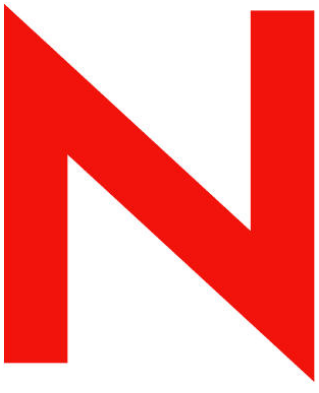
Novell® Sentinel™

5.1.3

7 luglio 2006

www.novell.com

Volume V - GUIDA ALL'INTEGRAZIONE CON SOLUZIONI DI TERZE PARTI



Novell®

Note legali

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 ://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 ://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.

Sommario

Prefazione

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

La documentazione tecnica di Sentinel è suddivisa in cinque 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™
- Volume V : Guida all'integrazione con soluzioni di terze parti di Sentinel™ 5

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™ 5

In questa guida vengono descritti gli argomenti seguenti:

- Funzionamento della console Sentinel
- Funzioni di Sentinel
- Architettura di Sentinel
- Comunicazione di Sentinel
- Valutazione delle vulnerabilità
- Monitoraggio degli eventi
- Filtraggio 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 manutenzione dei servizi di raccolta

Volume IV: Guida di riferimento dell'utente

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 del database di Sentinel

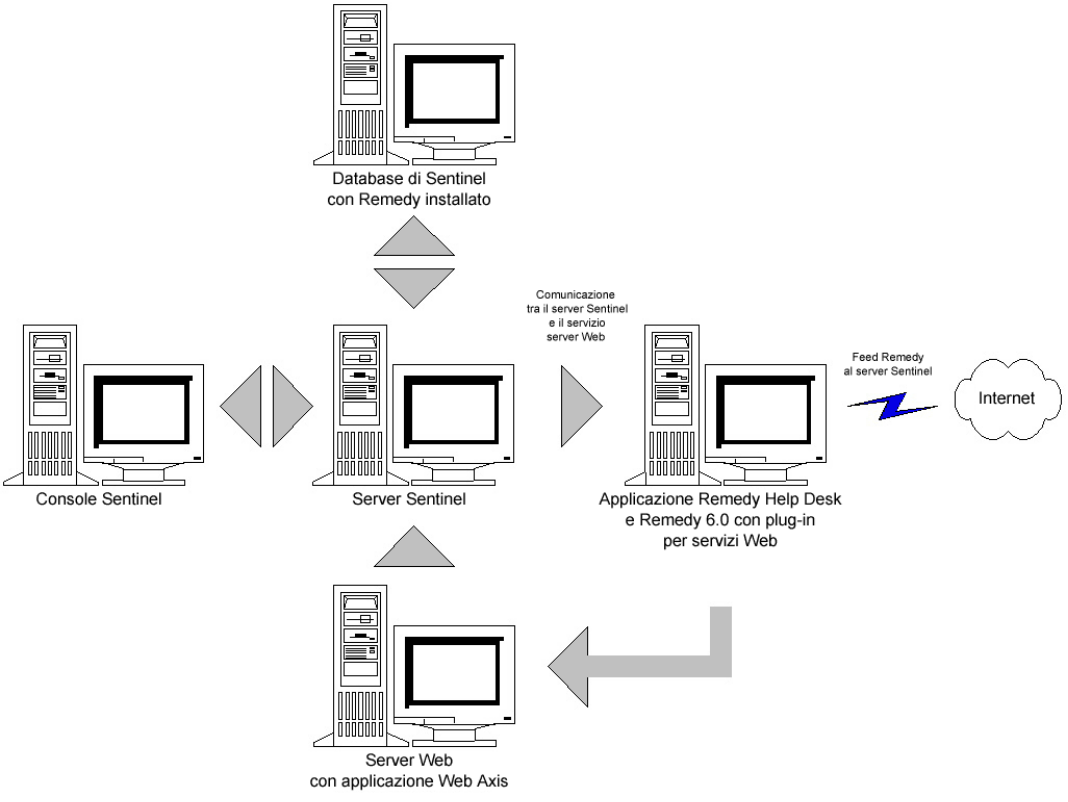
Volume V: Guida all'integrazione con soluzioni di terze parti

- Remedy
- HP OpenView Operations
- HP Service Desk

1 Remedy Integration

Remedy Integration per Sentinel v4.2 o v5 può essere utilizzato per creare applicazioni workflow integrate sia con Remedy Trouble Ticketing System sia con il sistema Sentinel. Le principali funzioni di Remedy Integration sono:

- Creazione di un nuovo caso in Remedy Help Desk sulla base di un caso di Sentinel.Aggiornamento di un caso in Help Desk quando viene aggiornato un caso correlato di Sentinel.
- Aggiornamento di un caso di Sentinel quando viene aggiornato un caso correlato in Help Desk.



