione per l'utente amministratore di Sentinel.

Autenticazione di Windows
 Autenticazione di SQL Server

Login:

4. Se si prevede di eseguire i rapporti di Sentinel utilizzando l'autenticazione di SQL Server (necessaria anche per le installazioni di Oracle Sentinel), accertarsi che nel database Sentinel esista già il login a SQL Server (esecrpt).
 - Nel caso del database MS SQL Sentinel eseguire questa operazione durante l'installazione di Sentinel per MS SQL. A questo scopo, selezionare *Autenticazione SQL Server* durante l'impostazione del "*Metodo di autenticazione per l'utente dei rapporti Sentinel Report*" come illustrato nell'immagine seguente.

Specificare le informazioni di autenticazione per l'utente dei rapporti di Sentinel.

Autenticazione di Windows
 Autenticazione di SQL Server

Login:

Password:

Conferma password:

- Nel caso del database Oracle Sentinel eseguire questa operazione durante l'installazione di Sentinel per Oracle. esecrpt presuppone l'utilizzo della stessa password di quella di esecadm.
5. Nel caso di Oracle 9i Client Release 2 (9.2.0.1.0) è necessario installare innanzitutto Oracle 9i Client Release 2 e quindi Crystal BusinessObjects Enterprise™ 11.
 6. Nel caso di MS SQL Server, installare innanzitutto MS SQL 2000 sp3a e quindi Crystal Reports Server 11.
 7. Risoluzione video di 1024 x 768 o superiore
 8. Installare Microsoft Internet Information Services (IIS) e NET.ASP

NOTA: Sentinel 5 non supporta MSDE. Installare innanzitutto MS SQL 2000 sp3a e quindi Crystal Reports Server 11.

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

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

Installazione di IIS e ASP.NET

1. In *Windows* passare a *Pannello di controllo > Installazione applicazioni*.
2. Nel pannello verticale sinistro fare clic su *Installazione componenti di Windows*.
3. Selezionare *Server applicazioni*.

<input checked="" type="checkbox"/>	Application Server	33.4 MB
-------------------------------------	--------------------	---------
4. Fare clic su *Dettagli*
5. Selezionare *ASP.NET e Internet Information Services (IIS)*.

<input checked="" type="checkbox"/>	ASP.NET	0.0 MB
<input checked="" type="checkbox"/>	Enable network COM+ access	0.0 MB
<input type="checkbox"/>	Enable network DTC access	0.0 MB
<input checked="" type="checkbox"/>	Internet Information Services (IIS)	26.9 MB
6. Fare clic su *OK*.
7. Fare clic su *Avanti*. È possibile che venga richiesto di inserire il CD di installazione di Windows.
8. Fare clic su *Finish (Fine)*.

Problemi noti

1. Installazione di Crystal Reports: vengono fornite due chiavi, una per Crystal Reports Server e l'altra per Crystal Reports Developer. Accertarsi che durante l'installazione di Crystal Reports Server venga utilizzata la relativa chiave.
2. 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 si danneggia. Per le procedure relative alla disinstallazione manuale di BusinessObjects Enterprise XI, visitare il sito Web di BusinessObjects all'indirizzo: <http://support.businessobjects.com/library/kbase/articles/c2017905.asp>.

NOTA: al momento della pubblicazione della presente documentazione l'URL indicato sopra risulta corretto.

3. Se durante la configurazione di .NET Administration Launchpad si modifica il livello di accesso da *'(Diritti ereditati)'* in *'Visualizza su richiesta'*, il processo di aggiornamento si arresterà. Attendere per circa trenta secondi. Il livello di accesso verrà aggiornato.

Uso di Crystal Reports

Per informazioni sull'uso di Crystal Reports per la generazione di rapporti in Sentinel, vedere la *Documentazione relativa a Crystal Reports* e la *Guida dell'utente di Sentinel*.

Panoramica relativa all'installazione

Panoramica relativa all'installazione di MS SQL 2000 Server con autenticazione di Windows

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

1. Installare Crystal Reports Server 11 – Se durante l’installazione dell’applicazione Sentinel 5 è stato selezionato *Autenticazione di Windows* per l’utente Sentinel Report, seguire il collegamento di [Installazione di Crystal Server per MS SQL 2000 Server con l'autenticazione di Windows](#).
2. [Configurare ODBC \(Open Database Connectivity\)](#)
3. [Eseguire la mappatura di Crystal Reports per l'uso con Sentinel](#)
4. [Applicare patch a Crystal Reports](#)
5. [Pubblicare rapporti](#)
6. [Impostare l'utente per un conto utente denominato](#)
7. [Importare i modelli di Crystal Reports](#)
8. Creare una pagina Web Crystal ([Configurazione di .NET Administration Launchpad](#))
9. [Configurare Sentinel per il server Crystal Enterprise](#)

Panoramica relativa all’installazione di MS SQL 2000 Server con autenticazione SQL Server

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

1. Installare Crystal Reports Server 11 – Se durante l’installazione dell’applicazione Sentinel 5 è stato selezionato *Autenticazione di SQL Server* per l’utente dei rapporti Sentinel, seguire il collegamento per [Installare Crystal Server per il server MS SQL 2000 con Autenticazione SQL o per Oracle](#).
2. [Configurare ODBC \(Open Database Connectivity\)](#)
3. [Eseguire la mappatura di Crystal Reports per l'uso con Sentinel](#)
4. [Importare i modelli di Crystal Reports](#)
5. Creare una pagina Web Crystal ([Configurazione di .NET Administration Launchpad](#))
6. [Configurare Sentinel per il server Crystal Enterprise](#)

Panoramica relativa all’installazione per Oracle

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

1. Installare Oracle 9i Client
2. Installare Crystal Reports Server 11 – seguire il collegamento di Installazione di Crystal [Installazione di Crystal Server per MS SQL 2000 Server con l'autenticazione di Windows](#).
3. [Configurare il driver nativo Oracle](#)
4. [Eseguire la mappatura di Crystal Reports per l'uso con Sentinel](#)
5. [Importare i modelli di Crystal Reports](#)
6. Creare una pagina Web Crystal ([Configurazione di .NET Administration Launchpad](#))
7. [Configurare Sentinel per il server Crystal Enterprise](#)

Installazione

In questa sezione è trattata la modalità di installazione di Crystal Server per:

- Database MS SQL 2000 Server Sentinel con autenticazione Windows.

- Database MS SQL 2000 Server Sentinel con autenticazione SQL Server
- Database Oracle Sentinel

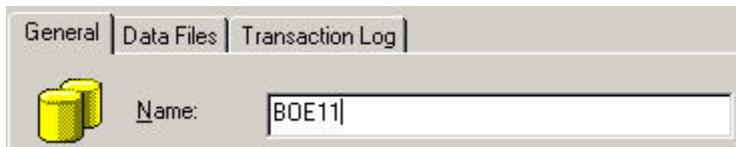
Installazione di Crystal Server per MS SQL 2000 Server con autenticazione Windows

Installazione di BOE XI Crystal Server con autenticazione di Windows

1. Installare MS SQL 2000 sp3a in modalità mista.
2. Avviare MS SQL Enterprise Manager.
3. Nel riquadro di navigazione espandere (locale)(Windows NT).
4. Evidenziare *Database* e fare clic su di esso con il pulsante destro del mouse, quindi scegliere *'Nuovo database...'*



5. Nel campo Nome della scheda Generale immettere 'BOE11', quindi fare clic su *OK*.



6. Uscire da MS SQL Enterprise Manager.
7. Inserire il CD di BOE XI Crystal Server nell'unità CD-ROM.
8. Se sul computer in uso la funzione di riproduzione automatica è disabilitata, eseguire *setup.exe*.
9. Nella finestra Selezionare client o Installazione server scegliere *Esegui installazione server*.

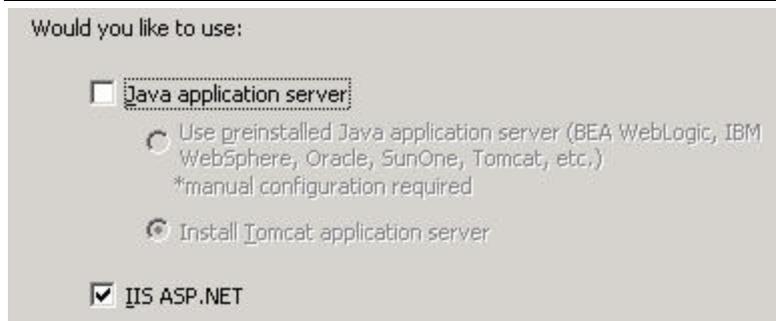


10. Per il tipo di installazione selezionare *Nuovo* e non *Installa MSDE o utilizza il server SQL Server locale*.

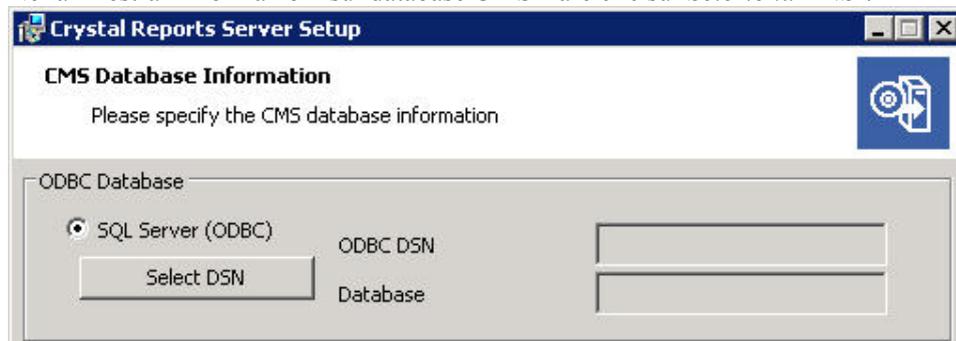


11. Nella finestra relativa al tipo di adattatore del componente Web, selezionare *IIS ASP.NET*.

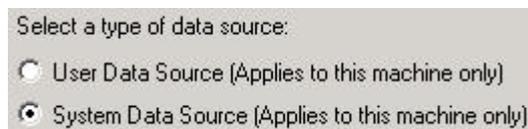
NOTA: se non si è installato IIS e ASP.NET mediante Pannello di *controllo > Installazione applicazioni > Installazione componenti di Windows*, *IIS ASP.NET* non sarà attivo.



12. Nella finestra 'Informazioni sul database CMS' fare clic su *Seleziona DNS*.

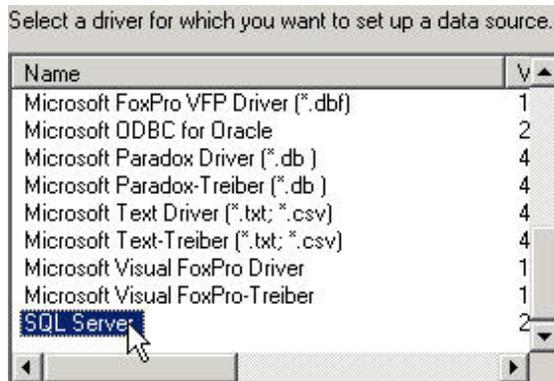


13. Fare clic sulla scheda *Origine dati computer*.
14. Fare clic su *Nuovo*.
15. Selezionare *Origine dati sistema*.

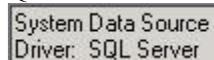


Fare clic su *Avanti*.

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

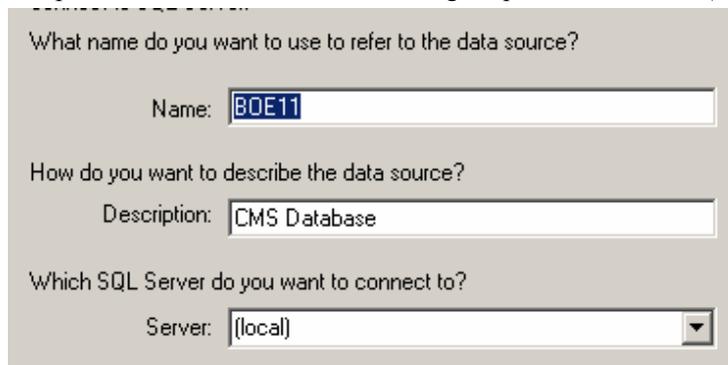


17. Quando viene visualizzata una nuova origine, fare clic su *Fine*.



18. Nella finestra '*...Nuova origine dati per un server SQL*', immettere:

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



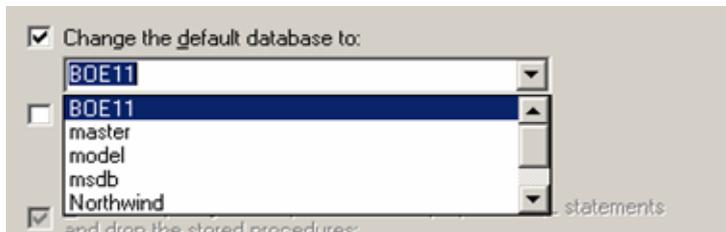
Fare clic su *Avanti*.

19. Se non è già stato fatto, selezionare '*con Windows NT*'. Fare clic su *Avanti*.



NOTA: l'ID login (non attivo) è il nome di accesso Windows.

20. Selezionare la casella di controllo *'Usa il seguente database predefinito:'*. Modificare il database di default impostandolo su *'BOE11'*. Fare clic su *Avanti*.

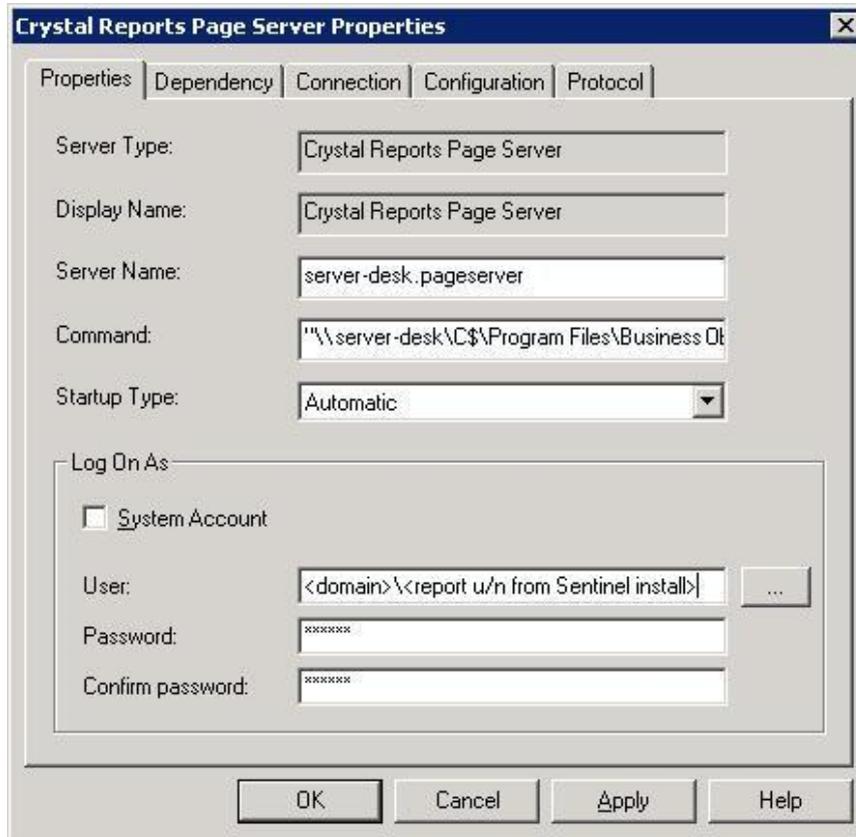


21. Nella finestra *'Crea nuova origine dati per un server SQL'*, fare clic su *Fine*.
22. Fare clic sul pulsante *'Verifica origine dati'*. L'operazione è completata. Fare clic su *OK*.
23. Nella finestra *Seleziona l'origine dei dati*, evidenziare *BOE11* e continuare a fare clic su *OK* finché non viene visualizzata la schermata *'Connessione SQL Server'*. Assicurarsi che la casella di controllo *'Usa connessione trusted'* sia selezionata. Fare clic su *OK*.



NOTA: l'ID login (non attivo) è il nome di accesso Windows.

24. Quando viene visualizzata la finestra di avviso fare clic su *OK*.
25. Quando viene visualizzata la finestra *'Informazioni sul database CMS'* fare clic su *'Avanti'*.
26. Fare clic su *Avanti* per continuare l'installazione.
27. 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.
 - a. Fare clic su *Start > Programmi > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager*.
 - b. Fare clic con il pulsante destro del mouse su *'Crystal Reports Page Server'* quindi scegliere *Interrompi*.
 - c. Fare di nuovo clic con il pulsante destro del mouse su *'Crystal Reports Page Server'* quindi scegliere *Proprietà*.
 - d. Deselezionare *"Log in come conto di sistema"*, quindi immettere il nome utente e la password del conto del dominio utente di Sentinel Report utilizzati per l'utente di Sentinel Report durante l'installazione dell'applicazione Sentinel 5. Fare clic su *OK*.



- e. Evidenziare Crystal Reports Page Server, quindi fare clic con il pulsante destro del mouse per avviarlo.

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

Questa procedura consente di impostare un'origine dati ODBC tra Crystal Reports in Windows e SQL Server. Questa operazione deve essere eseguita nel computer Crystal Server.

Configurazione di un'origine dati ODBC per l'autenticazione Windows

1. In Windows passare a *Pannello di controllo > Strumenti di amministrazione > Origine dati (ODBC)*.
2. Fare clic sulla scheda *DSN di sistema* e quindi sul pulsante *Aggiungi*.
3. Selezionare *SQL Server*. Fare clic su *Finish (Fine)*.
4. Verrà visualizzata una schermata che consente l'inserimento delle informazioni di configurazione del driver:
 - Nome origine dati, digitare *esecuritydb*
 - Campo Descrizione (facoltativo), digitare una descrizione
 - Campo Server, digitare il nome host o l'indirizzo IP del server Sentinel

Nome:

Immettere la descrizione desiderata per l'origine dati

Descrizione:

Specificare l'istanza di SQL Server a cui connettersi

Server:

Fare clic su *Avanti*.