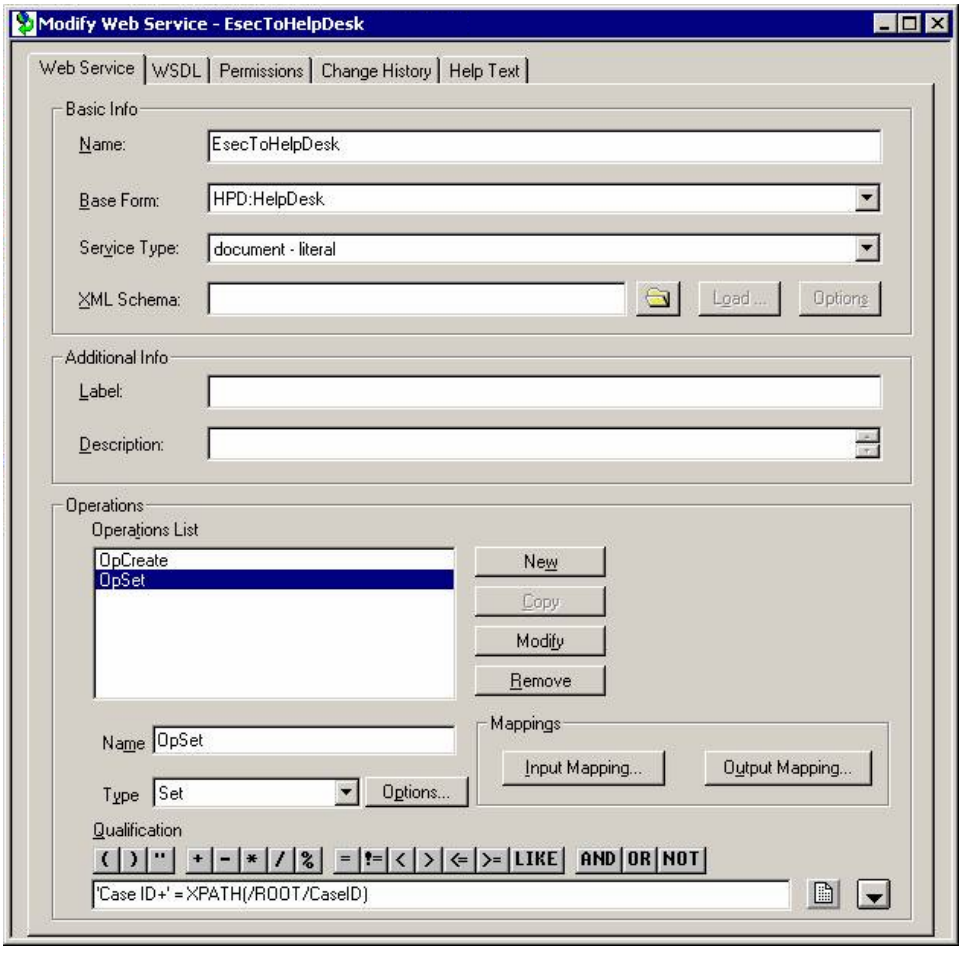
Configurazione

Per modificare il modulo dei casi di Remedy Help Desk

1. Eseguire il login a *Remedy Administrator* (*Amministratore di Remedy*) > (*Moduli*), quindi fare doppio clic su *HPD HelpDesk*.
2. Per poter supportare l'integrazione con Sentinel, è necessario aggiungere un campo di testo (EsecIncidentId) e di pool di allegati (Attachment Pool) al modulo dei casi di Help Desk. Queste voci verranno utilizzate per aggiungere allegati di casi di Sentinel al modulo.
3. Per aggiungere il campo di testo EsecIncidentId:
   - Fare clic sul pulsante New Character Field (Nuovo campo di testo), quindi posizionare il campo all'interno del modulo.
   - Impostare un'etichetta nella scheda Display (Visualizza).
   - Nel campo Name (Nome) della scheda Database, impostare il nome EsecIncidentID.
4. Per aggiungere il campo di testo pool di allegati con i tre campi seguenti: EsecEvents, EsecVuln e EsecAdv.
   - Fare clic sul pulsante *Create Attachment Pool* (*Crea pool di allegati*).
   - Nel campo etichetta della scheda Visualizza, immettere il nome relativo all'etichetta (ad esempio, esec allegati esec).
   - In Attach Fields (Allega campi), nel campo 'Enter Attachments Field LabelImmetti etichetta campi allegati), immettere:
     - EsecEvent, quindi fare clic su Add (Aggiungi).
     - EsecVuln, quindi fare clic su Add (Aggiungi).
     - EsecAdv, quindi fare clic su Add (Aggiungi).
5. Fare clic su *Save* (*Salva*).

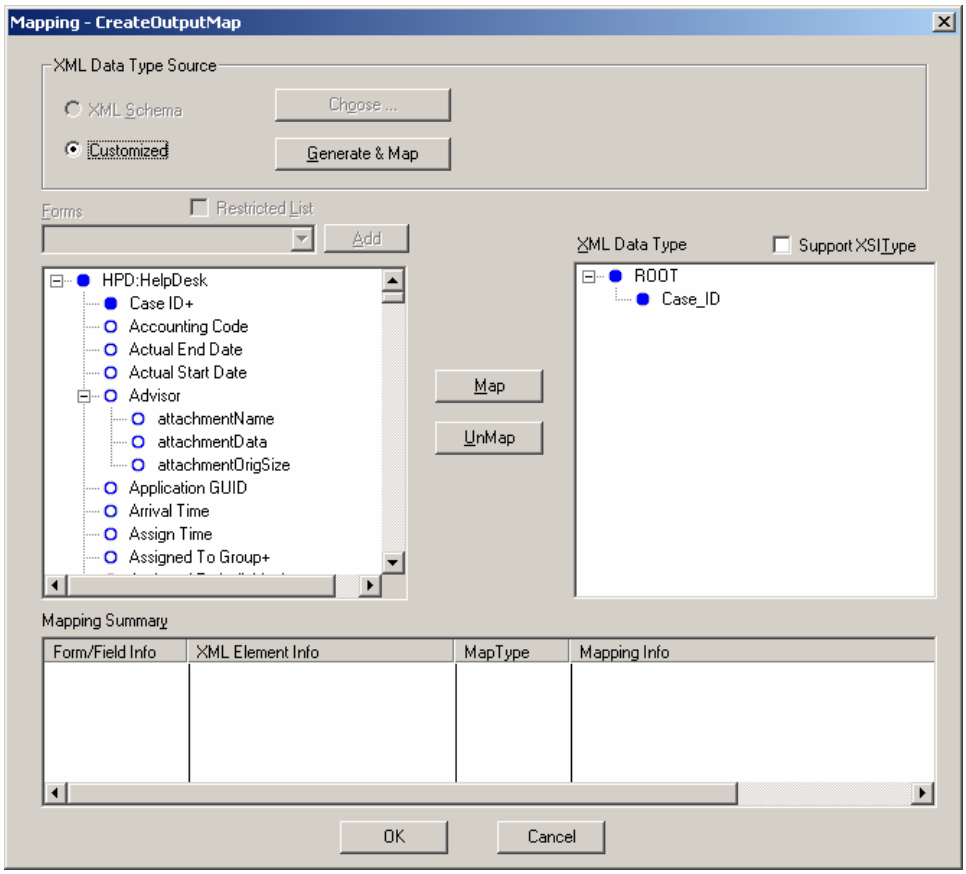
Creazione del servizio Web

1. Selezionare Web Services (Servizi Web) nel riquadro di spostamento di Remedy Administrator. Fare clic con il pulsante destro del mouse su New Web Services (Nuovi Servizi Web), quindi fare clic sulla scheda Web Services (Servizi Web).



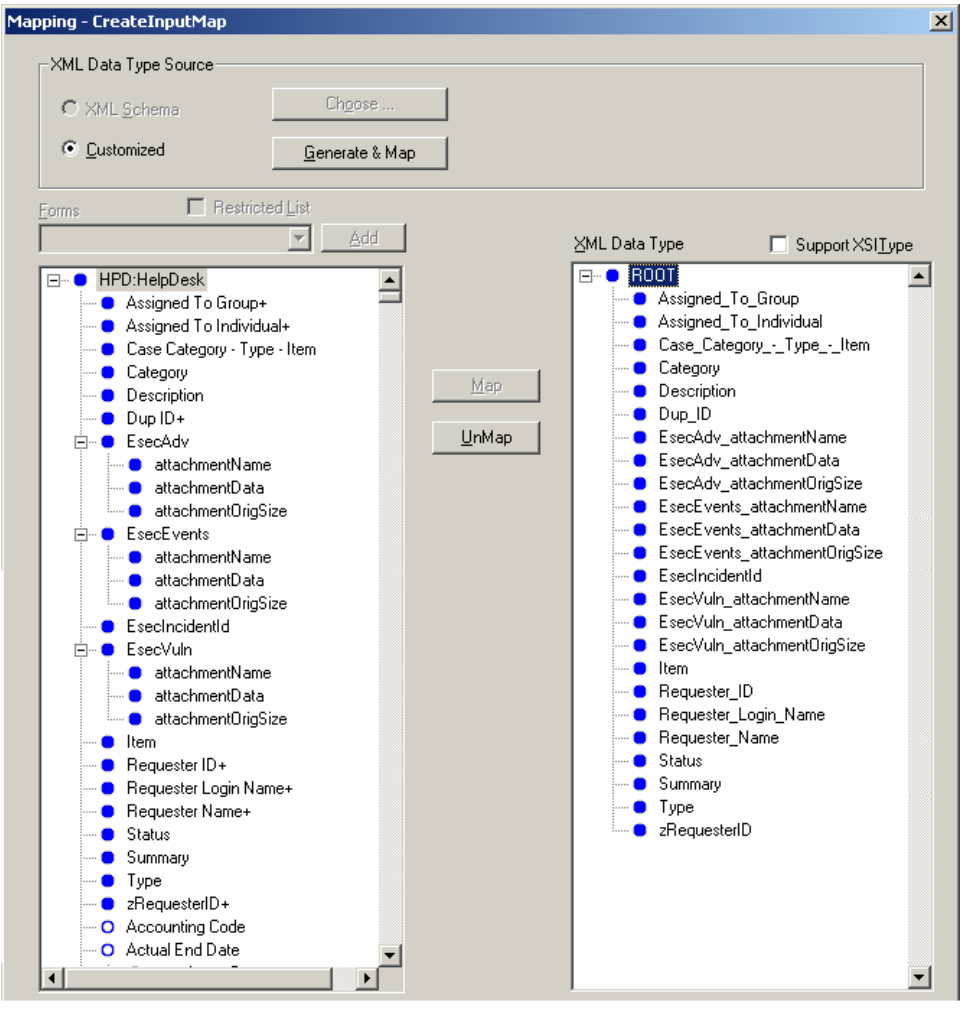
2. Utilizzando il modulo Case (Caso) di Help Desk come modello, creare un Servizio Web con il nome EsecToHelpDesk, quindi selezionare HPD HelpDesk nel campo Base Form (Modulo base).
3. Selezionare le due operazioni seguenti per il servizio Web:
   - OpCreate
   - OpSet

   Rimuovere tutte le altre operazioni.
4. Selezionare l'operazione OpCreate, quindi fare clic sul pulsante Output Mapping (Mappatura di output). Impostare la schermata in modo che corrisponda alla figura seguente.


Mapping - CreateOutputMap
XML Data Type Source
XML Schema
Choose ...
Customized
Generate & Map
Forms
Restricted List
Add
HPD:HelpDesk
Case ID+
Accounting Code
Actual End Date
Actual Start Date
Advisor
attachmentName
attachmentData
attachmentOrigSize
Application GUID
Arrival Time
Assign Time
Assigned To Group+
Map
UnMap
XML Data Type
Support XSIType
ROOT
Case_ID
Mapping Summary
Form/Field Info
XML Element Info
MapType
Mapping Info
OK
Cancel

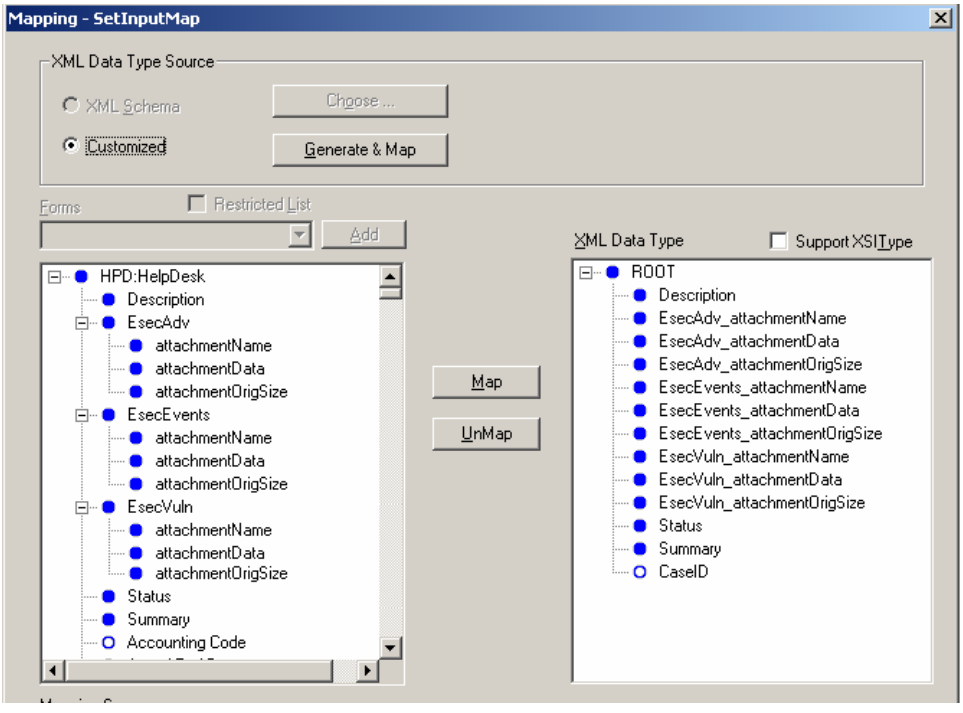
Selezionare l'operazione OpCreate, quindi fare clic sul pulsante Input Mapping (Mappatura di input). Configurare la schermata come illustrato nella figura.

NOTA: per rimuovere un elemento, selezionarlo, fare clic con il pulsante destro del mouse e scegliere Taglia.

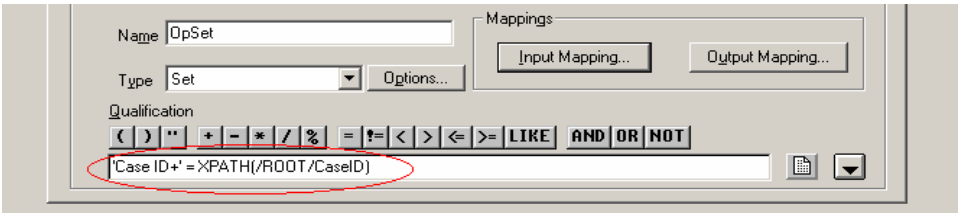


Fare clic su *Save* (*Salva*).

Selezionare l'operazione OpSet, quindi fare clic sul pulsante Input Mapping (Mappatura di input). Configurare la schermata come illustrato nella figura.



Il pulsante Output Mapping (Mappatura di output) non è disponibile per questa operazione. È necessario specificare una qualifica:



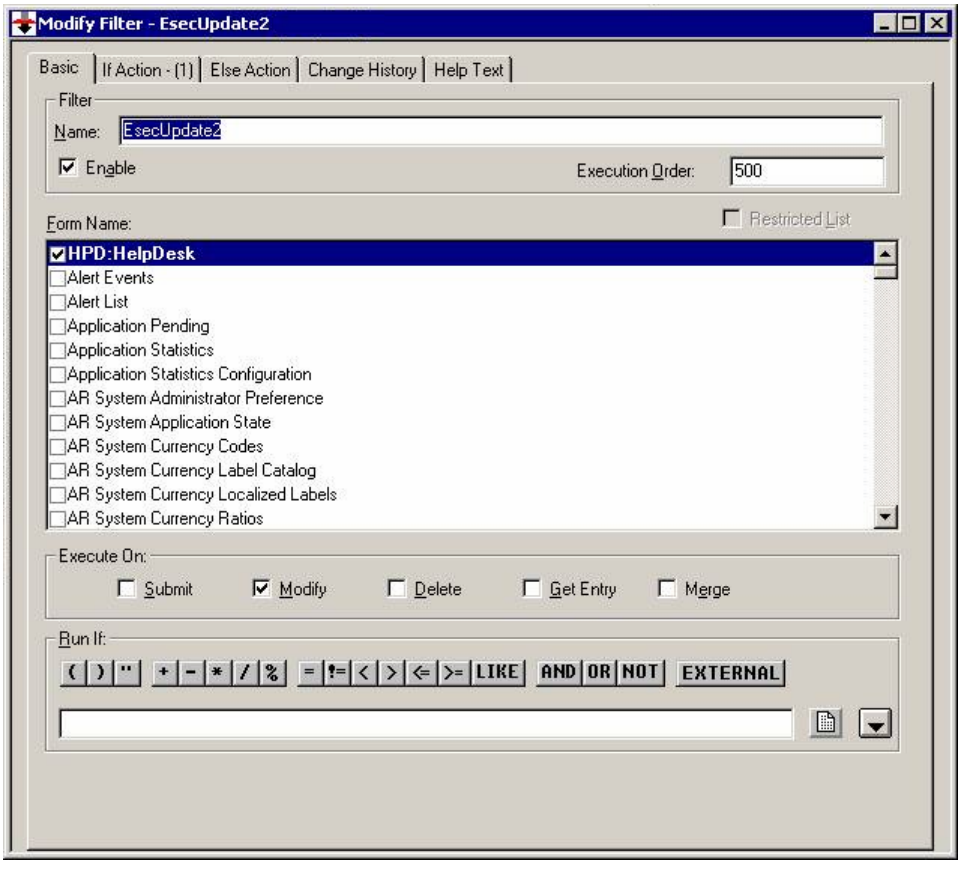
5. Passare alla scheda Autorizzazioni e rendere il servizio pubblico, spostando la relativa descrizione dal riquadro di sinistra a quello di destra. Fare clic su Salva.