5. Nella schermata successiva selezionare *Autenticazione di Windows*.

How should SQL Server verify the authenticity of the login ID?

With Windows NT authentication using the network login ID.

With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

Connect to SQL Server to obtain default settings for the additional configuration options.

Login ID:

Password:

NOTA: l'ID login (non attivo) è il nome di accesso Windows.

6. Nella schermata 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 *Finish (Fine)*.
8. Fare clic su *Verifica origine dati...* Dovrebbe essere attivata correttamente una connessione. Fare clic su *OK* fino al completamento della procedura.

Installazione di Crystal Server per MS SQL 2000 Server con autenticazione SQL

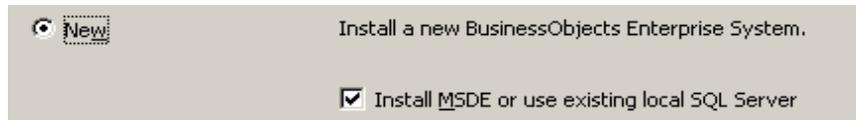
Installare Crystal Reports Server 11 accertandosi che le opzioni seguenti siano selezionate

- Perform Server Installation (Esegui installazione server)

Perform Client Installation.
Designer, Publishing Wizard, Business Views Manager, Import Wizard, and SDKs.

Perform Server Installation.
Installs all components, including the client SDK.

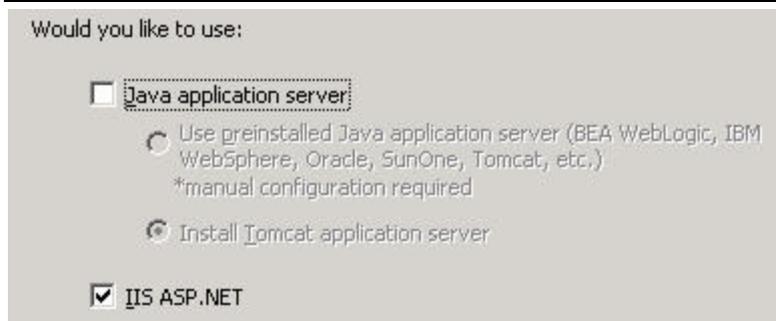
- Installare un nuovo sistema BusinessObjects Enterprise mediante l'opzione 'Install MSDE or use existing local SQL Server' (Installa MSDE o utilizza il server SQL Server locale).



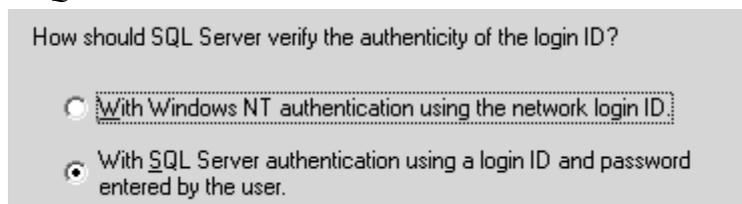
NOTA: Crystal Server e MS SQL Server 2000 devono trovarsi nello stesso computer.

- IIS ASP.NET.

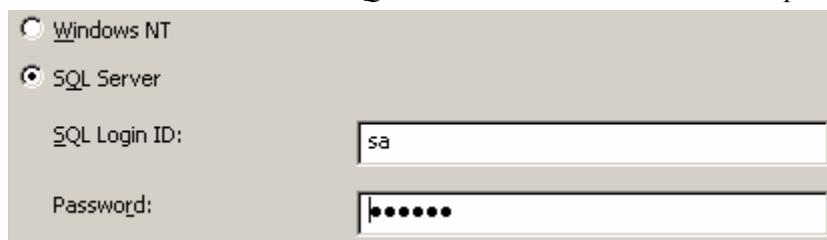
NOTA: se non si è installato IIS e ASP.NET mediante *Pannello di controllo > Installazione applicazioni > Installazione componenti di Windows*, IIS ASP.NET non sarà attivo.



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



- Selezionare *Autenticazione di SQL Server*. Immettere sa e la relativa password.



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

Questa procedura consente di impostare un'origine dati ODBC tra Crystal Reports in Windows e SQL Server. Questa operazione deve essere eseguita nel computer Crystal Server.

Configurazione di 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 quindi sul pulsante *Aggiungi*.
3. Selezionare *SQL Server*. Fare clic su *Finish (Fine)*.

4. Verrà visualizzata una schermata che consente l'inserimento delle informazioni di configurazione del driver:
 - Nome origine dati, digitare esecuritydb
 - Campo Descrizione (facoltativo), digitare una descrizione
 - Campo Server, digitare il nome host o l'indirizzo IP del server Sentinel

Fare clic su *Avanti*.

5. Nella schermata successiva selezionare *Autenticazione di SQL*. Immettere escript e la password come ID di login. Fare clic su *Avanti*.

6. Nella schermata 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 *Finish (Fine)*.
8. Fare clic su *Verifica origine dati...* Dovrebbe essere attivata correttamente una connessione. Fare clic su *OK* fino al completamento della procedura.

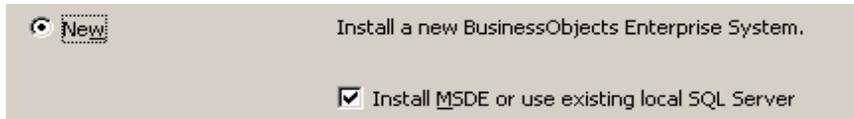
Installazione di Crystal Server per Oracle

Installare Crystal Reports Server 11 accertandosi che le opzioni seguenti siano selezionate

- Perform Server Installation (Esegui installazione server)



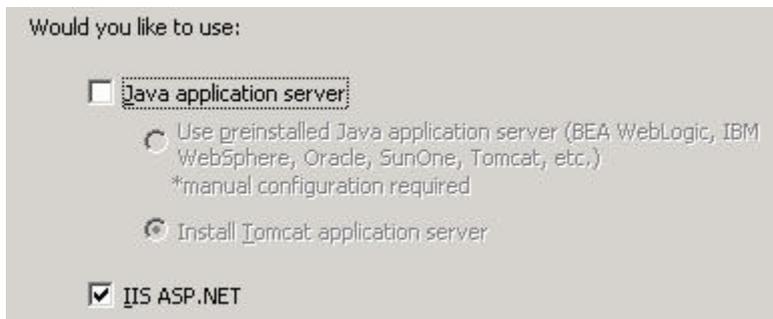
- Installare un nuovo sistema BusinessObjects Enterprise mediante l'opzione 'Install MSDE or use existing local SQL Server' (Installa MSDE o utilizza il server SQL Server locale).



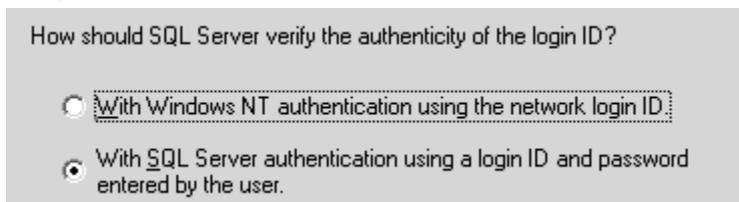
NOTA: Crystal Server e MS SQL Server 2000 devono trovarsi nello stesso computer.

- 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.



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



Crystal Reports supporta l'accesso diretto ai database Oracle 9. grazie al file di conversione crdb_oracle.dll. Questo file comunica con il driver del database Oracle 9, il quale interagisce direttamente con i client e i database Oracle recuperando i dati necessari per il rapporto.

NOTA: affinché Crystal Reports utilizzi i database Oracle 9, il software del client Oracle deve essere installato nel sistema e la relativa ubicazione deve trovarsi nella variabile di ambiente PATH.

Installazione e configurazione del software Oracle 9i Client

Durante l'installazione di Oracle 9i Client

- Accettare l'ubicazione di installazione di default.
- Non selezionare Esegui configurazione tipica

- Non selezionare Servizio di directory
- Selezionare Locale
- Nome del servizio TNS: ESEC
- Utente (facoltativo) esecrpt

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

Creazione di una configurazione Net Service name (Configurazione del driver nativo Oracle)

1. Selezionare *Oracle-OraHome92 > Strumenti di configurazione e migrazione > Net Manager*.
2. Nel riquadro di navigazione espandere Locale ed evidenziare Denominazione servizio.
3. Fare clic sul segno più a sinistra per aggiungere un nome di servizio.
4. Nella finestra Nome del servizio immettere un nome del servizio di rete.
 - Immettere ESECURITYDB
 Fare clic su *Avanti*.
5. Nella finestra Seleziona protocolli selezionare il protocollo di default:
 - TCP/IP (Internet Protocol)
 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
 - Selezionare la porta Oracle (di default 1521 durante l'installazione)
 Fare clic su *Avanti*.
7. Per identificare il database o il servizio:
 - Selezionare (*Oracle8i o versione successiva*), quindi immettere il nome del servizio, ovvero il nome dell'istanza Oracle.
 - Per il tipo di connessione selezionare *Impostazione predefinita database*.
 Fare clic su *Avanti*.
8. Nella finestra Test fare clic sul pulsante *'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 Connessione fare clic su *Modifica login*.
 - Immettere l'ID di Oracle Sentinel, ovvero esecrpt, e la password. Fare clic su *OK*.
 Se il test non riesce:
 - Eseguire il ping del Sentinel
 - Verificare che il nome host del server Sentinel sia incluso nel file hosts di Crystal Reports Server. Il file hosts è memorizzato in %SystemRoot%\system32\drivers\etc\.
10. Fare clic su *Finish (Fine)*.

Configurazione per tutte le autenticazioni e configurazioni

Mappatura di Crystal Reports per l'utilizzo con Sentinel

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

Configurazione di inetmgr

inetmgr

1. Copiare il file web.config da:

```
C:\Program Files\Business Objects\BusinessObjects  
Enterprise 11\Web Content
```

in c:\Inetpub\wwwroot.

2. Avviare Gestione servizio Internet 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 *Directory virtuale* fare clic sul pulsante *Configurazione...*
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	C:\Program Files\Business Objects\BusinessObjects Enterprise 11\win32_x86\cdzISAPI.dll

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*' fare clic con il pulsante destro del mouse quindi scegliere *Start*.

Applicazione di patch in Crystal Reports per l'utilizzo con Sentinel

Per visualizzare Crystal Reports dalla scheda Analisi di Sentinel Control Center, è necessario aggiornare diversi file di Crystal Enterprise per renderli compatibili con il browser incorporato in Sentinel.

Nella tabella seguente sono elencati tali file e viene descritto l'utilizzo di ognuno di essi.

File Name	descrizione
calendar.js	Consente di visualizzare un calendario popup quando si seleziona una data come parametro di un report.
calendar.html	

File Name	descrizione
grouptree.html	Consente di visualizzare il messaggio di caricamento in corso durante il caricamento dei rapporti.
exportframe.html	Consente di visualizzare la finestra nella quale è possibile esportare un rapporto per salvarlo o stamparlo.
exportIce.html	File utilizzato da Sentinel durante l'esportazione di un rapporto per il salvataggio o la stampa.
GetInfoStore.asp	File utilizzato per interrogare il server Crystal
GetReports.asp	File utilizzato da Sentinel Control Center per stabilire una connessione con Crystal Server e visualizzare l'elenco di rapporti.
GetReportURL.asp	File utilizzato per supportare i collegamenti ipertestuali tra i report.
helper_js.asp	File di chiamata utilizzato da GetInfoStore.asp.

Applicazione di patch a Crystal Reports

1. Nel CD-ROM del Sentinel Service Pack, passare a \content\reports\patch e copiare tutti i file *.html e *.js nell'ubicazione dei file del visualizzatore. Il percorso di default è:

```
C:\Program Files\Business Objects\BusinessObjects
Enterprise 11\Web Content\Enterprisell\viewer\en
```

2. Nel CD-ROM del Service Pack di Sentinel, passare a \content\reports\patch e copiare tutti i file *.asp e *.js in:

```
C:\inetpub\wwwroot
```

NOTA: è possibile che la cartella Web sia archiviata in un'unità o ubicazione diversa da quella sopra specificata.

Modelli di Crystal Reports

I modelli di Crystal Report vengono pubblicati mediante la Crystal Publishing Wizard.

È possibile scaricare i modelli di rapporto più recenti dal portale all'indirizzo <http://esecurity.custhelp.com/>.

NOTA: List of Attacks (Elenco attacchi) di CVE Report è un'intersezione di firme di attacchi dal feed di dati di Advisor e di vulnerabilità rilevate durante le scansioni.

NOTA: per eseguire uno qualsiasi dei primi dieci rapporti, è necessario che siano abilitati alcuni riepiloghi di aggregazioni e che EventFileRedirectService (nel processo DAS_Binary) sia impostato come attivo. Per informazioni su come abilitare i riepiloghi di aggregazione e attivare EventFileRedirectService vedere la sezione relativa all'[abilitazione dei primi 10 rapporti di Sentinel](#).

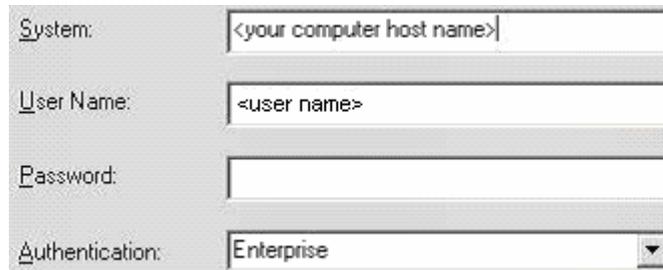
Publicazione di modelli di report mediante Crystal Publishing Wizard

Publicazione di modelli di Crystal Report

NOTA: se si pubblicano di nuovo i modelli di report, eliminare quelli importati in precedenza.

1. Fare clic su *Start > Tutti i programmi > BusinessObjects 11 > Crystal Reports Server > Publishing Wizard (Pubblicazione guidata)*.
2. Fare clic su *Avanti*.
3. Eseguire il login. System (Sistema) dovrebbe essere il nome del computer host e Authentication (Autenticazione) dovrebbe essere Enterprise. User Name (Nome utente) può essere Administrator (Amministratore). Per motivi di protezione, è consigliabile creare un nuovo utente diverso dall'amministratore. Immettere la password, quindi fare clic su *Next (Avanti)*.

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



4. Fare clic su *Add Folder (Aggiungi cartella)*.
5. Selezionare *'Include Subfolder' (Includi sottocartelle)*. Dal CD-ROM di Sentinel Service Pack passare a:

Per Crystal Reports (utenti MS SQL):

```
\content\reports\Crystal_v11\SQL-Server
```

Per Crystal Reports (utenti Oracle):

```
\content\reports\Crystal_v11\Oracle
```

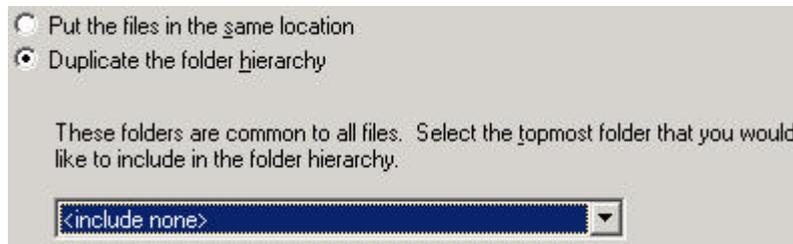
Fare clic su *OK*.

6. Fare clic su *Avanti*.
7. Nella finestra Specify Location (Specifica percorso), fare clic sul pulsante *New Folder (Nuova cartella)* posizionato nell'angolo superiore destro e creare una cartella denominata *eSecurity_Reports*. Fare clic su *Avanti*.



8. Selezionare:
 - Il pulsante di scelta *'Duplicate the folder hierarchy' (Duplica gerarchia cartelle)*.

- Fare clic sulla freccia giù e selezionare '<include none>' (*nessuno*)

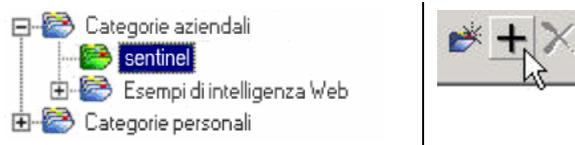


Fare clic su *Avanti*.

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

10. Nella finestra Specify Categories (Specifica categorie):

- selezionare il nome della categoria desiderata (ad esempio *sentinel*)
- evidenziare il nome e fare clic sul pulsante con il segno +



NOTA: dopo aver fatto clic su *Next (Avanti)* sotto la categoria sarà visualizzato solo il primo rapporto.

- Fare clic su *Next (Avanti)*.
11. 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*.
12. 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*.
13. 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*.
14. 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*.
15. Fare clic su *Next (Avanti)* per aggiungere gli oggetti.
16. Fare clic su *Avanti*.
17. Quando viene visualizzata la finestra con l'elenco degli oggetti pubblicati, fare clic su *Fine*.

Quando i modelli di Sentinel per Crystal Reports sono pubblicati sul server Crystal Enterprise, è necessario che i modelli siano memorizzati nella directory *e-Security_Reports*.

Impostazione di un account 'Named User' (Utente denominato)

Il codice di licenza fornito con Crystal Server è un codice di account 'Named User' (Utente denominato). L'account Guest (Ospite) deve essere modificato da 'Concurrent User' (Utente simultaneo) in 'Named User' (Utente denominato).

Impostazione del conto Guest (Ospite) come 'Named User' (Utente denominato)

1. Fare clic su Start > Tutti i programmi > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad.
2. Fare clic su *Central Management Console (Console di gestione centrale)*.
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. Fare clic su *Log On (Esegui login)*.
5. Nel riquadro Organize (Organizza) fare clic su *Users (Utenti)*.
6. Fare clic su *Guest (Ospite)*.
7. Modificare il tipo di connessione da *'Concurrent User' (Utente simultaneo)* in *'Named User' (Utente denominato)*.
8. Fare clic su *Aggiorna*.
9. Eseguire il logoff o chiudere la finestra, oppure passare alla sezione per la configurazione di *.NET Administration Launchpad*.