Flusso di dati da Remedy a Sentinel

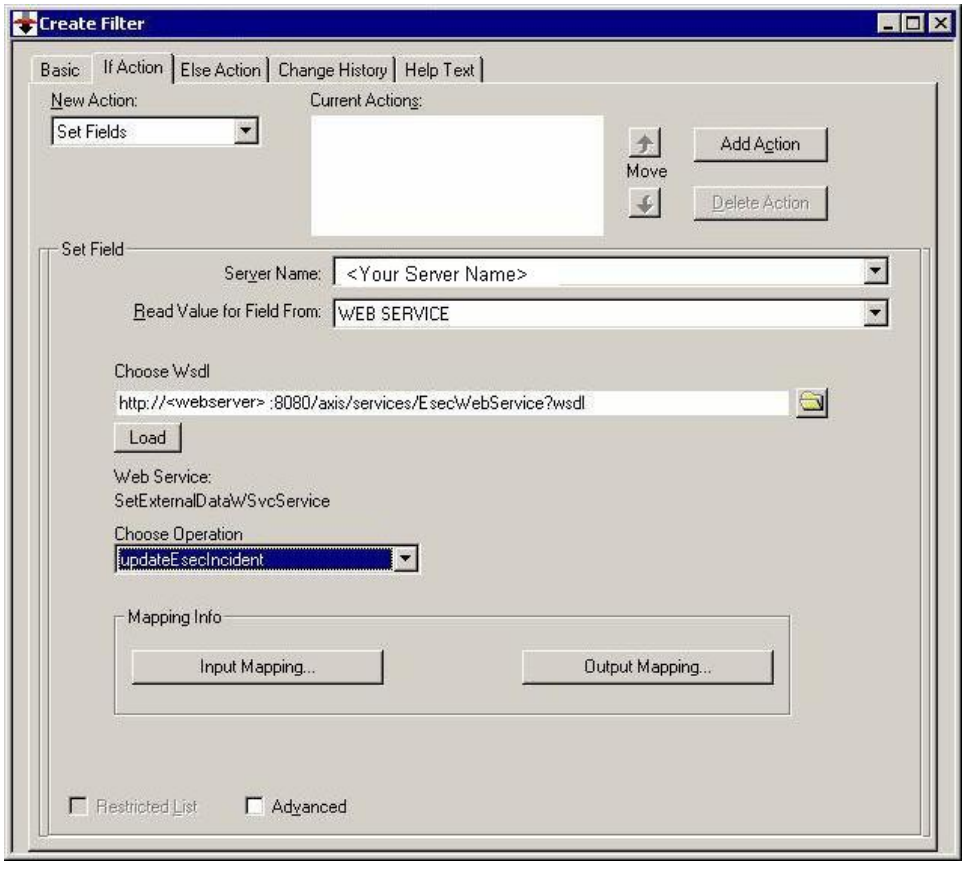
Per poter accedere al Servizio Web di Sentinel, è necessario che all'avvio del server Sentinel l'applicazione Web Axis sia installata sul server Web in uso.

Flusso di dati da Remedy a Sentinel

1. In Remedy Administrator selezionare Filters (Filtri), quindi fare clic con il pulsante destro del mouse su *Add Filter* (*Aggiungi filtro*).
2. Creare un filtro per il modulo Case (Caso) di Help Desk, il quale verrà eseguito in un evento modificato. Verificare che la schermata corrisponda alla figura seguente.

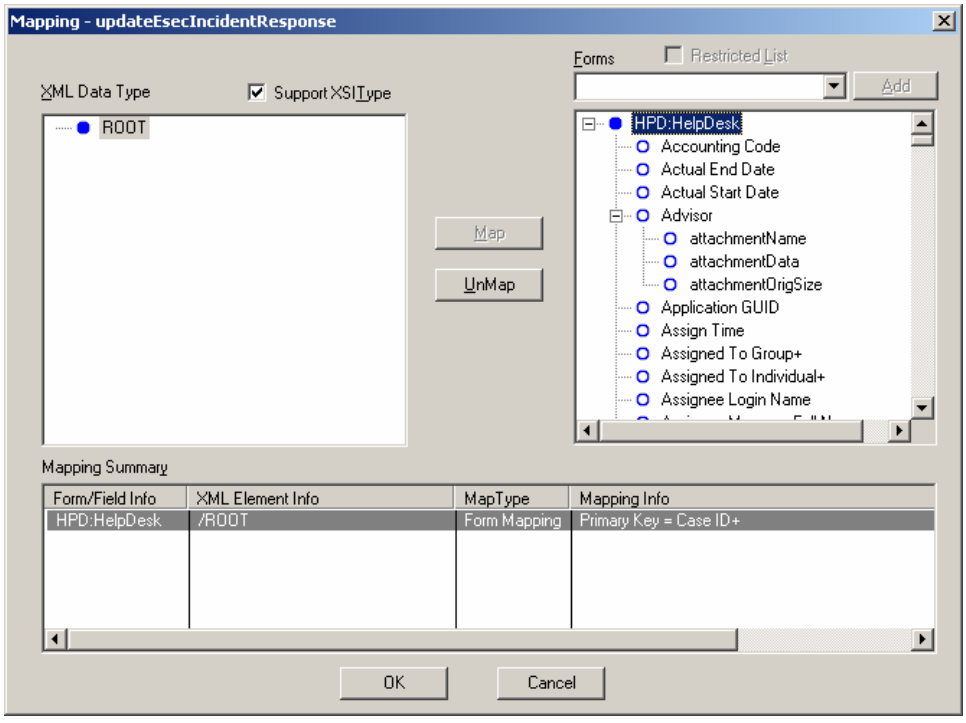


3. Nel menu a discesa *New Action* (*Nuova azione*) della scheda *If Action* (*Azione IF*), selezionare l'azione *Set field* (*Imposta campi*). Nel riquadro corrispondente selezionare *WEB SERVICE* (*SERVIZIO WEB*), quindi indicare l'URL per il servizio Web di Sentinel (http://<IP del server Web oppure nome DNS>:8080/axis/services/EsecWebService?wsdl).



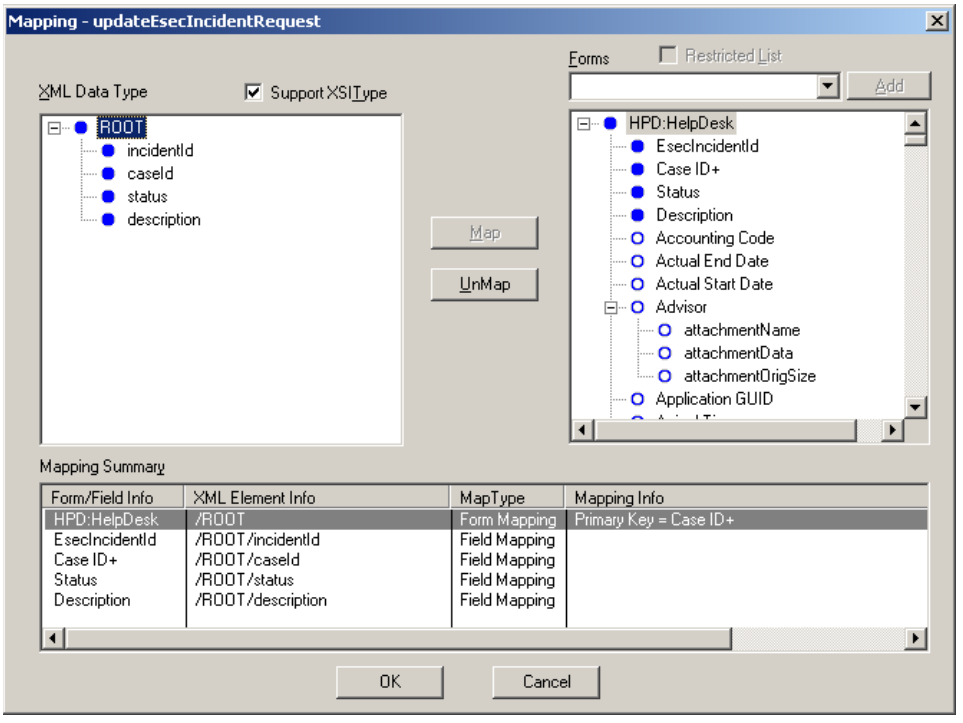
4. Nel menu a discesa *Choose Operation* (*Scegliere un'operazione*), selezionare il metodo updateEsecIncident e impostare le mappature di input e output.

Fare clic sul pulsante Output Mapping (Mappatura di output). Configurare la schermata come illustrato nella figura.



Fare clic sul pulsante Input Mapping (Mappatura di input). Configurare la schermata come illustrato nella figura.

NOTA: per impostare la mappatura, selezionare una voce a sinistra (ovvero, incidentId), quindi una voce a destra (ovvero, EsecIncidentId) e fare clic sul pulsante Map (Mappatura).



NOTA: in seguito a questa configurazione, ogni volta che si salva una modifica nel modulo Case (Caso) di Help Desk, tale modifica verrà inoltrata a un servizio Sentinel.

5. Fare clic su *Save* (*Salva*).

Installazione di Sentinel

Per poter installare Sentinel con Remedy, è necessario disporre di un conto Remedy in cui è necessario immettere le informazioni seguenti.

NOTA: è necessario disporre dell'autorizzazione Remedy Integration.

- Nome utente
- Password
- Nome richiedente
- ID richiedente
- Login richiedente
- Nome gruppo (non obbligatorio)
- Nome individuale (non obbligatorio)
- Nome server
- Nome servizio

Per quanto riguarda il flusso di dati da Remedy a Sentinel verranno richiesti i dati seguenti:

- Server Web Sentinel (<nome computer:porta>)
- Nome utente Sentinel (ad esempio, esecadm)
- ID utente Sentinel
- UUID Sentinel
- ID blocco Sentinel (di norma impostato su 1 o 2)

Installazione di Sentinel

1. Durante l'installazione selezionare Remedy Integration.
2. È consigliabile tenere queste informazioni a portata di mano durante l'installazione.

Configurazione del flusso di dati da Remedy a Sentinel

Se si decide di utilizzare un'integrazione di terze parti (Remedy Integration), è consigliabile eseguire l'installazione e la configurazione nell'ordine seguente:

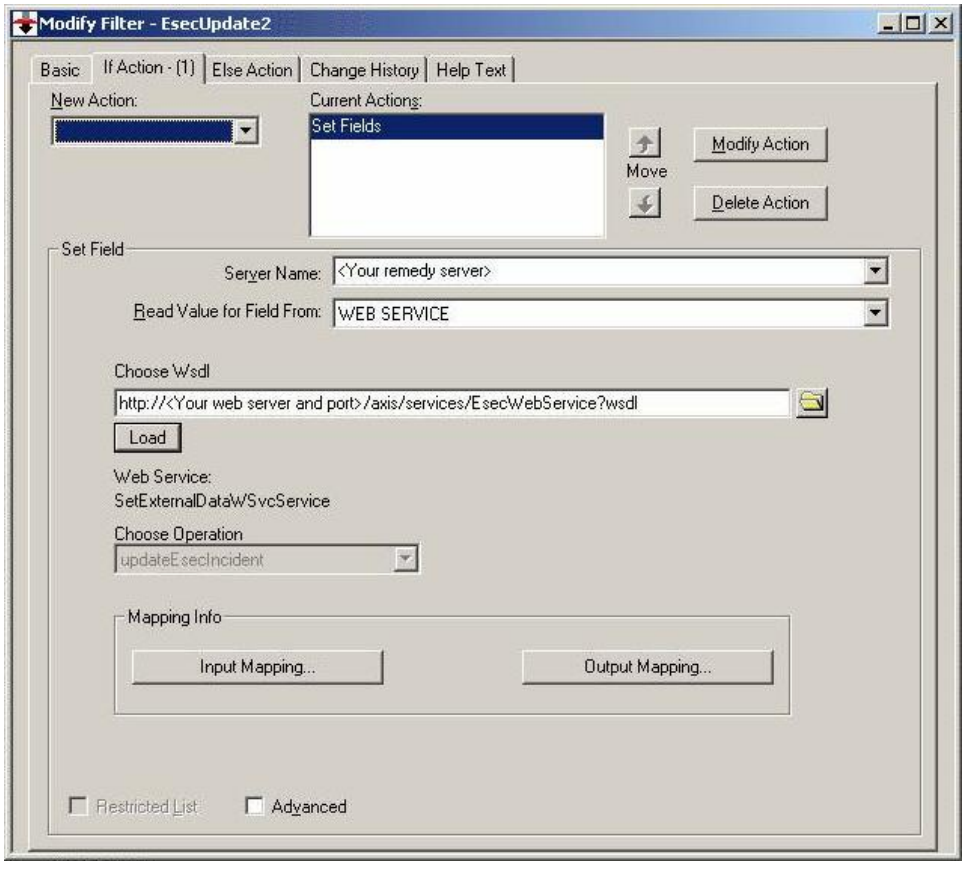
- Installare l'applicazione Remedy Help Desk e Remedy 6.0 con i plug-in dei servizi Web.
- Configurare i nuovi filtri e i servizi Web in Remedy Help Desk.
- Installare Sentinel.

Per avviare il flusso di dati da Remedy a Sentinel eseguire la procedura seguente:

- Per poter accedere al Servizio Web di Sentinel, è necessario che l'applicazione Web Axis sia installata sul server Web in uso, prima di avviare il server Sentinel.
- Copiare tutti i file con estensione jar dall'ubicazione seguente nel server Sentinel in <applicazione web axis>\webclient\lib:
  - %ESEC_HOME%\lib
  - %ESEC_HOME%\sentinel\console
  - %ESEC_HOME%\communicator (solo per v4.2)
- Copiare i file configuration.xml e .keystore del server Sentinel in un'ubicazione a propria scelta nel server Web. Entrambi i file si trovano in %ESEC_HOME%.
  - Modificare il file configuration.xml nel proprio server Web affinché punti al file .keystore.
  - Aggiungere l'opzione JVM seguente al server Web:

    ```
    Dcom.esecurity.configurationfile=<percorso file
       configuration.xml>\configuration.xml
    ```

- È necessario creare un filtro per il modulo Case (Caso) di Help Desk, il quale verrà eseguito in un evento "Modificato". Il server Web Sentinel viene richiamato attraverso questo filtro.


Modify Filter - EsecUpdate2
Basic
If Action - (1)
Else Action
Change History
Help Text
New Action:
Current Actions:
Set Fields
Move
Modify Action
Delete Action
Set Field
Server Name:
<Your remedy server>
Read Value for Field From:
WEB SERVICE
Choose Wsdl
http://<Your web server and port>/axis/services/EsecWebService?wsdl
Load
Web Service:
SetExternalDataWSvcService
Choose Operation
updateEsecIncident
Mapping Info
Input Mapping...
Output Mapping...
Restricted List
Advanced

2 Operazioni di Remedy Help Desk

È possibile utilizzare Remedy Integration per creare applicazioni di workflow.
In Remedy Integration sono disponibili le funzioni seguenti:

- Creazione di un nuovo caso in Remedy Help Desk sulla base di un caso di Sentinel.
- Aggiornamento di un caso in Help Desk quando viene aggiornato un caso correlato di Sentinel.
- Aggiornamento di un caso di Sentinel quando viene aggiornato un caso correlato in Help Desk.

Operazioni di Remedy Help Desk

Invio di un caso per Remedy Help Desk (versione 5.0.1 e successive)

1. Fare clic sulla scheda Casi.
2. Nel riquadro di navigazione espandere la cartella Visualizzazioni casi, quindi evidenziare Gestione visualizzazione caso.

   NOTA: se si è già impostato un caso per un altro sistema esterno, non è possibile modificarlo.