Configurazione di .NET Administration Launchpad

In questa procedura viene trattato come configurare .NET Administration Launchpad in modo da consentire la visualizzazione e la modifica dei rapporti.

Configurazione di .NET Administration Launchpad

1. Fare clic su Start > .NET Administration Launchpad (Fare clic su *Start > Tutti i programmi > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad*).
2. Fare clic su *Central Management Console (Console di gestione centrale)*.
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 (Esegui login)*.
4. Nel riquadro Organize (Organizza) fare clic su *Folders (Cartelle)*.
5. Fare clic su *eSecurity_Reports*.
6. Selezionare *tutto*.
7. Fare clic sulla scheda *Rights (Diritti)*.
8. Per Everyone, selezionare *'Visualizza su richiesta'* nel menu a discesa a destra nella sezione Livello di accesso. Fare clic su *Aggiorna*.

NOTA: se si modifica il livello di accesso da *'(Diritti ereditati)'* in *'Visualizza su richiesta'*, il processo di aggiornamento si arresterà. Attendere per circa trenta secondi. Il livello di accesso verrà aggiornato.

9. Eseguire il logoff e chiudere la finestra.

Test di Connessione server Web al Database.

Test della connessione tra il server Web e il database

1. Avviare .NET Administration Launchpad (Fare clic su *Start > Tutti i programmi > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad*).
2. Fare clic su *Central Management Console (Console di gestione centrale)*.

3. Immettere Administrator come nome utente. Immettere la password (per default, è vuota). Fare clic su *Log On (Esegui login)*.
4. Selezionare *Cartelle pubbliche > eSecurity_Reports > Eventi interni*.
5. Selezionare *'Dettagli visualizzazione colonna'*.
6. Fare clic su *Anteprima*.
7. In base al sistema in uso eseguire il login come esecrpt o come utente di Sentinel Report.
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

Test della connettività al server Web

1. Spostarsi su un computer diverso ma sulla stessa rete del server Web.
2. Digitare

```
http://<nome DNS o indirizzo IP del server
Web>/businessobjects/enterprisell/WebTools/adminlau
nch/default.aspx
```

3. Dovrebbe essere visualizzata una pagina Web di Crystal BusinessObjects.

Abilitazione dei primi 10 rapporti di Sentinel

Per abilitare i primi dieci rapporti di Sentinel è necessario eseguire le operazioni seguenti:

- Attivare Aggregazione
- Abilitare EventFileRedirectService

Attivazione Aggregazione

1. Avviare Gestione dati Sentinel.
2. Eseguire il login.
3. Fare clic sulla scheda *Rapporto dati*.
4. Abilitare i riepiloghi seguenti
 - EVT_DEST_SMRY_1
 - EVT_SEV_SMRY_1
 - EVT_SRC_SMRY_1

Fare clic sui pulsanti *'Disattivo'* nella colonna Stato finché diventano *'Attivo'*.

Summary Name	Time	Attributes	Source	Status
EventDestSummary	1 hour	CUST_ID,RSRC_ID...	TransformedEvent	Active
EventSevDestTxnmy...	1 hour	CUST_ID,DEST_Ev...	TransformedEvent	InActive
EventSevDestEvtSu...	1 hour	CUST_ID,DEST_Ev...	TransformedEvent	InActive
EventSevDestPortSu...	1 hour	SEV_DEST_PORT,C...	TransformedEvent	InActive
EventSevSummary	1 hour	CUST_ID,SEV,EVT...	TransformedEvent	Active
EventSrcSummary	1 hour	CUST_ID,RSRC_ID...	TransformedEvent	Active

Abilitazione di EventFileRedirectService

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

```
$ESEC_HOME/sentinel/config/das_binary.xml
```

In Windows:

```
%ESEC_HOME%\sentinel\config\das_binary.xml
```

2. Per EventFileRedirectService, modificare lo stato su on.

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

3. Riavviare il componente DAS eseguendo le operazioni seguenti:

In Windows:

```
Utilizzare Manager dei servizi per arrestare e quindi avviare il servizio "sentinel".
```

In Solaris:

```
$_ESEC_HOME/sentinel/scripts/sentinel.sh stop
```

```
Verificare che tutti i processi di Sentinel Server in esecuzione sul computer siano stato interrotti. A questo scopo utilizzare il comando 'ps -ef | grep $_ESEC_USER'. Se alcuni processi di Sentinel Server sono ancora in esecuzione, terminarli utilizzando il comando kill.
```

```
$_ESEC_HOME/sentinel/scripts/sentinel.sh start
```

Ottimizzare la creazione di rapporti sugli eventi

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 report sarà necessario riconfigurare Crystal Page Server. Esistono due metodi per eseguire questa operazione: mediante Central Configuration Manager oppure utilizzando la pagina Web di Crystal.

Riconfigurazione di Crystal Page Server mediante 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 *Interrompi*.
3. Fare clic con il pulsante destro del mouse su 'Crystal Reports Page Server' quindi scegliere *Proprietà*.
4. Nel campo Comando della scheda Proprietà, alla fine della riga di comando aggiungere `-maxDBResultRecords <valore maggiore di 20000 o 0 per disattivare il limite di default>`
5. Riavviare Crystal Page Server.

Riconfigurazione di Crystal Page Server mediante la pagina Web di Crystal

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

```
http://<nome DNS o indirizzo IP del server Web>/businessobjects/enterprisell/WebTools/adminlanch/default.aspx
```
2. Fare clic su *Central Management Console (Console di gestione centrale)*.

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 (Esegui login)*.
5. Fare clic su *Server*.
6. Fare clic su *<nome server>.pageserver*
7. 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), fare clic sul pulsante di scelta '*Unlimited records*' (*Senza limite di record*).
8. Fare clic su *Applica*.
9. Verrà visualizzato un prompt per il riavvio del page server. Fare clic su *OK*.
10. È possibile che vengano richiesti un nome di accesso e una password per accedere al manager dei servizi del sistema operativo.

Configurazione di Sentinel per l'integrazione con Crystal Enterprise Server

Dopo aver installato Crystal Enterprise Server è possibile configurare Sentinel Control Center in modo che acceda ai rapporti direttamente mediante Sentinel Control Center.

Configurazione di Sentinel per l'integrazione con Crystal Enterprise Server

1. Eseguire il login a Sentinel Control Center come utente con privilegi per la scheda Amministratore.
2. Nella scheda Amministratore, selezionare *Configurazione rapporti*.
3. Nel campo URL analisi, digitare:

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

NOTA: <nomehost_o_IP_del_server_web> deve essere sostituito con l'indirizzo IP o il nome host del server Crystal Enterprise Server.

NOTA: questo URL non funzionerà correttamente se APS è impostato sull'indirizzo IP. Deve corrispondere al nome host del server Crystal Server.

4. Fare clic sul pulsante *Aggiorna* accanto al campo URL analisi.
5. Se si è installato Advisor, nel campo URL Advisor digitare:

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

NOTA: <nomehost_o_IP_del_server_web> deve essere sostituito con l'indirizzo IP o il nome host del server Crystal Enterprise Server.

NOTA: questo URL non funzionerà correttamente se APS è impostato sull'indirizzo IP. Deve corrispondere al nome host del server Crystal Server.

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 Report nelle schede Analisi e Advisor (se Advisor è installato) dovrebbero ora essere visualizzati nella barra di spostamento.

10

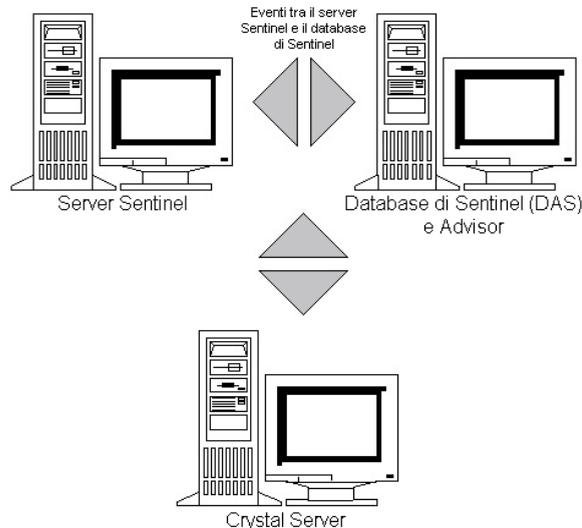
Crystal Reports per Linux

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Crystal BusinessObjects Enterprise™ 11 è uno degli strumenti per la generazione di rapporti con Sentinel.

In questo capitolo sono illustrate le operazioni relative all'installazione e alla configurazione di Crystal Reports Server per Sentinel in Linux. È necessario eseguire l'installazione nell'ordine indicato.

- Operazioni preliminari e successive all'installazione di Crystal BusinessObjects Enterprise™ 11
- Applicare la patch di Crystal Reports
- Pubblicazione (Importazione) di Crystal Reports
- Impostazione di un conto 'utente denominato'
- Test della connettività al server Web
- Abilitazione dei primi dieci rapporti (facoltativo)
- Ottimizzazione della creazione di rapporti su eventi (consigliato)
- Configurazione di Sentinel sul server Crystal Enterprise Server



Uso di Crystal Reports

Per informazioni sull'uso di Crystal Reports per la generazione di rapporti in Sentinel, vedere la *Documentazione relativa a Crystal Reports* e la *Guida dell'utente di Sentinel*.

Configurazione

- Versioni di Linux:
 - SuSE Linux Enterprise Server 9 (SLES 9)
 - Red Hat Enterprise Linux 3 Update 5 ES (x86)
- BusinessObjects Enterprise XI Server installato
- Per Oracle - Oracle 9i Client Release 2 (9.2.0.1.0)

Installazione

Operazioni preliminari all'installazione di Crystal BusinessObjects Enterprise™ 11

Operazioni preliminari all'installazione di Crystal BusinessObjects Enterprise

1. Se il database di Sentinel non si trova nello stesso computer di Crystal Server, sarà necessario installare il software Oracle Client nel computer Crystal Server. Questa operazione non è necessaria se il database di Sentinel si trova nello stesso computer di Crystal Server perché in questo caso il software Oracle necessario è già stato installato con il software del database Oracle necessario per il database di Sentinel.
2. Eseguire il login al computer Crystal Server come utente radice.
3. Creare il gruppo bobje

```
groupadd bobje
```

4. Creare l'utente 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_xi
```

6. Modificare la proprietà della directory del software Crystal (in modo ricorsivo) in crystal/bobje:

```
chown -R crystal:bobje /opt/crystal_xi
```

7. Passare all'utente crystal:

```
su - crystal
```

8. 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/9.2, aprire il file ~crystal/.bash_profile e aggiungere la riga seguente alla fine del file:

```
export ORACLE_HOME=/opt/oracle/product/9.2
```

9. 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 (al disotto della riga in cui è impostata la variabile di ambiente `ORACLE_HOME`):

```
export
LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

10. 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 Crystal Server eseguire le operazioni seguenti:
 - a. Eseguire il login come utente Oracle.
 - b. Passare alla directory `$ORACLE_HOME/network/admin`
 - c. Eseguire il backup del file `tnsnames.ora`.
 - d. Aprire il file `tnsnames.ora` per la modifica.
 - e. Se il database di Sentinel si trova nello stesso computer di Crystal 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)
  )
)
```

- f. Se il database di Sentinel non si trova nello stesso computer di Crystal Server, aprire il file `tnsnames.ora` nel computer del database di Sentinel per individuare la voce indicata sopra.
- g. Fare una copia della voce e incollarla alla fine del file `tnsnames.ora` nel computer di Crystal Server. La parte relativa al nome del servizio della voce 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)
  )
)
```

- h. Verificare che la parte HOST della voce sia corretta (verificare cioè che non sia impostata su localhost se Crystal Server e il database di Sentinel sono su computer diversi).
- i. Salvare le modifiche al file tnsnames.ora.
- j. Eseguire il comando seguente per verificare che il nome del servizio esecuritydb sia configurato correttamente:


```
tnsping esecuritydb
```
- k. Se il comando viene eseguito correttamente, dovrebbe essere visualizzato un messaggio relativo alla riuscita della connessione.

Installazione di Crystal BusinessObjects Enterprise™ 11

Installazione di Crystal BusinessObjects Enterprise

1. Eseguire il login come utente crystal.
2. Passare alla directory DISK_1 del programma di installazione di Crystal.
3. Eseguire:


```
./install
```
4. Selezionare Language (Lingua): *English (Inglese)*
5. Selezionare *New Installation (Nuova installazione)*
6. Accettare le condizioni del Contratto di licenza
7. Immettere il codice prodotto
8. Specificare la directory di installazione:


```
/opt/crystal_xi
```
9. Selezionare: *User install (Installazione utente)*
10. Selezionare: *New Install (Nuova installazione)*
11. Selezionare: *Install MySQL (Installa MySQL)*
12. Immettere le informazioni di configurazione per MySQL:
 - a. Utilizzare la porta di default 3306
 - b. Admin password (Password amministratore)
13. Immettere altre informazioni di configurazione per MySQL:
 - a. Default DB Name (Nome DB di default): BOE11
 - b. User ID (ID utente): mysqladm
 - c. Password
14. Immettere altre informazioni di configurazione per MySQL:
 - a. Local Name Server (Server dei nomi locale): <nome host del computer locale>
 - b. Default CMS Port Number (Numero di porta CMS di default): 6400
15. Selezionare: *Install Tomcat (Installa Tomcat)*
16. Immettere le informazioni di configurazione di Tomcat:
 - a. Default Receive HTTP requests port (Porta di default ricezione richieste HTTP): 8080
 - b. Default Redirect jsp requests port (Porta di default reindirizzamento richieste JSP): 8443
 - c. Default Shutdown Hook port (Porta di default aggancio arresto): 8005
17. Premere *Invio* per avviare l'installazione

Applicazione di patch in Crystal Reports per l'utilizzo con Sentinel

Per visualizzare Crystal Reports dalla scheda Analisi di Sentinel Control Center, è necessario aggiornare diversi file di Crystal Enterprise per renderli compatibili con il browser incorporato in Sentinel.

Nella tabella seguente sono elencati tali file e viene descritto l'utilizzo di ognuno di essi.

<i>Nome file</i>	<i>Descrizione</i>
calendar.js calendar.html	Consente di visualizzare un calendario popup quando si seleziona una data come parametro di un report.
grouptree.html	Consente di visualizzare il messaggio di caricamento in corso durante il caricamento dei rapporti.
exportframe.html	Consente di visualizzare la finestra nella quale è possibile esportare un rapporto per salvarlo o stamparlo.
exportIce.html	File utilizzato da Sentinel durante l'esportazione di un rapporto per il salvataggio o la stampa.
GetReports.jsp	File utilizzato da Sentinel Control Center per stabilire una connessione con Crystal Server e visualizzare l'elenco di rapporti.

Applicazione di patch in Crystal Reports

1. ORA DISPONIBILE SOLO DAL SERVICE PACK. Nel CD-ROM del Sentinel Service Pack, passare a \content\reports\patch e copiare tutti i file *.html e *.js nell'ubicazione dei file del visualizzatore. Il percorso di default è:

```
/opt/crystal_xi/bobje/webcontent/enterprise11/viewer/  
en/
```

2. Nel CD-ROM del Service Pack di Sentinel, passare a \content\reports\patch e copiare tutti i file *.jsp in:

```
/opt/crystal_xi/bobje/tomcat/webapps/esec-script/
```

NOTA: creare una cartella denominata **esec-script**

```
Copy all *.jar files
```

Da:

```
/opt/crystal_xi/bobje/tomcat/webapps/jsfadmin/WEB-  
INF/lib/
```

In:

```
/opt/crystal_xi/bobje/tomcat/webapps/esec-  
script/WEB-INF/lib
```

NOTA: creare una struttura di cartelle **WEB-INF/lib**

Publicazione di modelli di Crystal Reports

Questi modelli di rapporti sono creati da Novell per l'uso nelle schede Analisi e Advisor di Sentinel Control Center.

Sono disponibili due metodi per la pubblicazione di rapporti.

- Crystal Publishing Wizard (Pubblicazione guidata Crystal)
- Crystal Reports Central Management Console (Console di gestione centrale di Crystal Reports)

Sono inoltre forniti rapporti di esempio in formato PDF.

NOTA: List of Attacks (Elenco attacchi) di CVE Report è un'intersezione di firme di attacchi dal feed di dati di Advisor e di vulnerabilità rilevate durante le scansioni.

NOTA: per eseguire uno qualsiasi dei primi dieci rapporti, è necessario che l'aggregazione sia abilitata e che in DAS_Binary.xml [EventFileRedirectService](#) sia impostato come attivo. Per informazioni su come abilitare l'aggregazione, vedere il *capitolo 10 "Gestione dati Sentinel" nella Guida dell'utente di Sentinel*, nella sezione relativa alla scheda Rapporto dati o passare alla sezione [Abilitazione dei primi 10 rapporti Sentinel](#).

Publicazione di modelli di rapporti - Crystal Publishing Wizard (Pubblicazione guidata Crystal)

NOTA: per eseguire Crystal Publishing Wizard (Pubblicazione guidata Crystal) è necessaria una piattaforma Windows.

Importazione dei 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 11 > Crystal Reports Server > Publishing Wizard (Pubblicazione guidata)*.
2. Fare clic su *Avanti*.
3. Eseguire il login. System (Sistema) dovrebbe essere il nome del computer host e Authentication (Autenticazione) dovrebbe essere Enterprise. User Name (Nome utente) può essere Administrator (Amministratore). Per motivi di sicurezza, è opportuno utilizzare un utente diverso da Administrator (Amministratore). Immettere la password, quindi fare clic su *Next (Avanti)*.

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



The image shows a screenshot of the Crystal Publishing Wizard login dialog box. It has a light gray background and contains four input fields arranged vertically. The first field is labeled 'System:' and contains the placeholder text '<your computer host name>'. The second field is labeled 'User Name:' and contains the placeholder text '<user name>'. The third field is labeled 'Password:' and is currently empty. The fourth field is labeled 'Authentication:' and is a dropdown menu with 'Enterprise' selected. The dialog box has a standard Windows-style border and a close button in the top right corner.