3. Espandere una delle visualizzazioni di casi, quindi fare doppio clic sul caso desiderato. Il caso verrà aperto.
4. Fare clic sul pulsante Remedy.

   Per aggiornare il caso, selezionare la scheda Dati esterni, quindi il pulsante Remedy.

Aggiornamento di un caso in Remedy Help Desk (versione 5.0.1. e successive)

5. Fare clic sulla scheda *Casi*.
6. Espandere il riquadro di navigazione a sinistra, quindi fare doppio clic su un caso impostato in Remedy Help Desk.
7. Fare clic sul pulsante *Remedy* nel caso. L'annotazione verrà aggiunta nella scheda Esterni

Riconfigurazione manuale delle impostazioni di interfaccia di Remedy

Durante la prima installazione dell'interfaccia di Remedy Help Desk, le impostazioni di Remedy vengono memorizzate nel file das_query.xml. Per modificare queste impostazioni al termine dell'installazione, consultare le informazioni riportate in questa sezione del documento.

Impostazioni di Remedy

Le impostazioni di Remedy vengono memorizzate nel componente RemedyARServerService del file das_query.xml come illustrato di seguito:

Reimpostazione della password di Remedy

Le password di Remedy vengono memorizzate in formato cifrato nel file das_query.xml. Per reimpostare le password memorizzate in questo file, è quindi necessario utilizzare l'utility descritta di seguito.

Per reimpostare la password dell'interfaccia di Remedy.

8. Passare alla directory %ESEC_HOME%/sentinel/bin/
9. Immettere:

```
extconfig -n das_query.xml [-r password_remedy]
```

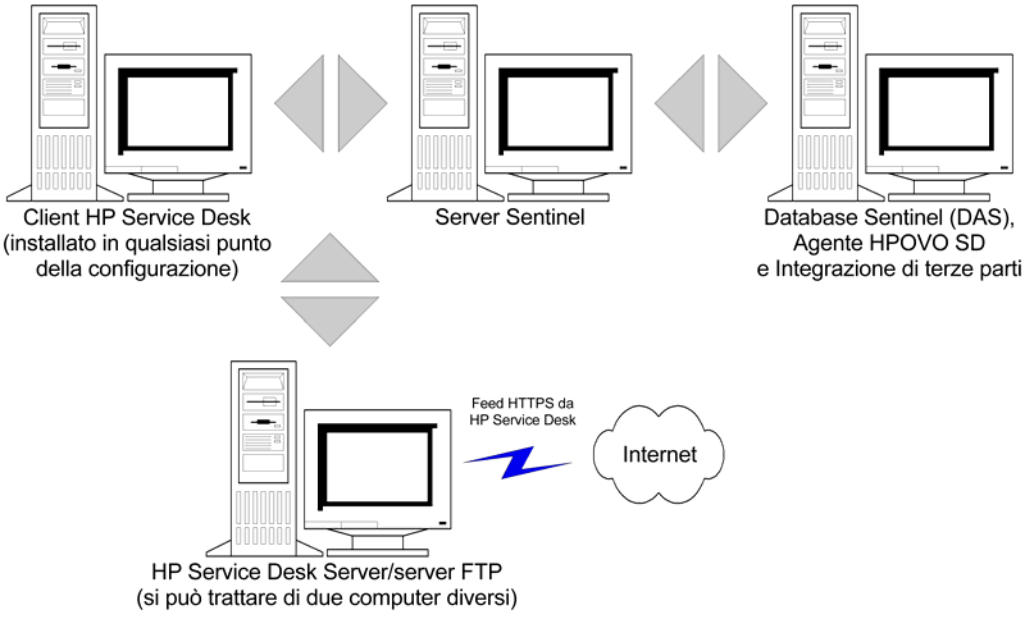
   - -r corrisponde alla password di Remedy

3 Installazione di HP OpenView Service Desk per Windows

L'integrazione bidirezionale di Sentinel con HP OpenView Service Desk, concesso in licenza separatamente, fornisce nuove importanti funzionalità alla console Sentinel. Sentinel sfrutta le funzionalità di gestione delle risorse di HP OpenView Service Desk per reperire informazioni di riferimento che consentano di rispondere in modo più efficace a minacce e attacchi alla sicurezza. Le nuove funzionalità consentono di:

- Inviare uno o più casi a HP Service Desk (SD)
- Allegare uno o più eventi a un caso HP SD
- Allegare informazioni sulle vulnerabilità a un caso HP SD
- Interrogare e inserire le informazioni sugli elementi di configurazione (risorse) nel caso della console Sentinel e in SD
- Eseguire l'integrazione round-trip: SD invia gli aggiornamenti a Novell che li invia a SD
- Aggiornare lo stato del caso SD dalla console Sentinel di Novell
- Aggiornare lo stato del caso di Sentinel da HP SD

Di seguito viene illustrata una configurazione di installazione tipica. La configurazione specifica può essere diversa.



Requisiti del sistema

Per conoscere i requisiti hardware e software di HP OpenView Service Desk Client, Server e Agent, fare riferimento alla guida all'installazione di HP OpenView Service Desk.

Sentinel supporta le versioni seguenti di HP OpenView Service Desk:

- HP OpenView Service Desk Server - Versione 4.5 con Service Pack 8 (4.5.0588.0802 SP 8)
- HP OpenView Service Desk Client - Versione 4.5 con Service Pack 8
- HP OpenView Service Desk Agent - Versione 4.5 con Service Pack 8
- Sentinel 4.2.1.8 o 4.2.1.15 per Windows
- Qualsiasi server FTP di terze parti

HP OpenView Service Desk (Server e Client) deve essere installato in un computer destinato a fungere da Service Desk Server. Per assistenza sull'installazione di Service Desk, consultare la guida all'installazione di HP OpenView Service Desk.

Per attivare l'interfaccia bidirezionale, è necessario installare HP OpenView Agent nello stesso computer in cui è installato il file das_cmd.bat. L'interfaccia bidirezionale consente di notificare in Sentinel da parte di HP Service desk le eventuali modifiche allo stato di un caso originato da Sentinel e apportate da un utente Service Desk. I casi devono essere originati nella console Sentinel.

Per consentire a Service Desk di gestire gli allegati, è necessario installare un server FTP (in genere in Service Desk Server) e configurare Service Desk in modo da permettere la comunicazione con il server. È possibile utilizzare qualsiasi server FTP di terze parti. Per assistenza sull'installazione del server FTP, consultare la relativa guida all'installazione.

Installazione

Se si installa anche HP OpenView Operations, è consigliabile installare HP OpenView Operations prima di HP OpenView Service Desk.

NOTA: durante la prima installazione di HP OpenView Service Desk Interface di terze parti, le impostazioni Service Desk e OpenView vengono memorizzate nel file das_query.xml. Per modificare una di queste impostazioni (come il nome utente o la password), fare riferimento a *Operation - HP OpenView and Service Desk for Windows 2000 (Funzionamento: HP OpenView e Service Desk per Windows 2000).*

È consigliabile installare i componenti nell'ordine seguente:

- FTP Server

  NOTA: per assistenza sull'installazione del server FTP, consultare la relativa guida all'installazione.

- HP OpenView Service Desk Server con Service Pack 8 (lo stesso del server FTP)
- HP OpenView Service Desk Client con Service Pack 8
- HP OpenView Service Desk Agent con Service Pack 8 (per abilitare l'interfaccia bidirezionale): deve essere installato nello stesso computer in cui è installato DAS

  NOTA: per assistenza sull'installazione del software HP OpenView Service Desk, fare riferimento alla guida all'installazione di HP OpenView Service Desk.

- Installare l'integrazione di terze parti di Sentinel
  - HP OpenView Service Desk

NOTA: per informazioni sull'installazione, fare riferimento alle Note di rilascio di Sentinel v4.2.1.8 e alla guida all'installazione di Sentinel v4.2 per Windows e Solaris.

Configurazione di HP OpenView Service Desk

La configurazione di HP OpenView Service Desk viene eseguita tramite Service Desk Client. Prima di modificare la configurazione di HP Service Desk per la comunicazione con il server FTP, assicurarsi di disporre delle informazioni seguenti:

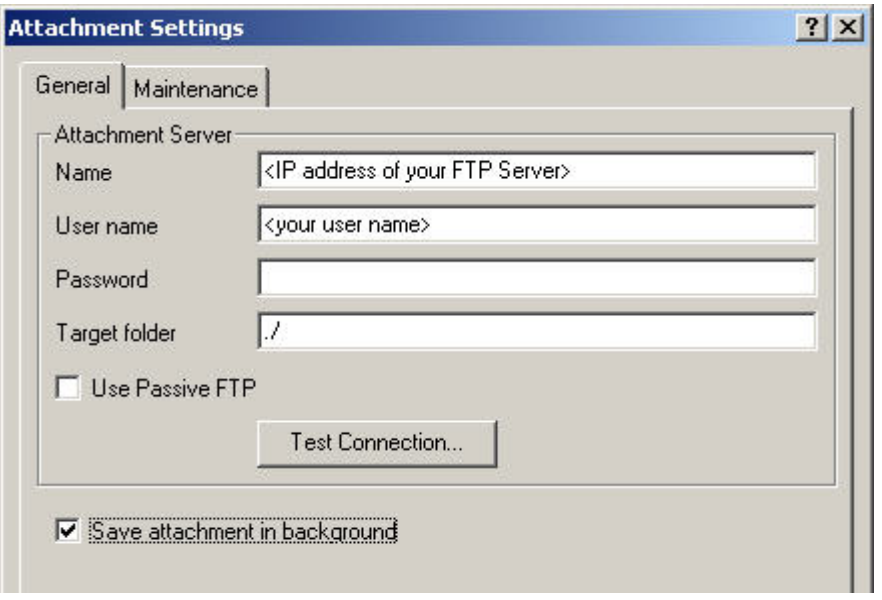
- Nome: indirizzo IP del server FTP
- Nome utente/Password: qualsiasi utente impostato nel server FTP
- Cartella di destinazione: è consigliabile digitare "./". In questo modo, la directory FTP viene posizionata nella directory FTP corrente.
- Deselezionare l'opzione Use Passive FTP (Utilizza FTP passivo).
- Selezionare l'opzione Save attachment in background (Salva allegato in background).

NOTA: per ulteriori informazioni sulla procedura di configurazione, fare riferimento alla sezione relativa ai task successivi all'installazione nella guida all'installazione di HP OpenView Service Desk.

Per configurare le impostazioni degli allegati

1. Avviare HP Service Desk Client.
2. Fare clic su *Tools* (*Strumenti*) > *System* (*Sistema*).
3. Fare clic su *System Panel* (*Pannello di sistema*) nel riquadro di navigazione a sinistra.
4. Fare doppio clic su *Attachment Settings* (*Impostazioni allegato*). Immettere:
   - Nome: indirizzo IP del server FTP
   - Nome utente/Password: qualsiasi utente impostato nel server FTP
   - Cartella di destinazione: è consigliabile digitare "./". In questo modo, la directory FTP viene posizionata nella directory FTP corrente.
   - Deselezionare l'opzione *Use Passive FTP* (Utilizza FTP passivo).
   - Selezionare l'opzione *Save attachment in background* (*Salva allegato in background*).

NOTA: per ulteriori informazioni sulla procedura di configurazione, fare riferimento alla sezione relativa ai task successivi all'installazione nella guida all'installazione di HP OpenView Service Desk.



5. Fare clic su *Test Connection* (*Test di connessione*).
6. Fare clic su *Apply* (*Applica*) e quindi su *OK*.

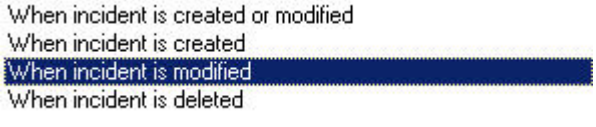
Attivazione di Service Desk sull'interfaccia (bidirezionale) di Sentinel

L'interfaccia bidirezionale consente a HP OVO OpenView Service Desk di notificare a Sentinel eventuali modifiche allo stato di un caso (originato da Sentinel) apportate da un utente Service Desk. Ciò consente di tenere traccia dello stato corrente di ogni caso che sia stato inviato in precedenza a HP OVO OpenView Service Desk.

Per attivare questa funzionalità, è necessario installare HP OVO OpenView Service Agent nello stesso computer in cui è installato Sentinel (das_cmd.bat). Ciò consente a HP Service Desk di eseguire l'utility das_cmd di Sentinel.

Attivazione dell'interfaccia bidirezionale

1. Avviare Service Desk Client.
2. Visualizzare la console dell'amministratore selezionando *Tool* (*Strumenti*) > *System* (*Sistema*).
3. Fare clic su Business Logic (Logica applicativa) nel riquadro di navigazione a sinistra.
4. Fare doppio clic su *Database Rules* (*Regole database*).
5. Fare doppio clic su *Incident* (*Caso*). Verrà visualizzata una finestra in cui sono elencate le regole del database.
6. Fare clic con il pulsante destro del mouse nel riquadro Database Rules (Regole database), quindi scegliere *New Database Rule* (*Nuova regola database*).
7. Evidenziare l'opzione *When incident is modified* (*Quando si modifica il caso*) e fare clic su *Next* (*Avanti*).

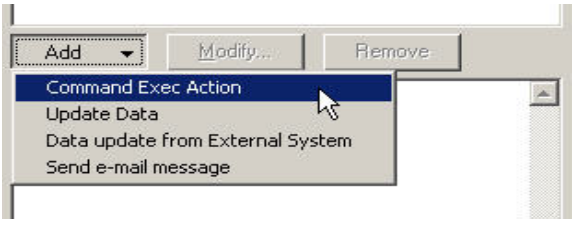


8. Fare clic sul pulsante *Condition*…(*Condizione*).

9. Fare clic sul pulsante *Add Criterion…* (*Aggiungi criterio*).
10. Fare clic sul pulsante *Quick Find* (*Ricerca rapida*), quindi selezionare *Status* (*Stato*) e is anything (qualsiasi valore) nel campo dell'operatore.

Fare clic due volte su *OK*.

11. Selezionare l'opzione *Command Exec Action* (*Azione exec comando*).



12. Aggiungere una nuova azione del comando Exec in modo tale che lo script "das_cmd.bat" venga eseguito nel server Sentinel ogni volta che viene valutata la regola.