4. Fare clic su *Add Folder (Aggiungi cartella)*.
5. Selezionare la casella di controllo *'Include Subfolder' (Includi sottocartelle)*.
Dal CD-ROM di Sentinel Service Pack passare a:

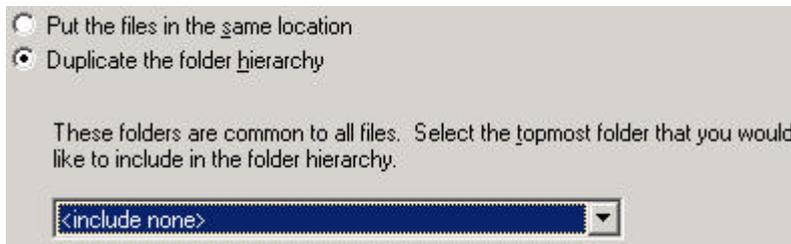
```
content\reports\Crystal_v11\Oracle
```

Fare clic su *OK*.

6. Fare clic su *Avanti*.
7. Nella finestra *Specify Location (Specifica percorso)*, fare clic sul pulsante *New Folder (Nuova cartella)* posizionato nell'angolo superiore destro e creare una cartella denominata *eSecurity_Reports*. Click *Next*.

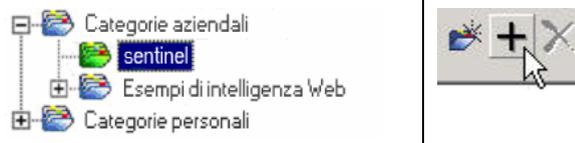


8. Selezionare:
 - Il pulsante di scelta *'Duplicate the folder hierarchy' (Duplica gerarchia cartelle)*.
 - Fare clic sulla freccia giù e selezionare *'<include none>' (nessuno)*



Fare clic su *Avanti*.

9. Nella finestra *Confirm Location (Conferma percorso)* fare clic su *Next (Avanti)*.
10. Nella finestra *Specify Categories (Specifica categorie)*:
 - selezionare il nome della categoria desiderata (ad esempio sentinel)
 - evidenziare il nome e fare clic sul pulsante con il segno +



NOTA: Dopo aver fatto clic su *Next (Avanti)* sotto la categoria sarà visualizzato solo il primo rapporto.

- Fare clic su *Next (Avanti)*.
11. 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*.
 12. 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*.

13. 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*.
14. 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*.
15. Fare clic su *Next (Avanti)* per aggiungere gli oggetti.
16. Fare clic su *Avanti*.
17. Fare clic su *Fine*.

Quando i modelli di Sentinel per Crystal Reports sono pubblicati sul server Crystal Enterprise, è necessario che i modelli siano memorizzati nella directory e-Security_Reports.

Publicazione di modelli di rapporti – Central Management Console (Console di gestione centrale)

Quando si pubblicano rapporti mediante Central Management Console (Console di gestione centrale), non è possibile pubblicare i rapporti in batch come quando si utilizza la pubblicazione guidata di Windows.

Importazione dei modelli di Crystal Reports

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


```
http://<nomehost_o_IP_del_server_web>:<server_web_port
      a_default_8080>/businessobjects/enterprisell/adminl
      aunch
```
2. Fare clic su *Central Management Console (Console di gestione centrale)*.
3. Eseguire il login al server Crystal Server.
4. Nel riquadro Organize (Organizza) fare clic su *Folders (Cartelle)*.
5. Nell'angolo superiore destro fare clic su *'new Folder (Nuova cartella)*.
6. Creare una cartella denominata *eSecurity_Reports*. Fare clic su *OK*.
7. Fare clic su *eSecurity_Reports*.
8. Fare clic sulla scheda Subfolders (Sottocartelle) e creare le sottocartelle seguenti.
 - Advisor_Vulnerability
 - Incident Management
 - Internal Events
 - Security Events
 - Top 10
9. Fare clic su *Home*.
10. Fare clic su *'Objects' (Oggetti)*.
11. Fare clic su *'New Object' (Nuovo oggetto)*.
12. Sul lato sinistro della pagina, evidenziare *Report (Rapporto)*.
13. Fare clic sul pulsante *Browse (Sfogliare)* e passare al CD del Service Pack di Sentinel:


```
content\reports\Crystal_v11\Oracle
```

Fare clic su una cartella e selezionare un rapporto.

14. Evidenziare *eSecurity_Reports*, fare clic su *'Show Subfolders'* (*Mostra sottocartelle*).
15. Selezionare la cartella appropriata per il rapporto e fare clic su *'Show Subfolders'* (*Mostra sottocartelle*).
16. Fare clic su *OK*.
17. Fare clic su *Update* (*Aggiorna*).
18. Fare clic sulla scheda *Reports* (*Rapporti*) e continuare ad aggiungere *rapporti*.
19. Per aggiungere i rapporti rimanenti a una cartella diversa, fare clic su *Folders* (*Cartelle*) nell'angolo superiore sinistro e ripetere i punti da 14 a 17.

Uso del server Web di Crystal Server XI

Crystal Server XI su Linux 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://<nomehost_o_IP_del_server_web>:<server_web_porta_
default_8080>/businessobjects/enterprise11/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_de
fault_8080>/businessobjects/enterprise11
```

Test della connettività al server Web

Test della connettività al server Web

1. Spostarsi su un computer diverso ma sulla stessa rete del server Web.
2. Digitare

```
http://<nomehost_o_IP_del_server_web>:<server_web_port
a_default_8080>/businessobjects/enterprise11/adminl
aunch
```

3. Dovrebbe essere visualizzata una pagina Web di Crystal BusinessObjects.

Impostazione di un account 'Named User' (Utente denominato)

Il codice di licenza fornito con Crystal Server è un codice di account 'Named User' (Utente denominato). L'account Guest (Ospite) deve essere modificato da 'Concurrent User' (Utente simultaneo) in 'Named User' (Utente denominato).

Impostazione del conto Guest (Ospite) come 'Named User' (Utente denominato)

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

```
http://<nomehost_o_IP_del_server_web>:<server_web_port
a_default_8080>/businessobjects/enterprise11/adminl
aunch
```

2. Fare clic su *Central Management Console*.

3. System (Sistema) dovrebbe essere il nome del computer host e Authentication (Autenticazione) dovrebbe essere Enterprise. In caso contrario, selezionare Enterprise.
4. Nel riquadro Organize (Organizza) fare clic su *Users (Utenti)*.
5. Fare clic su Guest (Ospite).
6. Modificare il tipo di connessione da *'Concurrent User' (Utente simultaneo)* in *'Named User' (Utente denominato)*.
7. Fare clic su *Update (Aggiorna)*.
8. Eseguire il logoff e chiudere la finestra.

Configurazione dei rapporti

In questa procedura viene illustrato come configurare Administration Launchpad in modo da consentire la visualizzazione e la modifica dei rapporti.

Configurazione di Administration Launchpad

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


```
http://<nomehost_o_IP_del_server_web>:<server_web_port
a_default_8080>/businessobjects/enterprise11/adminl
aunch
```
2. Fare clic su *Central Management Console*.
3. System (Sistema) dovrebbe essere il nome del computer host e Authentication (Autenticazione) dovrebbe essere Enterprise. In caso contrario, selezionare *Enterprise*.
4. Immettere nome utente e password e fare clic su *Log On (Esegui login)*.
5. Nel riquadro Organize (Organizza) fare clic su *Folders (Cartelle)*.
6. Fare clic su *eSecurity_Reports*.
7. Selezionare *tutto*.
8. Fare clic sulla scheda Rights (Diritti).
9. Per Everyone, selezionare *View on Demand (Visualizza su richiesta)* nel menu a discesa a destra. Fare clic su *Update (Aggiorna)*.
10. Eseguire il logoff e chiudere la finestra.

Abilitazione dei primi 10 rapporti di Sentinel

Per abilitare i primi dieci rapporti di Sentinel è necessario eseguire le operazioni seguenti:

- Attivare Aggregazione
- Abilitare EventFileRedirectService

Attivazione Aggregazione

1. Avviare Gestione dati Sentinel.
2. Eseguire il login.
3. Fare clic sulla scheda *Rapporto dati*.
4. Abilitare i riepiloghi seguenti
 - EventDestSummary

- EventSevSummary
- EventSrcSummary

Fare clic sui pulsanti 'Disattivo' nella colonna Stato finché diventano 'Attivo'.

Summary Name	Time	Attributes	Source	Status
EventDestSummary	1 hour	CUST_ID.RSRC_ID...	TransformedEvent	Active
EventSevDestTxnmy...	1 hour	CUST_ID.DEST_EV...	TransformedEvent	InActive
EventSevDestEvtSu...	1 hour	CUST_ID.DEST_EV...	TransformedEvent	InActive
EventSevDestPortSu...	1 hour	SEV.DEST_PORT.C...	TransformedEvent	InActive
EventSevSummary	1 hour	CUST_ID.SEV.EVT...	TransformedEvent	Active
EventSrcSummary	1 hour	CUST_ID.RSRC_ID...	TransformedEvent	Active

Abilitazione di EventFileRedirectService

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


```
$ESEC_HOME/sentinel/config/das_binary.xml
```
2. Per EventFileRedirectService, modificare lo stato su on.


```
<property name="status">on</property>
```
3. Riavviare il processo DAS_Binary. Questa operazione può essere eseguita mediante Sentinel Control Center o riavviando il computer.

Mediante Sentinel Control Center:

- Eseguire il login a Sentinel Control Center come utente con diritti di amministrazione. Questo utente dovrà disporre delle autorizzazioni di visualizzazioni server seguenti:
 - Visualizzazione server
 - Controllo server
- Dalla scheda Amministratore, aprire una visualizzazione server per visualizzare tutti i processi del server Sentinel.
- Fare clic con il pulsante destro del mouse sul processo *DAS_Binary* e selezionare *Riavvia*.
- Il numero di avvii per il processo aumenterà di un'unità se il processo viene riavviato correttamente.

Aumentare al massimo la generazione di rapporti

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 report sarà necessario riconfigurare Crystal Page Server.

Riconfigurazione di Crystal Page Server

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


```
http://<nomehost_o_IP_del_server_web>:<server_web_port_a_default_8080>/businessobjects/enterprise1/admin1aunch
```
2. Fare clic su *Central Management Console*.

3. System (Sistema) dovrebbe essere il nome del computer host e Authentication (Autenticazione) dovrebbe essere Enterprise. In caso contrario, selezionare Enterprise.
4. Immettere nome utente e password e fare clic su *Log On (Esegui login)*.
5. Fare clic su *Server*.
6. Fare clic su *<nome server>.pageserver*
7. 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)*, fare clic sul pulsante di scelta *'Unlimited records' (Senza limite di record)*.
8. Fare clic su *Applica*.
9. Verrà visualizzato un prompt per il riavvio del page server. Fare clic su *OK*.
10. È possibile che vengano richiesti un nome di accesso e una password per accedere al manager dei servizi del sistema operativo.

Configurazione di Sentinel sul server Crystal Enterprise Server

Dopo aver installato Crystal Enterprise è necessario specificare in Sentinel Control Center Gli URL per i rapporti di Analysis.

Configurazione di Sentinel per Crystal Enterprise Server

1. Eseguire il login a Sentinel Control Center come utente con privilegi per la scheda Amministratore.
2. Nella scheda Amministratore, selezionare *Configurazione rapporti*.
3. Nel campo URL analisi, digitare:

```
http://<nomehost_o_IP_del_server_web>:<server_web_port
a_default_8080>/esec-
script/GetReports.jsp?APS=<nomehost>&user=Guest&pas
sword=&tab=Analysis
```

NOTA: <nomehost_o_IP_del_server_web> deve essere sostituito con l'indirizzo IP o il nome host del server Crystal Enterprise Server.

NOTA: questo URL non funzionerà correttamente se APS è impostato sull'indirizzo IP. Deve corrispondere al nome host.

NOTA: <server_web_porta_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 si è installato Advisor, nel campo URL Advisor digitare:

```
http://<nomehost_o_IP_del_server_web>:<server_web_port
a_default_8080>/esec-
script/GetReports.jsp?APS=<nomehost>&user=Guest&pas
sword=&tab=Advisor
```

NOTA: <nomehost_o_IP_del_server_web> deve essere sostituito con l'indirizzo IP o il nome host del server Crystal Enterprise Server.

NOTA: questo URL non funzionerà correttamente se APS è impostato sull'indirizzo IP. Deve corrispondere al nome host.

NOTA: <server_web_porta_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.
7. Fare clic su *Salva*.
8. Eseguire il logout e quindi il login in Sentinel Control Center. Gli alberi di Crystal Report nelle schede Analisi e Advisor (se Advisor è installato) dovrebbero ora essere visualizzati nella barra di spostamento.

Utility e soluzione dei problemi

Avvio di MySQL

Per verificare che MySQL sia in esecuzione:

1. Eseguire il login come utente crystal.
2. passare alla directory /opt/crystal_xi/bobje
3. ./mysqlstartup.sh

Avvio di Tomcat

Per verificare che Tomcat sia in esecuzione:

1. Eseguire il login come utente crystal.
2. passare alla directory /opt/crystal_xi/bobje
3. ./tomcatstartup.sh

Avvio di Server Crystal Server

Per verificare che i server Crystal Server siano in esecuzione:

1. Eseguire il login come utente crystal.
2. passare alla directory /opt/crystal_xi/bobje
3. ./startservers

Errore del nome host Crystal

Errore del nome host

1. Se viene visualizzato l'errore seguente:

```
Warning: ORB::BOA_init: hostname lookup returned
`localhost' (127.0.0.1) (Avviso: ORB: :BOA_init: la
ricerca del nome host ha restituito 'host locale'
(127.0.0.1))
```

```
Use the -OAhost option to select some other hostname
(Utilizzare l'opzione -OAhost per selezionare un
altro nome host)
```

Verificare che l'indirizzo IP e il nome host siano presenti nel file /etc/hosts. Esempio:

```
192.0.2.46 linuxCE02
```

Impossibile connettersi a CMS

Se il sistema indica l'impossibilità di connettersi a CMS, provare a eseguire i comandi seguenti.

Soluzione dei problemi di errore di connessione a CMS

1. Se il comando "netstat -an | grep 6400" non ottiene alcun risultato, provare il seguente:
 - Reimmettere le informazioni di connessione a MySQL:
 - a. Eseguire il login come utente crystal.
 - b. passare alla directory /opt/crystal_xi/bobje
 - c. ./cmsdbsetup.sh
 - d. Premere Invio quando viene visualizzato "[<nomehost>.cms]"
 - e. Scegliere "select" (*seleziona*) e reimmettere tutte le informazioni sul database MySQL specificate al momento dell'installazione (fare riferimento alle istruzioni per l'installazione).
 - f. Al termine, chiudere cmsdbsetup.sh
 - g. ./stopservers
 - h. ./startservers
 - Inizializzare di nuovo il database MySQL:
 - a. Eseguire il login come utente crystal.
 - b. passare alla directory /opt/crystal_xi/bobje
 - c. ./cmsdbsetup.sh
 - d. Premere Invio quando viene visualizzato "[<nomehost>.cms]"
 - e. Scegliere "reinitialize" (Reinizializza) e seguire le istruzioni.
 - f. Al termine, chiudere cmsdbsetup.sh
 - g. ./stopservers
 - h. ./startservers
2. Verificare che tutti i server CCM siano abilitati:
 - a. Eseguire il login come utente crystal.
 - b. passare alla directory /opt/crystal_xi/bobje
 - c. ./ccm.sh -enable all

11

Configurazione di Advisor

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Sentinel di Advisor, con tecnologia SecurityNexus, offre funzioni di analisi in tempo reale delle vulnerabilità aziendali, suggerimenti, indicazioni e procedure per l'adozione delle misure di risposta appropriate. In Advisor è incluso un riferimento incrociato tra le firme degli attacchi IDS in tempo reale e la Knowledge Base dell'applicazione relativa alle vulnerabilità. Per ulteriori informazioni, visitare il sito all'indirizzo <http://www.esecurity.net/Software/Products/Advisor.asp>.

L'installazione di Advisor è facoltativa. Si tratta tuttavia di un componente necessario se si desidera utilizzare le funzionalità di rilevamento dell'utilizzo di Sentinel o di creazione di rapporti di Advisor.

Crystal BusinessObjects Enterprise™ 11 è uno degli strumenti per la generazione di rapporti che si integra con Sentinel. Per informazioni sull'installazione di Crystal BusinessObjects Enterprise™ 11, vedere il capitolo '*Crystal Reports*' adeguato alla piattaforma sulla quale si desidera eseguire il server Crystal Enterprise (Windows o Linux). Se si intende utilizzare Advisor solo per il rilevamento dell'utilizzo, non sarà necessario installare un server Crystal Server che è infatti necessario solo se si intende eseguire rapporti.

In questo capitolo viene illustrato come configurare Sentinel per l'esecuzione di rapporti di Advisor direttamente da Sentinel Control Center. I rapporti di Advisor Reports sono stati creati da Novell per essere utilizzati per la creazione di rapporti e di analisi e, una volta configurata correttamente l'integrazione con Sentinel Control Center, venire visualizzati nella scheda Advisor di Sentinel Control Center.

Installazione di Advisor

Advisor può essere solo installato nello stesso computer in cui si trova il servizio DAS (Database Access Service).

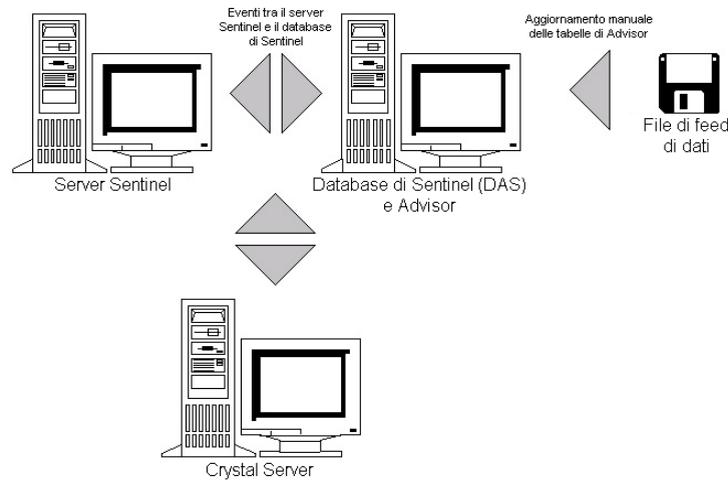
Sono disponibili due diverse opzioni di installazione, ovvero:

- Autonoma
- Download Internet diretto

Se si desidera eseguire Crystal Reports di Advisor, vedere prima il capitolo di *Crystal Reports* sull'installazione e la configurazione del server Crystal Server. Pubblicare quindi Crystal Reports di Advisor sul server Crystal Server. Per istruzioni sulla pubblicazione dei rapporti vedere [Importazione dei modelli di rapporti](#).

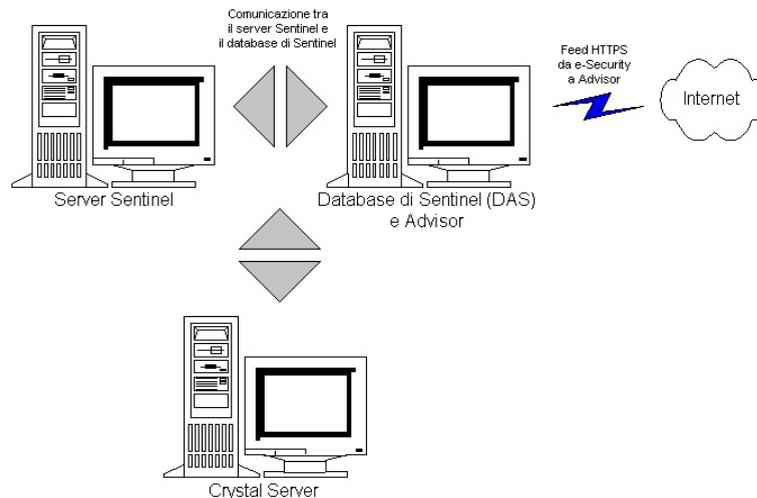
Configurazione autonoma

L'installazione autonoma prevede che Advisor sia configurato come sistema isolato che necessita di interventi manuali per ricevere aggiornamenti da Novell.



Configurazione download Internet diretto

Il download Internet diretto prevede che il computer che esegue Advisor sia connesso direttamente a Internet. In questa configurazione, gli aggiornamenti vengono scaricati da Novell automaticamente e a scadenze regolari mediante Internet.



Installazione di Advisor

NOTA: prima di installare Advisor, verificare di disporre del nome utente e della password di Advisor forniti da Novell. Durante l'installazione verranno infatti richiesti nome utente e password.

Se si intende eseguire rapporti di Advisor (Crystal Reports), eseguire la procedura seguente nell'ordine indicato. Se si intende utilizzare Advisor solo per il rilevamento dell'utilizzo, non sarà necessario eseguire la procedura indicata.

- Se non lo si è già fatto, eseguire le operazioni seguenti (vedere il capitolo *Crystal Reports*):
 - Installare Microsoft Internet Information Server (IIS)
 - **Per il database Sentinel su Oracle (Linux)** – Eseguire le operazioni preliminari all'installazione di Crystal BusinessObjects Enterprise

- Installare Crystal BusinessObjects Enterprise™ 11
- **Per il database Sentinel su Oracle (Solaris)** – Eseguire la configurazione del driver nativo Oracle (per installazioni Oracle)
- **Per il database Sentinel su MS SQL (Windows)** – Eseguire la configurazione di ODBC (Open Database Connectivity)
- Applicare la patch in Crystal Reports – Vedere il capitolo '*Crystal Reports*'.
- Installare Advisor – Se Advisor non è già stato installato, vedere il capitolo '*Aggiunta di componenti a un'installazione esistente*'.
- Importare i modelli di Crystal Reports
- Creare una pagina Web Crystal
- Configurare Sentinel Control Center per l'integrazione con Crystal Enterprise Server

Importazione dei modelli di Crystal Reports

A seconda del sistema operativo in uso fare riferimento a:

- *Capitolo 9 – Crystal Reports per Windows e Solaris*
- *Capitolo 10 – Crystal Reports per Linux*

Configurazione di Administration Launchpad

A seconda del sistema operativo in uso fare riferimento a:

- *Capitolo 9 – Crystal Reports per Windows e Solaris*
- *Capitolo 10 – Crystal Reports per Linux*

Impostazione dell'integrazione di Sentinel Control Center con rapporti di Advisor

Sentinel Control Center può essere integrato con rapporti di Advisor mediante la scheda Advisor. Grazie a questa funzionalità sarà possibile visualizzare un rapporto di Advisor direttamente da Sentinel Control Center.

Per abilitare questa funzionalità, installare prima Crystal Server, importare i modelli di rapporti di Advisor in Crystal Server e installare Advisor. Una volta eseguite queste operazioni, seguire le istruzioni riportate nella sezione "Configurazione di Sentinel per l'integrazione con Crystal Enterprise Server" in:

- *Capitolo 9 – Crystal Reports per Windows e Solaris*
- *Capitolo 10 – Crystal Reports per Linux*

Aggiornamento dei dati nelle tabelle di Advisor

A meno che non si disponga di una configurazione autonoma, i dati nelle tabelle di Advisor saranno aggiornati automaticamente durante il successivo download pianificato del feed di Advisor. È in ogni caso possibile aggiornare i dati anche in modo manuale. Per aggiornarli manualmente, vedere la *Guida dell'utente di Sentinel*.

Ripristino della password di Advisor (solo download diretto)

Se si sta eseguendo Advisor in modalità di download diretto e si è ottenuta una nuova password di Advisor o la password di Advisor impostata durante l'installazione non era corretta, sarà necessario ripristinare la password cifrata di Advisor memorizzata nel file di configurazione di Advisor.

L'aggiornamento della password cifrata di Advisor non è applicabile se si sta eseguendo Advisor in modalità autonoma perché in questa modalità la password non viene memorizzata nel file di configurazione di Advisor.

Per ripristinare la password cifrata di Advisor memorizzata nel file di configurazione di Advisor, eseguire le operazioni seguenti:

1. Per UNIX eseguire il login come utente `esecadm` oppure per Windows eseguire il login come utente con diritti di amministrazione. Eseguire il login al computer in cui è installato Advisor.

2. Passare alla directory:

Per UNIX:

```
$ESEC_HOME/sentinel/bin
```

Per Windows:

```
%ESEC_HOME%\sentinel\bin
```

3. Eseguire il comando seguente, dove `<nuovapassword>` è la password di Advisor che si desidera impostare:

Per UNIX:

```
./adv_change_passwd.sh <nuovapassword>
```

Per Windows:

```
adv_change_passwd.bat <nuovapassword>
```

12 Test dell'installazione

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

I seguenti servizi di raccolta di test vengono installati con Gestione servizi di raccolta allo scopo di consentire la verifica dell'installazione. Il nome e la descrizione di ognuno di tali servizi di raccolta è:

Per il test del flusso di eventi di base:

- **SendOneEvent:** invia un evento tramite Sentinel e quindi si interrompe.
- **SendMultipleEvents:** invia 20 eventi tramite Sentinel e quindi si interrompe.

Per il testo della mappatura delle risorse di evento e il rilevamento degli exploit:

- **DemoEvents:** invia 13 eventi tramite Sentinel e quindi si interrompe.
- **DemoAssetUpload:** carica dati di risorsa dimostrativi in Sentinel. Quando il servizio di raccolta DemoEvents viene eseguito in questo servizio di raccolta, i dati di risorse di quest'ultimo verranno visualizzati come risultato della mappatura di eventi. Questo servizio di raccolta non genera eventi esterni.
- **DemoVulnerabilityUpload:** carica dati di vulnerabilità dimostrativi in Sentinel. Quando il servizio di raccolta DemoEvents viene eseguito dopo questo servizio di raccolta, nonché dopo l'esecuzione dello scaricamento del feed di Advisor, alcuni eventi di tale servizio di raccolta attiveranno un rilevamento di exploit, ovvero il campo Vulnerabilità dell'evento verrà impostato su 1). Questo servizio di raccolta non genera eventi esterni.

Per ulteriori informazioni, inclusa la configurazione, negli altri servizi di raccolta accedere a:

```
%ESEC_HOME%\wizard\Elements\raccolta>\docs\
```

Test dell'installazione mediante i servizi di raccolta di prova

In Sentinel v5.1.2 e versioni successive, i servizi di raccolta vengono installati preconfigurati in tutte le istanze di Gestione servizi di raccolta. Se pertanto si utilizza questa versione di Sentinel, è possibile passare direttamente all'esecuzione dei servizi di raccolta di prova per verificare l'installazione.

In Sentinel v5.1.1 e versioni precedenti, è necessario configurare manualmente i servizi di raccolta in Gestione servizi di raccolta prima di poterli utilizzare. Per configurare i servizi di raccolta di prova, seguire le istruzioni nella sezione [Configurazione dei servizi di raccolta di prova](#). Tornare quindi a questa sezione per verificare l'installazione mediante tali servizi di raccolta.

Esecuzione dei servizi di raccolta di prova per verificare l'installazione

1. Aprire Sentinel Control Center.
2. Fare clic sulla scheda *Servizi di raccolta*.

3. Nella finestra di dialogo Gestione visualizzazione servizi di raccolta, fare doppio clic sulla visualizzazione di *tutti gli agenti* per visualizzare tutte le porte dei servizi di raccolta.
4. Verranno visualizzate tutte le porte dei servizi di raccolta attualmente configurate, raggruppate in base al nome di Gestione servizi di raccolta. Se non viene visualizzata alcuna porta, significa che nessuna delle istanze di Gestione servizi di raccolta è attualmente connessa a Sentinel. Se si ritiene che una o più istanze di Gestione servizi di raccolta debbano essere connesse a Sentinel, verificare che siano in esecuzione e l'eventuale presenza di errori nei file di log del server Sentinel e di Gestione servizi di raccolta.
5. Prima di eseguire un servizio di raccolta, aprire una visualizzazione Active Views in modo da poter visualizzare gli eventi generati dai servizi di raccolta di prova. A tale scopo:
 - Fare clic sulla scheda *Active Views*.
 - Selezionare *Active Views > Crea visualizzazione Active Views* nella barra dei menu.
 - Selezionare il filtro *PUBLIC::External_Events*
 - Fare clic su *Fine*.
6. Per eseguire un servizio di raccolta per verificare il flusso di eventi di base:
 - Passare alla scheda *Servizi di raccolta*.
 - Fare clic con il pulsante destro del mouse sulla porta del servizio di raccolta *SendMultipleEvents* nella visualizzazione Servizi di raccolta e scegliere l'azione *Avvia*. Poiché i servizi di raccolta di test vengono eseguiti solo per un breve periodo e quindi vengono arrestati, lo stato della porta del servizio di raccolta passerà brevemente a "attivo" per tornare quindi a "disattivo".
 - Per verificare l'effettivo flusso degli eventi nel sistema, tornare alla scheda *Active Views* e controllare la visualizzazione *Active Views* creata. Può essere necessario qualche minuto perché l'evento sia visualizzato nella visualizzazione *Active Views* dopo l'esecuzione del servizio di raccolta.
7. Per eseguire un servizio di raccolta per verificare la mappatura delle risorse di evento:
 - Passare alla scheda *Servizi di raccolta*.
 - Fare clic con il pulsante destro del mouse sulla porta del servizio di raccolta *DemoAssetUpload* nella visualizzazione Servizi di raccolta e scegliere l'azione *Avvia*. Poiché i servizi di raccolta di test vengono eseguiti solo per un breve periodo e quindi vengono arrestati, lo stato della porta del servizio di raccolta passerà brevemente a "attivo" per tornare quindi a "disattivo".
 - Attendere un minuto o due affinché i dati della risorsa vengano caricati in Sentinel, generati nella mappatura mediante l'apposito servizio e distribuiti alle istanze di Gestione servizi di raccolta. Sarà possibile verificare il completamento di queste operazioni osservando l'evento interno *RefreshingMapFromServer* con "Asset" nel relativo messaggio di evento. Per visualizzare questo evento interno, è necessario utilizzare una visualizzazione *Active Views* con un filtro che consenta agli eventi interni di passare (ovvero *PUBLIC::Internal_Events*). Il filtro *PUBLIC::External_Events* non consente il passaggio degli eventi interni.
 - Fare clic con il pulsante destro del mouse sulla porta del servizio di raccolta *DemoEvents* nella visualizzazione Servizi di raccolta e selezionare l'azione *Avvia*. Poiché i servizi di raccolta di test vengono eseguiti solo per un breve periodo e quindi vengono arrestati, lo stato della porta del servizio di raccolta passerà brevemente a "attivo" per tornare quindi a "disattivo".

- Per verificare che le mappature di risorsa siano state effettuate, fare doppio clic su un evento (nella tabella degli eventi nella parte inferiore della visualizzazione Active Views) appena generato dal servizio di raccolta DemoEvents in modo da visualizzarne i dettagli. Nei dettagli di evento visualizzati a sinistra della tabella degli eventi, espandere il gruppo Risorsa per visualizzarne i dati di mappatura. Può essere necessario qualche minuto perché l'evento sia visualizzato nella visualizzazione Active Views dopo l'esecuzione del servizio di raccolta.
8. Per eseguire un servizio di raccolta per verificare il rilevamento degli exploit (è necessario che il componente Advisor sia installato):
- Eseguire lo scaricamento del feed di Advisor. L'operazione potrebbe richiedere alcuni minuti.

In Windows:

- Accedere al computer in cui è installato Advisor. Eseguire l'operazione pianificata di Advisor (*Start > Pannello di controllo > Operazioni pianificate > {e-Security_Advisor | at1}*)

In UNIX:

- Eseguire il login al computer in cui è installato Advisor come utente esecadm ed eseguire:

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

- In Sentinel Control Center, passare alla scheda Servizi di raccolta
- Fare clic con il pulsante destro del mouse sulla porta del servizio di raccolta *DemoVulnerabilityUpload* nella visualizzazione Servizi di raccolta e scegliere l'azione Avvia. Poiché i servizi di raccolta di test vengono eseguiti solo per un breve periodo e quindi vengono arrestati, lo stato della porta del servizio di raccolta passerà brevemente a "attivo" per tornare quindi a "disattivo".
- Attendere finché i dati aggiornati del rilevamento degli exploit non vengono completati in Gestione servizi di raccolta. Sarà possibile verificare il completamento di queste operazioni osservando l'evento interno RefreshingMapFromServer con "IsExploitWatchlist" nel relativo messaggio di evento. Per visualizzare questo evento interno, è necessario utilizzare una visualizzazione Active Views con un filtro che consenta agli eventi interni di passare (ovvero PUBLIC::Internal_Events). Il filtro PUBLIC::External_Events non consente il passaggio degli eventi interni. L'invio dei dati di rilevamento degli exploit aggiornati a Gestione servizi di raccolta potrebbe richiedere poco più di mezz'ora a causa dell'aggiornamento di tali dati eseguito per default da DAS ogni 30 minuti.
- Fare clic con il pulsante destro del mouse sulla porta del servizio di raccolta *DemoEvents* nella visualizzazione Servizi di raccolta e selezionare l'azione Avvia. Poiché i servizi di raccolta di test vengono eseguiti solo per un breve periodo e quindi vengono arrestati, lo stato della porta del servizio di raccolta passerà brevemente a "attivo" per tornare quindi a "disattivo".
- Per verificare che il rilevamento degli exploit sia stato effettuato, fare doppio clic su un evento (nella tabella degli eventi nella parte inferiore della visualizzazione Active Views) appena generato dal servizio di raccolta DemoEvents in modo da visualizzarne i dettagli. Nei dettagli di evento visualizzati a sinistra della tabella degli eventi, espandere il gruppo Exploit per visualizzarne i dati di rilevamento degli exploit. Il campo Vulnerabilità di alcuni eventi dovrebbe essere impostato su 1.

Può essere necessario qualche minuto perché l'evento sia visualizzato nella visualizzazione Active Views dopo l'esecuzione del servizio di raccolta.

Configurazione dei servizi di raccolta di prova

In Sentinel v5.1.1 e versioni successive, i servizi di raccolta di prova non vengono preconfigurati al momento dell'installazione. È pertanto necessario utilizzare Generatore servizi di raccolta (su un computer Windows) per configurare i servizi di raccolta ai fini dell'esecuzione.

In sentinel v5.1.2 e versioni successive, queste operazioni di configurazione non sono necessarie a meno che le porte dei servizi di raccolta di prova siano state eliminate.

Configurazione del servizio di raccolta SendOneEvent

Configurazione, caricamento ed esecuzione del servizio di raccolta SendOneEvent

1. Aprire l'applicazione Generatore servizi di raccolta.
2. Fare clic sulla scheda *Host Wizard*.
3. Evidenziare il nome host del computer in uso. Il nome host sarà visualizzato nel campo sotto il menu nella parte superiore dell'applicazione.
4. Fare doppio clic su *Nuovo* sotto l'intestazione Nome porta.
5. Specificare un nome della porta di Wizard (ad esempio SendOneEvent).
6. Nella casella relativa al tipo Rx/Tx, scegliere *Nessuno*.
7. Lasciare vuoto il valore di Rx/Tx.
8. Sulla stessa riga, fare clic sul menu a discesa della colonna Servizio di raccolta e scegliere SendOneEvent:
9. Fare clic su *Salva*.
10. Fare clic sulla scheda *Servizi di raccolta*.
11. Espandere il servizio di raccolta SendOneEvent.
12. Fare clic con il pulsante destro del mouse sul file del modello SendOneEvent e scegliere *Genera script*.
13. Fare clic con il pulsante destro del mouse sul servizio di raccolta SendOneEvent, quindi scegliere di *caricare il servizio di raccolta*.
14. Nella scheda Servizi di raccolta, il computer in uso dovrebbe essere selezionato. Fare clic su *Carica*.
15. Se richiesto, digitare la password di Gestione servizi di raccolta.
16. Fare clic su *OK*.

Configurazione del servizio di raccolta SendMultipleEvents

Configurazione, caricamento ed esecuzione del servizio di raccolta SendMultipleEvents

1. Aprire l'applicazione Generatore servizi di raccolta.
2. Fare clic sulla scheda *Host Wizard*.
3. Evidenziare il nome host per il computer in uso. Il nome host sarà visualizzato nel campo sotto il menu nella parte superiore dell'applicazione.
4. Fare doppio clic su *Nuovo* sotto l'intestazione Nome porta e specificarne il nome, ad esempio SendMultipleEvents.

5. Sulla stessa riga, fare clic sul menu a discesa della colonna relativa al tipo Rx/Tx e selezionare di archiviare tutto:
6. Sulla stessa riga, fare clic sulla casella di testo relativa alla colonna del valore Rx/Tx e digitare il percorso al file di input:


```
Elements\SendMultipleEvents\config\test_events.csv
```
7. Sulla stessa riga, fare clic sul menu a discesa della colonna Servizio di raccolta e scegliere SendMultipleEvents.
8. Fare clic su *Salva*.
9. Fare clic sulla scheda *Servizi di raccolta*.
10. Espandere il servizio di raccolta SendMultipleEvents.
11. Fare clic con il pulsante destro del mouse sul file del modello SendMultipleEvents e scegliere *Genera script*.
12. Fare clic con il pulsante destro del mouse sul servizio di raccolta SendMultipleEvents, quindi scegliere di *caricare il servizio di raccolta*.
13. Nella scheda Servizi di raccolta, il computer in uso dovrebbe essere selezionato. Fare clic su *Carica*.
14. Se richiesto, digitare la password di Gestione servizi di raccolta.
15. Fare clic su *OK*.

Configurazione del servizio di raccolta DemoEvents

Configurazione, caricamento ed esecuzione del servizio di raccolta DemoEvents

1. Aprire l'applicazione Generatore servizi di raccolta.
2. Fare clic sulla scheda Host Wizard.
3. Evidenziare il nome host per il computer in uso. Il nome host sarà visualizzato nel campo sotto il menu nella parte superiore dell'applicazione.
4. Fare doppio clic su Nuovo sotto l'intestazione Nome porta e specificarne il nome (ad esempio DemoEvents).
5. Sulla stessa riga, fare clic sul menu a discesa della colonna del tipo Rx/Tx e selezionare Archivia tutto:
6. Sulla stessa riga, fare clic sulla casella di testo relativa alla colonna del valore Rx/Tx e digitare il percorso al file di input:


```
Elements\DemoEvents\data\Generic_Events.csv
```
7. Sulla stessa riga, fare clic sul menu a discesa della colonna Servizio di raccolta e scegliere DemoEvents.
8. Fare clic su *Salva*.
9. Fare clic su *Carica*.
10. Selezionare la scheda Servizi di raccolta.
11. Fare clic sulla freccia giù e selezionare il servizio di raccolta DemoEvents.
12. Fare clic su *Carica*.
13. Se richiesto, digitare la password di Gestione servizi di raccolta.
14. Fare clic su *OK*.

Configurazione del servizio di raccolta DemoAssetUpload

Configurazione, caricamento ed esecuzione del servizio di raccolta DemoAssetUpload

1. Aprire l'applicazione Generatore servizi di raccolta.
2. Fare clic sulla scheda Host Wizard.
3. Evidenziare il nome host per il computer in uso. Il nome host sarà visualizzato nel campo sotto il menu nella parte superiore dell'applicazione.
4. Fare doppio clic su *Nuovo* sotto l'intestazione Nome porta e specificarne il nome, ad esempio DemoAssetUpload.
5. Sulla stessa riga, fare clic sul menu a discesa della colonna del tipo Rx/Tx e selezionare Archivia tutto:
6. Sulla stessa riga, fare clic sulla casella di testo relativa alla colonna del valore Rx/Tx e digitare il percorso al file di input:

```
Elements\DemoAssetUpload\data\asset_info.csv
```

7. Sulla stessa riga, fare clic sul menu a discesa della colonna Servizio di raccolta e scegliere DemoAssetUpload.
8. Fare clic su *Salva*.
9. Fare clic su *Carica*.
10. Selezionare la scheda Servizi di raccolta.
11. Fare clic sulla freccia giù e selezionare il servizio di raccolta DemoAssetUpload.
12. Fare clic su *Carica*.
13. Se richiesto, digitare la password di Gestione servizi di raccolta.
14. Fare clic su *OK*.

Configurazione del servizio di raccolta DemoVulnerabiltyUpload

Configurazione, caricamento ed esecuzione del servizio di raccolta DemoVulnerabiltyUpload

1. Aprire l'applicazione Generatore servizi di raccolta.
2. Fare clic sulla scheda Host Wizard.
3. Evidenziare il nome host per il computer in uso. Il nome host sarà visualizzato nel campo sotto il menu nella parte superiore dell'applicazione.
4. Fare doppio clic su *Nuovo* sotto l'intestazione Nome porta e specificarne il nome, ad esempio DemoVulnerabiltyUpload.
5. Sulla stessa riga, fare clic sul menu a discesa della colonna del tipo Rx/Tx e selezionare Archivia tutto:
6. Sulla stessa riga, fare clic sulla casella di testo relativa alla colonna del valore Rx/Tx e digitare il percorso al file di input:

```
Elements\DemoVulnerabiltyUpload\data\vuln_info.csv
```

7. Sulla stessa riga, fare clic sul menu a discesa della colonna Servizio di raccolta e scegliere DemoVulnerabiltyUpload.
8. Fare clic su *Salva*.
9. Fare clic su *Carica*.
10. Selezionare la scheda Servizi di raccolta.

11. Fare clic sulla freccia giù e selezionare il servizio di raccolta DemoVulnerabiltyUpload.
12. Fare clic su *Carica*.
13. Immettere la password di Gestione servizi di raccolta.
14. Fare clic su *OK*.

13

Modifiche al livello di comunicazione (iSCALE)

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

livello di comunicazione: AES *Vedere* .archivio chiavi livello di comunicazione: ARC4 *Vedere* .archivio chiavi il livello di comunicazione (iSCALE) che connette tutti i componenti dell'architettura è una connessione TCP/IP cifrata. Per default questa comunicazione è cifrata utilizzando chiavi AES a 256 bit. È inoltre possibile utilizzare le chiavi ARC4.

keymgr consente di scegliere il metodo di cifratura da utilizzare e di modificare la chiave. Il programma genera un file nella directory lib dell'installazione di Sentinel (\$ESEC_HOME/lib or %ESEC_HOME%\lib) denominata keystore (archivio chiavi). È necessario copiare il file in ogni computer in cui è installato un componente di Sentinel.

È consigliabile modificare la chiave di sicurezza di default per fornire parametri di cifratura e autenticazione univoci.

NOTA: se in tutti i computer che eseguono Gestione servizi di raccolta è configurato il connettore DBConnector o RDEP, è necessario aggiornare le password in tutte le istanze del file di configurazione di questo connettore. È necessario eseguire questa operazione perché la chiave di cifratura utilizzata per cifrare la password prima che venga memorizzata nel file di configurazione è basata sulla chiave inclusa nel file .keystore appena aggiornato.

Modifiche delle chiavi di cifratura

Modifiche alle chiavi o abilitazione di altri metodi di cifratura

1. Per UNIX, eseguire il login come utente esecadm. Per Windows, accedere come utente con diritti di amministrazione.

2. Passare alla directory:

Per Windows:

```
%ESEC_HOME%\lib
```

Per UNIX:

```
$ESEC_HOME/lib
```

3. Eseguire il comando seguente:

In Windows:

```
"%ESEC_JAVA_HOME%\java" -jar keymgr.jar --keyalgo  
<encryption [AES or ARC4]> --keysize 256
```

In UNIX:

```
$ESEC_JAVA_HOME/java -jar keymgr.jar --keyalgo  
<encryption [AES or ARC4]> --keysize 256
```

Ciò consentirà di impostare il metodo di cifratura. Verrà creato un file denominato .keystore nella directory lib.

4. Copiare il file .keystore in ogni computer in cui è installato un componente Sentinel. È necessario copiare il file in:

Per Windows:

```
%ESEC_HOME%
```

Per UNIX:

```
$ESEC_HOME
```

5. Se in tutti i computer che eseguono Gestione servizi di raccolta è configurato il connettore DBConnector o RDEP, è necessario aggiornare le password in tutte le istanze del file di configurazione di questo connettore. È necessario eseguire questa operazione perché la chiave di cifratura utilizzata per cifrare la password prima che venga memorizzata nel file di configurazione del connettore è basata sulla chiave inclusa nel file .keystore appena aggiornato. Per istruzione sull'impostazione delle password nei file di configurazione del connettore, vedere la documentazione relativa ai connettori DBConnector e RDEP Connector.
6. Se si esegue Advisor in modalità di scaricamento diretto, è necessario aggiornare la password cifrata di Advisor memorizzata nel relativo file di configurazione. È necessario eseguire questa operazione perché la chiave di cifratura utilizzata per cifrare la password prima che venga memorizzata nel file di configurazione di Advisor è basata sulla chiave inclusa nel file .keystore appena aggiornato. L'aggiornamento della password cifrata di Advisor non è applicabile se si sta eseguendo Advisor in una configurazione autonoma perché in questa modalità la password non viene memorizzata nel file di configurazione di Advisor. Per aggiornare la password cifrata di Advisor memorizzata nel file di configurazione di Advisor, eseguire i passaggi seguenti nell'ordine indicato:

- Per UNIX eseguire il login come utente esecadm oppure per Windows eseguire il login come utente con diritti di amministrazione. Eseguire il login al computer in cui è installato Advisor.
- Passare alla directory:

Per UNIX:

```
$ESEC_HOME/sentinel/bin
```

Per Windows:

```
%ESEC_HOME%\sentinel\bin
```

- Immettere i comandi seguenti:

Per UNIX:

```
./adv_change_passwd.sh <nuovapassword>
```

Per Windows:

```
adv_change_passwd.bat <nuovapassword>
```

14

Aggiunta di componenti a un'installazione esistente

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Il programma di installazione di Sentinel 5 Enterprise Security Management supporta l'aggiunta di componenti Sentinel in un'installazione esistente. Un esempio di aggiunta di un componente potrebbe essere se si installasse in un computer solo Gestione servizi di raccolta di Wizard e in seguito si decidesse di installarvi anche Sentinel Control Center. In questo caso, si dovrebbe aggiungere il componente Sentinel Control Center nell'installazione di Gestione servizi di raccolta di Wizard.

NOTA: prima di aggiungere un componente, assicurarsi di disporre del gruppo di variabili corretto di Sentinel.

```
ESEC_HOME
ESEC_JAVA_HOME
WORKBENCH_HOME
ESEC_CONF_FILE
ESEC_VERSION
ESEC_USER
LD_LIBRARY_PATH
```

Aggiunta di componenti in Solaris o Linux

Aggiunta di componenti in Solaris

1. Eseguire il login come utente radice.
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 digitare:

```
./setup.sh
```

oppure

```
./setup.sh -console (se X Windows non è disponibile)
```

4. Verrà visualizzato un messaggio che indica l'ubicazione dell'installazione precedente e i componenti già installati. Fare clic su *Avanti*.
5. Scegliere i componenti che si desidera aggiungere, quindi fare clic su *Avanti*.
6. Seguire i prompt, digitando le informazioni appropriate. Per ulteriori informazioni su un particolare prompt, fare riferimento al capitolo di installazione appropriato.

Aggiunta di componenti in Windows

Aggiunta di componenti in Windows

1. Inserire il CD di installazione di Sentinel nell'unità CD-ROM.
2. Passare al CD e fare doppio clic su *setup.bat*.

NOTA: l'installazione in modalità console non è supportata in Windows.

3. Fare clic su *Avanti* nella schermata introduttiva.
4. Accettare le condizioni del Contratto di licenza per l'utente finale e fare clic su *Avanti*.
5. Verrà visualizzato un messaggio che indica l'ubicazione dell'installazione precedente e i componenti già installati. Fare clic su *Avanti*.
6. Scegliere i componenti che si desidera aggiungere, quindi fare clic su *Avanti*.
7. Seguire i prompt, digitando le informazioni appropriate. Per ulteriori informazioni su un particolare prompt, fare riferimento al Capitolo 3 (per Solaris), al capitolo 4 (per Linux) o al capitolo 5 (per Windows).

15

Disinstallazione del software

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Disinstallazione di Sentinel, Gestione servizi di raccolta e Advisor

Disinstallazione per Solaris e Linux

Avvio del programma di disinstallazione Sentinel per Solaris

1. Eseguire il login come utente radice.
2. Arrestare il server Sentinel.
3. Passare alla directory:

```
$ESEC_HOME/_uninst
```

4. Immettere:

```
./uninstall.bin
```

NOTA: in Solaris e Linux, dopo aver disinstallato il server Sentinel, è necessario rimuovere manualmente l'utente esecadm dal sistema operativo se lo si desidera.

Disinstallazione per Windows

Utilizzo del programma di disinstallazione per Windows di Sentinel

1. Eseguire il login come Amministratore.
 2. Arrestare il server Sentinel.
 3. Fare clic su *Start > Programmi > Sentinel > Disinstalla Sentinel 5.x*
- Seguire i prompt visualizzati. Selezionare le applicazioni da disinstallare.

- Database
- Communication Server (bus di messaggi)
- Advisor
- Servizi Sentinel di base
- Correlazione
- DAS
- Servizio di raccolta (Gestione servizi di raccolta)
- Sentinel Control Center
- Gestione dati Sentinel (Sentinel Database Manager, SDM)
- HP OpenView Service Desk
- Remedy Integration

Disinstallazione mediante il Pannello di controllo

Per disinstallare le applicazioni per Windows di Sentinel

1. Fare clic su *Start > Programmi > Impostazioni > Pannello di controllo > Installazione applicazioni*
2. Fare clic su *Sentinel 5.x*.
3. Seguire le istruzioni visualizzate . Verrà chiesto di selezionare l'applicazione da disinstallare. Selezionare le applicazioni che si desidera disinstallare.

Operazioni successive alla disinstallazione

Al termine del processo di disinstallazione di Sentinel 5 nel computer rimangono alcuni file che è necessario eliminare manualmente. È possibile eliminare la directory \$ESEC_HOME o %ESEC_HOME% e tutte le relative sottodirectory. Nel caso di Advisor può essere opportuno eliminare la cartella degli attacchi e degli avvisi relativi ai file di dati.

Alcuni file che possono rimanere sul computer sono i seguenti:

- File di log di Sentinel
- File di logo di Wizard
- File di log di DAS
- File di log di Gestione servizi di raccolta

A volte, dopo la disinstallazione, possono rimanere le impostazioni del sistema. Vedere *l'Appendice E* per informazioni sulle procedure necessarie per rimuovere manualmente le impostazioni di sistema rimanenti.

A

Questionario preliminare all'installazione

NOTA: per gli utenti di MS SQL 2000, la dimensione degli eventi non può superare gli 8 KB.

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Domande preliminari all'installazione

1. Dopo aver determinato il computer da utilizzare come sistema DAS e avere verificato che soddisfi i requisiti hardware e del sistema operativo necessari:
 - a. Recuperare il numero id dell'host del computer DAS
 - b. Richiedere a Novell il codice di licenza
2. Per quale scopo o intenzione si utilizza Novell Sentinel?
 - a. Conformità
 - b. SEM
 - c. Altro _____
3. In quale architettura di rete, per i dispositivi di origine riguardo al segmento di sicurezza si desidera cercare l'hardware Sentinel/Wizard?

NOTA: questa informazione è importante per comprendere la gerarchia dalla raccolta dati della procedura guidata e identificare tutti i firewall che è necessario attraversare per consentire le comunicazioni tra Wizard e Sentinel, Sentinel e DB o Crystal Server e DB.

Immettere le informazioni (testo e/o illustrazione) oppure il collegamento alle informazioni nella sezione seguente.

4. Quali rapporti si desidera escludere dal sistema? Questa informazione serve a garantire che i servizi di raccolta raccolgano i dati corretti da trasferire al database di Sentinel.
- a. _____
- b. _____
- c. _____
- d. _____
- e. _____
- f. _____
5. Da quali dispositivi di origine si desidera raccogliere dati (IDS, HIDS, Router, Firewall, ecc...), frequenza eventi (EPS eventi al secondo, events per second), 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? Queste informazioni servono a garantire che Sentinel fornisca i dati desiderati.

6. 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.
 - Questi dati non possono essere applicati alle installazioni Solaris. Sentinel non supporta NIS.
7. Quali componenti hardware sono stati allocati per l'installazione di Sentinel? I componenti hardware allocati sono conformi alle specifiche hardware menzionate nei capitoli 1 e 2 della Guida all'installazione?
8. Specificare il periodo di memorizzazione dei dati in termini di giorni? È generalmente consigliabile il valore 30 giorni. MS SQL non supporta la memorizzare dati per oltre 60 giorni. Oracle non presenta limiti di tempo.
9. 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.

10. È stato verificato che i requisiti di Sentinel per il funzionamento rispettino la configurazione specificata nei capitoli 1 e 2 della Guida all'installazione?
- Livelli patch sistema operativo
 - Service Pack
 - Hot Fix, e così via.

B

Manutenzione relativa alle operazioni preliminari e successive all'installazione per il database Oracle in Solaris

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Elenco di controllo relativo alle operazioni preliminari all'installazione

Questo elenco di controllo relativo alle operazioni preliminari all'installazione di Oracle è destinato principalmente alle installazioni distribuite. Può in ogni caso essere utilizzato per installazioni autonome. Se il numero di istanze di Gestione servizi di raccolta e del motore di correlazione è superiore a tre, prenderne nota. Questo elenco di controllo non consente un numero di istanze di Gestione servizi di raccolta e del motore di correlazione superiore a tre.

Per ulteriori informazioni, vedere il *capitolo 3 "Installazione di Sentinel 5 per Oracle"*.

	Variabile di configurazione		
1.	<i>Versione di Sentinel:</i>	<i>Data attuale:</i>	
	<i>Sistema operativo</i>		
	▪ Sistema operativo corretto per DB	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	▪ Patch corretta <input type="checkbox"/> : Sì <input type="checkbox"/> : No
	▪ DB Oracle corretto con partizionamento	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	▪ Patch corretta <input type="checkbox"/> : Sì <input type="checkbox"/> : No
	▫ Versione		▫ Livello patch
	▪ Copia di Oracle Note: 148673.1	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	
	▪ Variabili di ambiente corrette impostate per l'utente del sistema operativo Oracle.	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	
	▪ Sistema operativo corretto per i componenti di Sentinel	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	▪ Patch corretta <input type="checkbox"/> : Sì <input type="checkbox"/> : No
2.	<i>Computer DAS</i>		
	▪ ID host		
	▪ numero di serie		
	▪ codice di licenza		
3.	<i>Installazione DAS</i>		
	▪ Nome host o IP database		Valore di default: ESEC

Variabile di configurazione			
	▪ Nome database		Valore di default: 1521
	▪ Porta database		
	▪ Ubicazione file JDBC		
4.	<i>Valori kernel UNIX per Oracle. I seguenti sono i valori minimi.</i>		
	▪ shminfo_shmmax	4294967295 <input type="checkbox"/> : Sì <input type="checkbox"/> : No	Valore se superiore:
	▪ shminfo_shmmin	1 <input type="checkbox"/> : Sì <input type="checkbox"/> : No	Valore se superiore:
	▪ shminfo_shmseg	50 <input type="checkbox"/> : Sì <input type="checkbox"/> : No	Valore se superiore:
	▪ shminfo_shmmni	400 <input type="checkbox"/> : Sì <input type="checkbox"/> : No	Valore se superiore:
	▪ seminfo_semmns	14000 <input type="checkbox"/> : Sì <input type="checkbox"/> : No	Valore se superiore:
	▪ seminfo_semmni	1024 <input type="checkbox"/> : Sì <input type="checkbox"/> : No	Valore se superiore:
	▪ seminfo_semmssl	1024 <input type="checkbox"/> : Sì <input type="checkbox"/> : No	Valore se superiore:
	▪ seminfo_shmopm	100 <input type="checkbox"/> : Sì <input type="checkbox"/> : No	Valore se superiore:
	▪ seminfo_shmvmx	32767 <input type="checkbox"/> : Sì <input type="checkbox"/> : No	Valore se superiore:
5.	<i>Istanza database (SID)</i>		
6.	<i>Nome database</i>		
7.	<i>Componenti di Sentinel:</i>		
	▪ Database di Sentinel (IP o DNS)		OS: Patch:
	▫ Log di installazione DB		
	▫ Memoria Oracle (RAM)		
	▫ Nome istanza		
	▫ Porta listener	Default: 1521	
	▫ Password SYS		
	▫ Password di sistema		
	▪ Communication Server (iSCALE) (IP o DNS)		OS: Patch:

Variabile di configurazione			
	▪ Servizi Sentinel di base (IP o DNS)		OS: Patch:
	▪ DAS/Advisor (IP o DNS). Advisor è facoltativo		OS: Patch:
	▫ RAM DAS		
	▪ Motore di correlazione (IP e sistema operativo)		
		IP:	OS:
		IP:	OS:
		IP:	OS:
	▪ Crystal Server (IP o DNS)		
	▫ MS SQL (facoltativo, ma consigliato)	Versione di MS SQL: Patch di MS SQL: contenitore di password o password sa:	
	▪ Generatore servizi di raccolta (IP o DNS, consigliata un'unica installazione)		
▪ Gestione servizi di raccolta (servizi di raccolta)	NOTA: è possibile impostare Gestione servizi di raccolta senza l'uso di password.		
▫ IP:	PW:	OS:	
▫ IP:	PW:	OS:	
▫ IP:	PW:	OS:	
8.	<i>Advisor (facoltativo)</i>		
	▪ Ubicazione file feed di dati		
	▪ Indirizzo mittente Advisor		
	▪ Indirizzo destinatario Advisor		
	▪ Nome utente e password	n/u:	PW:
9.	<i>Ubicazione file di database:</i>		
	▪ File di dati		
	▪ File di indice		
	▪ File di dati di riepilogo		
	▪ File di indice di riepilogo		
	▪ File dello spazio delle tabelle di annullamento e temporanei		
	▪ Directory log di ripetizione membro A		
	▪ Directory log di ripetizione membro B		

	Variabile di configurazione		
10.	<i>Dimensioni database:</i>		Valore di default: /export/home
	▪ Standard (20 GB)		
	▪ Grandi (400 GB)		
	▪ Personalizzate (dimensioni)		
11.	<i>SMTP Server: (DNS o IP)</i>		
12.	<i>Password utente</i>		
	▪ esecadm	PW:	
	▫ Home directory		
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	

Manutenzione successiva all'installazione

Sono disponibili alcune utility per eseguire una manutenzione periodica sul database. Tali utility includono:

- Analyze Partitions (Analizza partizioni): consente di raccogliere statistiche sulle partizioni popolate di recente.
- Analyze Tables (Analizza tabelle): consente di raccogliere statistiche globali per gli eventi e le tabelle eventi correlate.
- Database Health Check (Controllo stato database): consente di raccogliere informazioni sul database. Viene visualizzato:
 - Consente di verificare se l'istanza del database è attiva
 - Consente di verificare se il listener Oracle è attivo
 - Consente di visualizzare l'utilizzo dello spazio
 - Consente di verificare l'esistenza di indici non utilizzabili
 - Consente di verificare l'esistenza di oggetti di database non validi
 - Consente di verificare l'esistenza di analisi di database

Per ulteriori informazioni, vedere la *sezione relativa alle procedure consigliate per la manutenzione del capitolo 2 – 'Procedure consigliate'*.

Con Sentinel viene fornita un'applicazione denominata Gestione dati Sentinel. Utilizzare questa applicazione per eseguire la gestione del database. Per ulteriori informazioni, vedere il *capitolo 10 – 'Gestione dati Sentinel'* della *Guida dell'utente di Sentinel*

C

Manutenzione relativa alle operazioni preliminari e successive all'installazione per il database Oracle in Linux

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Elenco di controllo relativo alle operazioni preliminari all'installazione

Questo elenco di controllo relativo alle operazioni preliminari all'installazione di Oracle è destinato principalmente alle installazioni distribuite. Può in ogni caso essere utilizzato per installazioni autonome. Se il numero di istanze di Gestione servizi di raccolta e del motore di correlazione è superiore a tre, prenderne nota. Questo elenco di controllo non consente un numero di istanze di Gestione servizi di raccolta e del motore di correlazione superiore a tre.

Per ulteriori informazioni, vedere il capitolo 3 "Installazione di Sentinel 5 per Oracle".

	Variabile di configurazione		
1.	<i>Versione di Sentinel:</i>		<i>Data attuale:</i>
	<i>Sistema operativo</i>		
	▪ Sistema operativo corretto per DB	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	▪ Patch corretta <input type="checkbox"/> : Sì <input type="checkbox"/> : No
	▫ Versione		▫ Livello patch
	▪ DB Oracle corretto con partizionamento	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	▪ Patch corretta <input type="checkbox"/> : Sì <input type="checkbox"/> : No
	▫ Versione		▫ Livello patch
	▪ Variabili di ambiente corrette impostate per l'utente del sistema operativo Oracle.	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	
	▪ Script di avvio (computer con il database)	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	
	▪ Processi (computer con il database)	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	
	▪ Socket	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	
	▪ Sistema operativo corretto per i componenti di Sentinel	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	▪ Patch corretta <input type="checkbox"/> : Sì <input type="checkbox"/> : No
2.	<i>Computer DAS</i>		
	▪ ID host		
	▪ numero di serie		
	▪ codice di licenza		

Variabile di configurazione		
3.	<i>Installazione DAS</i>	
	▪ Nome host o IP database	
	▪ Nome database	Valore di default: ESEC
	▪ Porta database	Valore di default: 1521
	▪ Ubicazione file JDBC	
4.	<i>Valori kernel UNIX per Oracle. I seguenti sono i valori minimi.</i>	
	▪ shmmax	2147483648 <input type="checkbox"/> : Sì <input type="checkbox"/> : No
		Valore se superiore:
	▪ shmmin	1 <input type="checkbox"/> : Sì <input type="checkbox"/> : No
		Valore se superiore:
	▪ shmseg	4096 <input type="checkbox"/> : Sì <input type="checkbox"/> : No
		Valore se superiore:
	▪ shmmni	400 <input type="checkbox"/> : Sì <input type="checkbox"/> : No
		Valore se superiore:
	▪ semmns	500 <input type="checkbox"/> : Sì <input type="checkbox"/> : No
		Valore se superiore:
	▪ semmni	1024 <input type="checkbox"/> : Sì <input type="checkbox"/> : No
		Valore se superiore:
	▪ semmsl	1024 <input type="checkbox"/> : Sì <input type="checkbox"/> : No
		Valore se superiore:
	▪ shmopm	100 <input type="checkbox"/> : Sì <input type="checkbox"/> : No
		Valore se superiore:
	▪ shmvmx	32767 <input type="checkbox"/> : Sì <input type="checkbox"/> : No
		Valore se superiore:
5.	<i>Istanza database (SID)</i>	
6.	<i>Nome database</i>	
7.	<i>Componenti di Sentinel:</i>	
	▪ Database di Sentinel (IP o DNS)	OS: Patch:
	▫ Log di installazione DB	
	▫ Memoria Oracle (RAM)	
	▫ Nome istanza	
	▫ Porta listener	Default: 1521
	▫ Password SYS	
	▫ Password di sistema	

Variabile di configurazione				
	▪ Communication Server (iSCALE) (IP o DNS)		OS: Patch:	
	▪ Servizi Sentinel di base (IP o DNS)		OS: Patch:	
	▪ DAS/Advisor (IP o DNS). Advisor è facoltativo		OS: Patch:	
	▫ RAM DAS			
	▪ Motore di correlazione (IP e sistema operativo)			
		▫ IP:		OS:
		▫ IP:		OS:
	▪ Crystal Server (IP o DNS)			
		▫ MS SQL (facoltativo, ma consigliato)	Versione di MS SQL: Patch di MS SQL: Password SA o contenitore o password:	
	▪ Generatore servizi di raccolta (IP o DNS, consigliata un'unica installazione)			
	▪ Gestione servizi di raccolta (servizi di raccolta)		NOTA: è possibile impostare Gestione servizi di raccolta senza l'uso di password.	
		▫ IP:	n/u:	PW: OS:
▫ IP:		n/u:	PW: OS:	
▫ IP:		n/u:	PW: OS:	
8.	<i>Advisor (facoltativo)</i>			
	▪ Ubicazione file feed di dati			
	▪ Indirizzo mittente Advisor			
	▪ Indirizzo destinatario Advisor			
	▪ Nome utente e password	n/u:	PW:	
9.	<i>Ubicazione file di database:</i>			
	▪ File di dati			
	▪ File di indice			
	▪ File di dati di riepilogo			
	▪ File di indice di riepilogo			
	▪ File dello spazio delle tabelle di annullamento e temporanei			
	▪ Directory log di ripetizione membro A			

	Variabile di configurazione	
	▪ Directory log di ripetizione membro A	
10.	Dimensioni database:	
	▪ Standard (20 GB)	
	▪ Grandi (400 GB)	
	▪ Personalizzate (dimensioni)	
11.	SMTP Server: (DNS o IP)	
12.	Password utente	
	▪ esecadm	PW:
	▫ Home directory	
	▪ esecapp	PW:
	▪ esecdba	PW:
	▪ esecrpt	PW:

Valore di default: /export/home

Manutenzione successiva all'installazione

Sono disponibili alcune utility per eseguire una manutenzione periodica sul database. Tali utility includono:

- Analyze Partitions (Analizza partizioni): consente di raccogliere statistiche sulle partizioni popolate di recente.
- Analyze Tables (Analizza tabelle): consente di raccogliere statistiche globali per gli eventi e le tabelle eventi correlate.
- Database Health Check (Controllo stato database): consente di raccogliere informazioni sul database. Viene visualizzato:
 - Consente di verificare se l'istanza del database è attiva
 - Consente di verificare se il listener Oracle è attivo
 - Consente di visualizzare l'utilizzo dello spazio
 - Consente di verificare l'esistenza di indici non utilizzabili
 - Consente di verificare l'esistenza di oggetti di database non validi
 - Consente di verificare l'esistenza di analisi di database

Per ulteriori informazioni, vedere la sezione relativa alle procedure consigliate per la manutenzione del *capitolo 2 – 'Procedure consigliate'*.

Con Sentinel viene fornita un'applicazione denominata Gestione dati Sentinel. Utilizzare questa applicazione per eseguire la gestione del database. Per ulteriori informazioni, vedere il *capitolo 10 – 'Gestione dati Sentinel'* della *Guida dell'utente di Sentinel*

D

Manutenzione preliminare e successiva all'installazione per il database MS SQL in Windows

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

NOTA: per gli utenti di MS SQL 2000, la dimensione degli eventi non può superare gli 8 KB.

Elenco di controllo relativo alle operazioni preliminari all'installazione

Questo elenco di controllo relativo alle operazioni preliminari all'installazione di MS SQL è destinato principalmente alle installazioni distribuite. Può in ogni caso essere utilizzato per installazioni autonome. Se il numero di istanze di Gestione servizi di raccolta e del motore di correlazione è superiore a tre, prenderne nota. Questo elenco di controllo non consente un numero di istanze di Gestione servizi di raccolta e del motore di correlazione superiore a tre.

Per ulteriori informazioni, vedere il *capitolo 4 "Installazione di Sentinel 5 per MS SQL"*.

	Variabile di configurazione		
1.	<i>Versione di Sentinel:</i>	<i>Data attuale:</i>	
	<i>Sistema operativo</i>		
	▪ Sistema operativo corretto per DB	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	▪ Patch corretta <input type="checkbox"/> : Sì <input type="checkbox"/> : No
	▪ DB SQL corretto	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	▪ Patch corretta <input type="checkbox"/> : Sì <input type="checkbox"/> : No
	▫ Versione		▫ Livello patch
	▪ Sistema operativo corretto per i componenti di Sentinel	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	▪ Patch corretta <input type="checkbox"/> : Sì <input type="checkbox"/> : No
2.	<i>Per l'installazione di DAS con un account di dominio di Windows, assegnare "Accesso come servizio"</i>	<input type="checkbox"/> : Sì <input type="checkbox"/> : No	
3.	<i>Computer DAS</i>		
	▪ ID host		
	▪ numero di serie		
	▪ codice di licenza		
4.	<i>IP o nome host database</i>	<i><nomehost>[/\<Nome istanza>]</i>	

	Variabile di configurazione		
5.	<i>Database Name:</i>		Valore di default: ESEC
6.	<i>Porta:</i>		Valore di default: 1433
7.	<i>Installazione SQL</i>	<input type="checkbox"/> : mista <input type="checkbox"/> : non mista	
8.	<i>Password SA o contenitore di password SQL server.</i>	PW:	
9.	<i>Componenti di Sentinel:</i>		
	▪ Database di Sentinel (IP o DNS)		OS: Patch:
	▪ Communication Server (iSCALE) (IP o DNS)		OS: Patch:
	▪ Servizi Sentinel di base (IP o DNS)		OS: Patch:
	▪ DAS/Advisor (IP o DNS). Advisor è facoltativo		OS: Patch:
	▪ Motore di correlazione (IP e sistema operativo)		
		IP:	OS:
		IP:	OS:
		IP:	OS:
	▪ Crystal Server (IP o DNS)		OS: Patch:
	▫ MS SQL (facoltativo, ma consigliato)	Versione di MS SQL: Patch di MS SQL: sa password or holder of password:	
	▪ Generatore servizi di raccolta (IP o DNS, consigliata un'unica installazione)		
	▪ Gestione servizi di raccolta (password servizi di raccolta w/ IP o DNS e sistema operativo)	NOTA: è possibile impostare Gestione servizi di raccolta senza l'uso di password.	
	▫ IP:	PW:	OS:
	▫ IP:	PW:	OS:
	▫ IP:	PW:	OS:
10.	<i>Advisor (facoltativo)</i>		
	▪ Ubicazione file feed di dati		
	▪ Indirizzo mittente Advisor		
	▪ Indirizzo destinatario Advisor		
	▪ Nome utente e password	n/u:	PW:

	Variabile di configurazione		
11.	<i>Ubicazione file di database:</i>		
	▪ File di dati		
	▪ File di indice		
	▪ File di dati di riepilogo		
	▪ File di indice di riepilogo		
	▪ File di log		
12.	<i>Dimensioni database:</i>		
	▪ Standard (20 GB)		
	▪ Grandi (400 GB)		
	▪ Personalizzate (dimensioni)		
13.	<i>SMTP Server: (DNS o IP)</i>		
14.	<i>Per autenticazione SQL (password)</i>		
	▪ esecadm	PW:	
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	
15.	<i>Per autenticazione Windows (password)</i>		
	▪ DBA (login)	n/u:	
	▪ Utente applicazione (login e password)	n/u:	PW:
	▪ Amministratore Sentinel (login)	n/u:	
	▪ Utente dei rapporti di Sentinel (login)	n/u:	

Manutenzione successiva all'installazione

Il sistema operativo Windows consente di archiviare automaticamente i dati e aggiungere partizioni: Per ulteriori informazioni, vedere la sezione relativa alle procedure consigliate per la manutenzione del *capitolo 2 – 'Procedure consigliate'*.

E

Pulitura manuale delle installazioni precedenti

NOTA: il termine agente è equivalente a servizio di raccolta. Si farà in seguito riferimento agli agenti come servizi di raccolta.

Quando si esegue un'installazione completa di Sentinel, è fortemente consigliabile eseguire tutti i passaggi seguenti per accertarsi che non rimangano file o impostazioni di sistema di una installazione precedente di Sentinel che potrebbero impedire l'esecuzione della nuova installazione. Eseguire passaggi seguenti su ogni computer sul quale si sta eseguendo una nuova installazione PRIMA di avviare il programma di installazione.

ATTENZIONE: 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.

Solaris

Pulitura manuale di Sentinel in Solaris

1. Eseguire il login come utente radice.
2. Accertarsi che non vi siano processi di Sentinel in esecuzione.
3. Rimuovere il contenuto di `/opt/sentinelXX` (o della directory in cui è stato installato e denominato il software di Sentinel)
4. Rimuovere i file seguenti dalla directory `/etc/rc3.d`:
 - S98sentinel
 - S99wizard
 - S99esyslogserver (v5.1.1.1)
 - S99esdee (se è installato il connettore SDEE)
5. Rimuovere i file seguenti dalla directory `/etc/rc0.d`:
 - K01wizard
 - K02sentinel
 - K01esdee (se è installato il connettore SDEE)
 - K01esyslogserver (v5.1.1.1)
6. Rimuovere i file seguenti dalla directory `/etc/init.d`:
 - sentinel
 - wizard
 - esdee (se è installato il connettore SDEE)
 - esyslogserver (v5.1.1.1)
7. Rimuovere i file seguenti dalla directory `/usr/local/bin`:
 - restart_wizard.sh

- stop_wizard.sh
 - start_wizard.sh
8. Pulire i riferimenti installshield in /var/sadm/pkg. Rimuovere i file seguenti 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)
 9. Rimuovere l'utente esecadm (e la home directory) e il gruppo esec. Prima di eseguire questa operazione verificare che non vi siano utenti che hanno eseguito il login come utente esecadm.
 - Eseguire: userdel -r esecadm
 - Eseguire: groupdel esec
 10. Rimuovere la sezione Installshield di /etc/profile, /etc/.login
 11. Rimuovere l'eventuale directory /InstallShield.
 12. Rimuovere il database Oracle di Sentinel seguendo le istruzioni illustrate nella sezione "Pulitura manuale del database Oracle di Sentinel in Solaris".
 13. Riavviare il sistema operativo.

Pulitura manuale del database Oracle di Sentinel in Solaris

1. In qualità di utente Oracle, arrestare il listener Oracle:
 - Eseguire: lsnrctl stop
2. Arrestare il database di Sentinel
 - Passare all'utente Oracle
 - Impostare la variabile di ambiente ORACLE_SID sul nome dell'istanza del database di Sentinel (in genere ESEC).
 - Eseguire: sqlplus '/ as sysdba'
 - Al prompt di sqlplus, eseguire: shutdown immediate
3. Rimuovere la voce relativa al database Sentinel nel file /var/opt/oracle/oratab
4. Rimuovere il file init<nome_istanza>.ora (in genere initESEC.ora) dalla directory \$ORACLE_HOME/dbs.
5. Rimuovere le voci dal database di Sentinel dai file seguenti nella directory \$ORACLE_HOME/network/admin:
 - tnsnames.ora
 - listener.ora
6. Eliminare i file di dati del database dall'ubicazione in cui si è scelto di installarli.

Linux

Pulitura manuale di Sentinel in Linux

1. Eseguire il login come utente radice.
2. Accertarsi che non vi siano processi di Sentinel in esecuzione.
3. Rimuovere il contenuto di /opt/sentinelXX (o della directory in cui è stato installato e denominato il software di Sentinel)

4. Rimuovere i file seguenti dalla directory /etc/rc5.d:
 - S98sentinel
 - S99wizard
 - S99esyslogserver (v5.1.1.1)
 - S99esdee (se è installato il connettore SDEE)
5. Rimuovere i file seguenti dalla directory /etc/rc3.d:
 - S98sentinel
 - S99wizard
 - S99esyslogserver (v5.1.1.1)
 - S99esdee (se è installato il connettore SDEE)
6. Rimuovere i file seguenti dalla directory /etc/rc0.d:
 - K01esyslogserver (v5.1.1.1)
 - K01wizard
 - K02sentinel
 - K01esdee (se è installato il connettore SDEE)
7. Rimuovere i file seguenti dalla directory /etc/init.d:
 - sentinel
 - wizard
 - esyslogserver (v5.1.1.1)
 - esdee (se il connettore SDEE è installato)
8. Rimuovere i file seguenti dalla directory /usr/local/bin:
 - restart_wizard.sh
 - stop_wizard.sh
 - start_wizard.sh
9. Rimuovere la directory /root/InstallShield
10. Rimuovere il file /root/vpd.properties
11. Rimuovere l'utente esecadm (e la home directory) e il gruppo esec. Prima di eseguire questa operazione verificare che non vi siano utenti che hanno eseguito il login come utente esecadm.
 - Eseguire: userdel -r esecadm
 - Eseguire: groupdel esec
12. Rimuovere la sezione Installshield di /etc/profile, /etc/.login
13. Rimuovere il database Oracle di Sentinel seguendo le istruzioni illustrate nella sezione “Pulitura manuale del database Oracle di Sentinel in Linux”.
14. Riavviare il sistema operativo.

Pulitura manuale del database Oracle di Sentinel in Linux

1. In qualità di utente Oracle, arrestare il listener Oracle:
 - Eseguire: lsnrctl stop
2. Arrestare il database di Sentinel
 - Passare all'utente Oracle
 - Impostare la variabile di ambiente ORACLE_SID sul nome dell'istanza del database di Sentinel (in genere ESEC).

- Eseguire: sqlplus '/ as sysdba'
 - Al prompt di sqlplus, eseguire: shutdown immediate
3. Rimuovere la voce relativa al database Sentinel nel file /etc/oratab
 4. Rimuovere il file init<nome_istanza>.ora (in genere initESEC.ora) dalla directory \$ORACLE_HOME/dbs.
 5. Rimuovere le voci dal database di Sentinel dai file seguenti nella directory \$ORACLE_HOME/network/admin:
 - tnsnames.ora
 - listener.ora
 6. Eliminare i file di dati del database dall'ubicazione in cui si è scelto di installarli.

Windows

Pulitura manuale di Sentinel in Windows

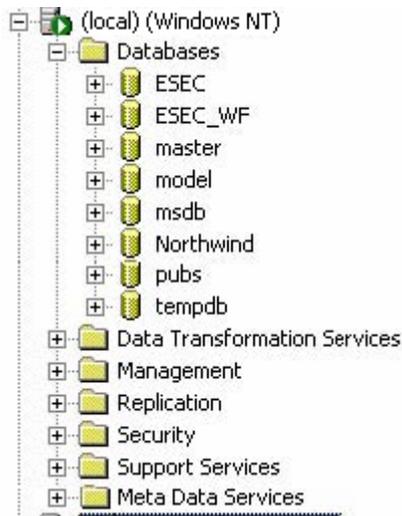
1. Eliminare la cartella C:\Programmi\File comuni\InstallShield\Universal e tutti i relativi componenti.
2. Eliminare la cartella della precedente installazione di Sentinel, ad esempio C:\Programmi\sentinel[%ESEC_HOME%).
3. Eliminare le variabili di ambiente seguenti, se esistenti, facendo clic con il pulsante destro del mouse su Risorse del computer, selezionare Proprietà, quindi fare clic sulla scheda Avanzate e selezionare il pulsante Variabili di ambiente:
 - ESEC_HOME
 - ESEC_VERSION
 - ESEC_JAVA_HOME
 - ESEC_CONF_FILE
 - WORKBENCH_HOME
4. Rimuovere tutte le voci nella variabile di ambiente Path che fanno riferimento a un'installazione precedente

ATTENZIONE: fare attenzione a rimuovere solo i percorsi delle installazioni precedenti di Sentinel. Se si rimuovono altre voci, il sistema potrebbe non funzionare correttamente.

5. Eliminare tutti i collegamenti a Sentinel nel desktop.
6. Eliminare la cartella dei collegamenti *Start > Programmi > Sentinel* dal menu Start.
7. Rimuovere il database Microsoft SQL Server seguendo le istruzioni illustrate nella sezione “*Pulitura manuale del database Microsoft SQL Server di Sentinel in Windows*”.
8. Riavviare il sistema operativo.

Pulitura manuale del database Microsoft SQL Server di Sentinel in Windows

1. Aprire Microsoft SQL Server Enterprise Manager e connettersi all'istanza di SQL Server in cui è installato il database Sentinel.
2. Espandere l'albero dei database e individuare il database Sentinel.



3. Per ogni database ESEC e ESEC_WF (o qualsiasi altro nome assegnato al database durante l'installazione), fare clic con il pulsante destro del mouse sul database, quindi scegliere "Elimina".
4. Quando richiesto, selezionare *Sì* per eliminare il database.

.archivio chiavi.....	13-1	installazione per Oracle	9-13
AES	13-1	massimizzazione della	
ARC4.....	13-1	generazione eventi	9-22, 10-11
cifratura	13-1	modelli	9-18, 10-6, 10-8
Advisor		operazioni preliminari all'installazione	
aggiornamento tabelle.....	11-3	(Linux).....	10-2
aggiornamento codice di licenza		panoramica dell'installazione per	
ID host (Linux).....	4-28	l'autenticazione di SQL Server.....	9-5
aggiornamento del codice di licenza.....	5-20	panoramica dell'installazione per	
ID host (Solaris).....	3-21	l'autenticazione di Windows.....	9-4
archivio chiavi.....	<i>Vedere</i> .archivio chiavi	panoramica dell'installazione per Oracle ...	9-5
ASP.NET		pubblicazione	9-18, 10-6, 10-8
installazione.....	9-4	uso.....	10-1
configurazione kernel Oracle su		deleteData	2-20
Red Hat Linux	4-4	disinstallazione di v4.2 (Solaris).....	6-5
configurazione kernel Oracle su		disinstallazione di v4.2 (Windows)	7-4
SuSE Linux	4-4	esempio	
Crystal (Linux)		DemoAssetUpload.....	12-6
avvio di Crystal Server	10-13	DemoEvents	12-5
avvio di MySQL	10-13	DemoVulnerabilityUpload	12-6
avvio di Tomcat	10-13	invio di un evento.....	12-1
connessione a MySQL	10-14	SendMultipleEvents.....	12-4
errore del nome host	10-13	SendOneEvent	12-4
reinizializzazione del database		esportazione	
MySQL.....	10-14	regole di correlazione	6-4, 7-4
Crystal Enterprise Launchpad		evento	
configurazione.....	9-20, 10-10	DemoAssetUpload - esempio.....	12-6
Crystal Reports		DemoEvents - esempio	12-5
uso	9-4	DemoVulnerabilityUpload - esempio	12-6
abilitazione dei primi 10 rapporti		invio di più eventi - esempio	12-4
di Sentinel (aggregazione).....	9-21, 10-10	invio di un evento - esempio.....	12-1
abilitazione dei primi 10		SendOneEvent - esempio	12-4
rapporti di Sentinel		Generatore servizi di raccolta.....	1-4
(EventFileRedirestService).....	9-21, 10-11	Gestione servizi di raccolta	1-4
applicazione di patch.....	9-16, 9-17	disinstallazione per Linux	15-1
aumentare al massimo la generazione		disinstallazione per Solaris	15-1
di rapporti di eventi	2-13	disinstallazione per Windows	15-1, 15-2
configurazione di Sentinel	9-23, 10-12	IIS	
connessione tra il server Web e il		installazione.....	9-4
database - test.....	9-20	impostazione del kernel Oracle	
connettività server Web	9-21, 10-9	in Solaris	3-4
conto Named User	9-20, 10-9	installazione	
inetmgr	9-16	aggiunta di componenti in Windows	14-2
installazione (Linux).....	10-4	aggiunta di componenti su Linux	14-1
installazione per autenticazione SQL	9-11	aggiunta di componenti su Solaris.....	14-1
installazione per autenticazione		applicazione di patch a Crystal.....	9-16, 9-17
Windows	9-6	configurazione kernel Oracle su	
		Red Hat Linux.....	4-4

configurazione kernel Oracle su SuSE Linux.....	4-4
creazione di un'istanza Oracle	3-21, 4-28
ID host (Linux).....	4-2
ID host (Solaris).....	3-2
ID host (Windows).....	5-2
IIS e ASP.NET.....	9-4
impostazione del kernel Oracle in Solaris.....	3-4
inetmger per Crystal Reports.....	9-16
installazione di Oracle in Red Hat Linux.....	4-8
installazione di Oracle in Solaris.....	3-5
installazione di Oracle in SuSE Linux.....	4-5
operazioni preliminari all'installazione – server Sentinel (Oracle)....	3-3, 4-4, 5-2, 5-3
operazioni preliminari all'installazione – server Sentinel (Windows).....	5-4
requisiti della patch di Solaris.....	3-4
server Sentinel (personalizzata) - Linux ...	4-15
server Sentinel (personalizzata) - Windows	5-7
Server Sentinel (semplice) - Linux.....	4-12
server Sentinel (semplice) - Solaris.....	3-6, 3-9
server Sentinel (semplice) - Windows	5-5
server Sentinel in Solaris.....	14-2
server Sentinel su Linux	14-1
server Sentinel su Solaris.....	14-1
Wizard in Solaris	14-2
Wizard su Linux.....	4-12, 4-15, 14-1
Wizard su Solaris	3-6, 3-9, 14-1
Installazione di Oracle in Red Hat Linux	4-8
Installazione di Oracle in Solaris	3-5
Installazione di Oracle in SuSE Linux	4-5
iSCALE.....	13-1
livello di comunicazione	
AES.....	<i>Vedere</i> .archivio chiavi
ARC4.....	<i>Vedere</i> .archivio chiavi
metodi di cifratura	
abilitazione	13-1
modifica.....	13-1
migrazione di dati	
Solaris	6-12
Windows.....	7-12
modifiche alle chiavi	13-1
Motore del servizio di raccolta	1-4
Novell	
sito Web	1-10
supporto tecnico.....	1-10

ODBC	
autenticazione di SQL	9-12
autenticazione Windows.....	9-10
impostazione di un'origine dati	9-10, 9-12
Open Database Configuration.....	<i>Vedere</i>
ODBC, <i>Vedere</i> ODBC	
operazioni preliminari alla migrazione	
disinstallazione di v4.2 (Solaris)	6-5
disinstallazione di v4.2 (Windows).....	7-4
esportazione di regole di correlazione	6-4, 7-4
installazione del database di Sentinel 5 (Solaris)	6-6
installazione del database di Sentinel 5 (Windows).....	7-5
operazioni successive alla migrazione	
impostazioni ODBC per Crystal Reporting (Windows)	6-16, 7-16
installazione di Sentinel 5 (Solaris).....	6-15
installazione di Sentinel 5 (Windows)	7-15
modelli di Crystal Report (Windows).....	6-17, 7-16
Oracle	
configurazione di Net Service Name	9-15
creazione di un'istanza	3-21, 4-28
istanza	3-21, 4-28
procedure consigliate	
aggiunta di partizioni.....	2-17
analisi	2-14
archiviazione di dati	2-17
assegnazioni LUN MS SQL.....	2-7
backup di database	2-8
configurazione di MS SQL.....	2-6
Configurazione di rete	2-8
correlazione – aggiornamento di trigger ...	2-22
correlazione – controllo del tempo.....	2-22
correlazione – espressioni booleane	2-22
correlazione – formato libero	2-22
correlazione – regole di correlazione avanzate	2-22
Crystal – ottimizzazione della creazione di rapporti su eventi	2-13
directory di dati	2-8
directory di dati di riepilogo	2-8
directory di indice.....	2-8
directory di indice riepiloghi	2-8
directory di log	2-8
directory di spazi delle tabelle di annullamento	2-8
directory log di ripetizione membro A	2-8
directory log di ripetizione membro B	2-8
directory temporanea.....	2-8
gruppi di memorizzazione di MS SQL	2-7

gruppi RAID di MS SQL RAID	2-7
log	2-23
log delle transazioni	2-23
Log delle transazioni	2-8
motore di correlazione	2-21
parametri	2-10
patch di database	2-9
pulitura disinstallazione	2-11
RAID Oracle	2-8
Redo log	2-8
registrazione nell'archivio	2-8
spazio delle tabelle	2-10
verifica stato database	2-16
proprietà di esecuzione	3-19, 4-26
regole di correlazione	
esportazione	6-4, 7-4
Sentinel	
disinstallazione per Linux	15-1
disinstallazione per Solaris	15-1
disinstallazione per Windows	15-1, 15-2
installazione in Windows	14-2
installazione personalizzata su Linux	4-15
installazione semplice su Linux	4-12
installazione semplice su Solaris	3-6, 3-9
installazione su Linux	14-1
installazione su Solaris	14-1
Servizio di raccolta	1-4
spazio delle tabelle	3-21, 4-28
upgrade	
aggiornamento delle autorizzazioni di gestione utenti in Solaris (da v5.0.x a v5.1.2)	7-20
aggiornamento delle autorizzazioni di gestione utenti in Solaris (da v5.0.x a v5.1.3)	6-18
aggiornamento delle autorizzazioni di visualizzazione server in Windows	7-20
aggiornamento di una voce di configurazione menu	6-19
da v5.1.1.1 a v5.1.3 (Linux)	8-1
da v5.x.x a v5.1.2 (autenticazione di SQL)	7-17
da v5.x.x a v5.1.2 (autenticazione di Windows)	7-18
da v5.x.x a v5.1.3 (Solaris)	6-17
disinstallazione di v4.2 (Solaris)	6-5
disinstallazione di v4.2 (Windows)	7-4
esportazione di regole di correlazione	6-4, 7-4
impostazioni 5 per Crystal Reporting (Windows)	7-16
impostazioni ODBC per Crystal Reporting (Windows)	6-16
installazione del connettore syslog (Linux)	8-2
installazione del connettore syslog (Solaris)	6-18
installazione del connettore syslog (Windows)	7-20
installazione del database di Sentinel 5 (Solaris)	6-6
installazione del database di Sentinel 5 (Windows)	7-5
installazione di Sentinel 5 (Solaris)	6-15
installazione di Sentinel 5 (Windows)	7-15
migrazione di dati (Solaris)	6-12
migrazione di dati (Windows)	7-12
modelli di Crystal Report (Windows)	6-17, 7-16
rimozione del connettore syslog (Linux)	8-2
rimozione del connettore syslog (Solaris)	6-18
rimozione del connettore syslog (Windows)	7-19
Wizard	
installazione in Windows	14-2
installazione su Linux	4-12, 4-15, 14-1
installazione su Solaris	3-6, 3-9, 14-1