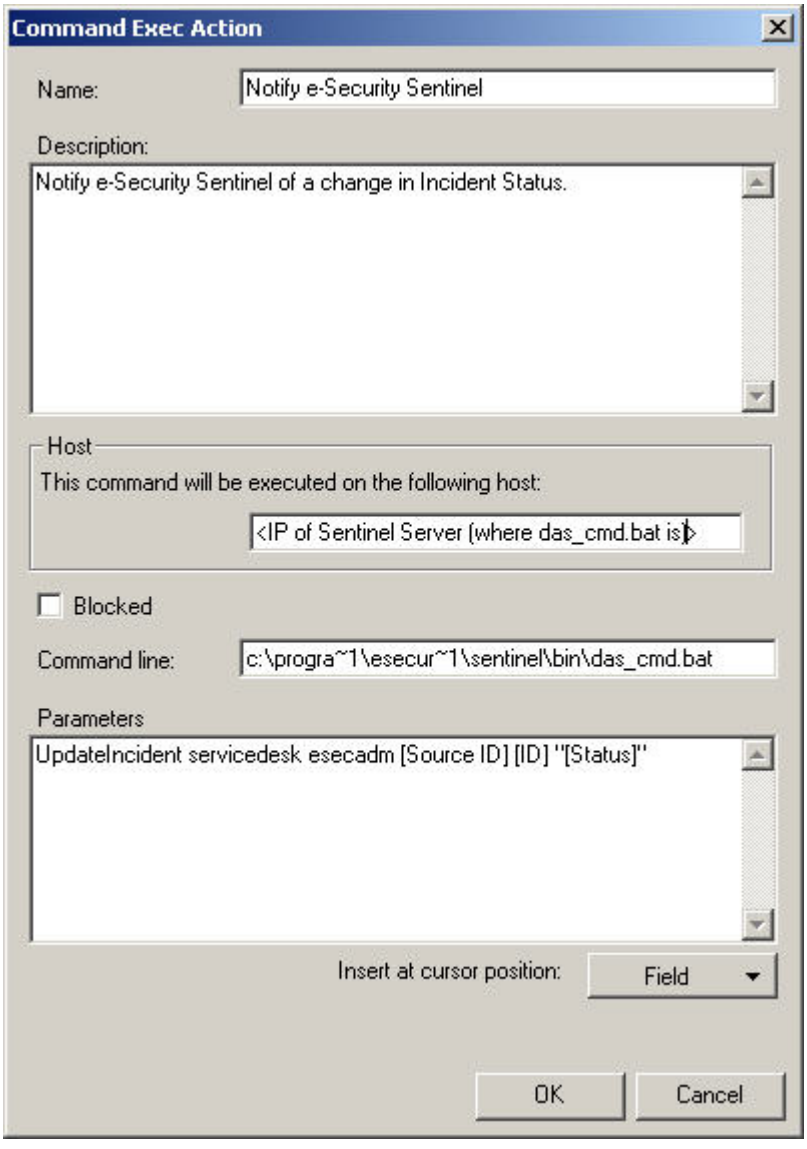
    Durante la configurazione dell'azione, assicurarsi di specificare il nome (o l'indirizzo IP) del server Sentinel (computer in cui si trova das_cmd.bat) come computer host. Accertarsi inoltre di specificare il percorso completo del file "das_cmd.bat" nel server Sentinel nella riga di comando, come:

    ```
    c:\progra~1\esecur~1\sentinel\bin\das_cmd.bat
    ```

NOTA: è necessario utilizzare la convenzione di denominazione dei file DOS 8.3 per specificare i nomi delle directory con gli spazi. Utilizzare ad esempio "progra~1" anziché "Programmi".

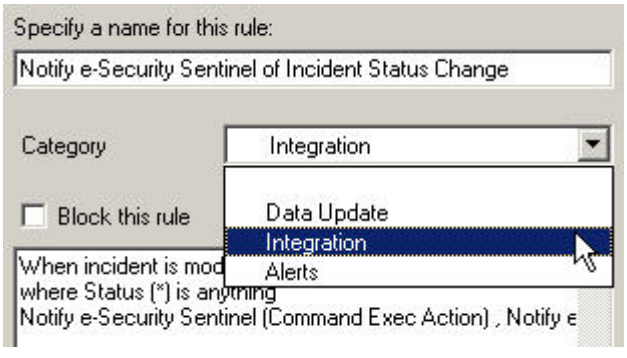
Infine assicurarsi di specificare l'azione Parameters (Parametri) come:

```
UpdateIncident servicedesk esecadm [Source ID] [ID]
   "[Status]"
```



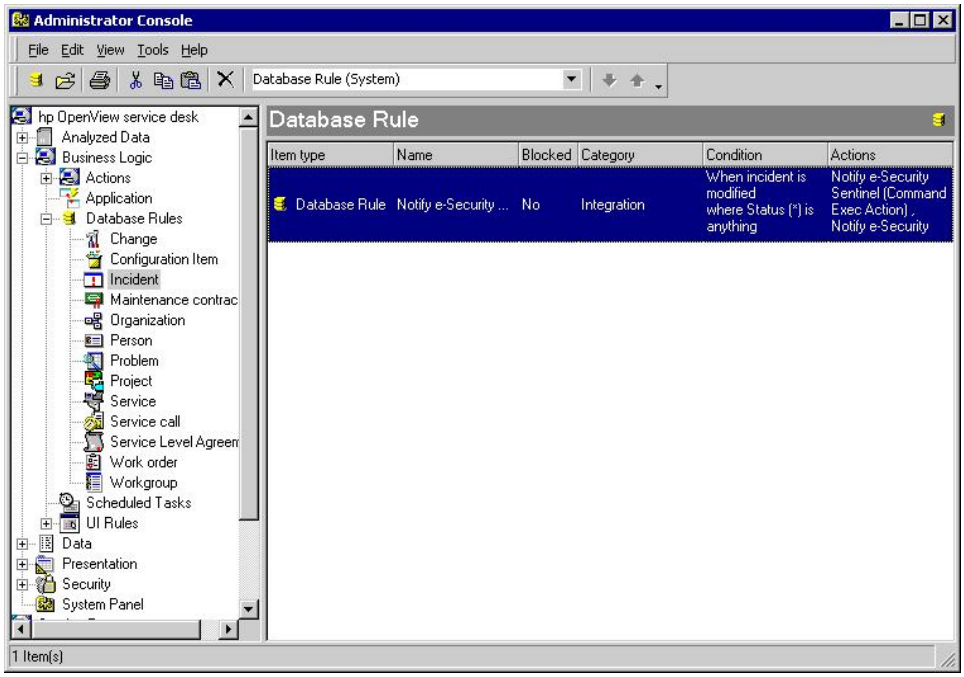
Assegnare un nome descrittivo alla nuova regola del database. Fare clic su OK, quindi su Next (Avanti).

13. Nel campo Category (Categoria), selezionare Integration (Integrazione) e specificare un nome per questa regola. Non selezionare l'opzione *Block this rule* (*Blocca la regola*).



Fare clic su *Fine*.

14. Una volta completata, la nuova regola sarà aggiunta all'elenco delle regole del database.



4 Integrazione di HP OpenView Service Desk

HP OpenView Service Desk per Sentinel consente di inviare casi da una schermata che visualizza casi ed eventi a HP OpenView Service Desk.

HP OpenView Service Desk

L'integrazione di Sentinel con HP OpenView Service Desk fornisce nuove importanti funzionalità per la gestione delle risorse che consentono di eseguire le operazioni seguenti:

- Inviare uno o più casi a HP Service Desk (SD)
  - Allegare uno o più eventi a un caso HP SD
  - Allegare informazioni sulle vulnerabilità a un caso HP SD
  - Allegare informazioni di Advisor a un caso HP SD
  - Interrogare e inserire le informazioni sugli elementi di configurazione (risorse) nella console di Sentinel Control
- Aggiornare lo stato del caso SD dalla console di Sentinel Control
- Aggiornare lo stato del caso di Sentinel da HP SD

Le informazioni sul caso di Sentinel inviate a HP OpenView Service Desk includono:

- ID del caso Sentinel
- Stato
- Titolo
- Annotazioni/Cronologia
- Casi (allegato)
- Informazioni sulla vulnerabilità (allegato)
- Informazioni di Advisor (allegato)

Durante l'invio o la ricezione di informazioni da HP OpenView Service Desk, si verificano operazioni di stato automatico, mappatura dello stato e conversione.

Nella tabella seguente sono riportati la mappatura e la conversione degli stati da Sentinel a Service Desk:

Stato di Sentinel	Stato di Service Desk
Aperto	Registrato
Riconosciuto	In attesa
Assegnato	Informato
In fase di analisi	In corso
Falso positivo	Chiuso
Verificato	Completato
Approvato	In corso
Chiuso	Chiuso

Nella tabella seguente sono riportati la mappatura e la conversione degli stati da Service Desk a Sentinel:

Stato di Service Desk	Stato di Sentinel
Registrato	Aperto
In corso	In fase di analisi
In attesa	Riconosciuto
Completato	Verificato
Informato	Assegnato
Chiuso	Chiuso

Invio di uno o più casi a HP OpenView Service Desk

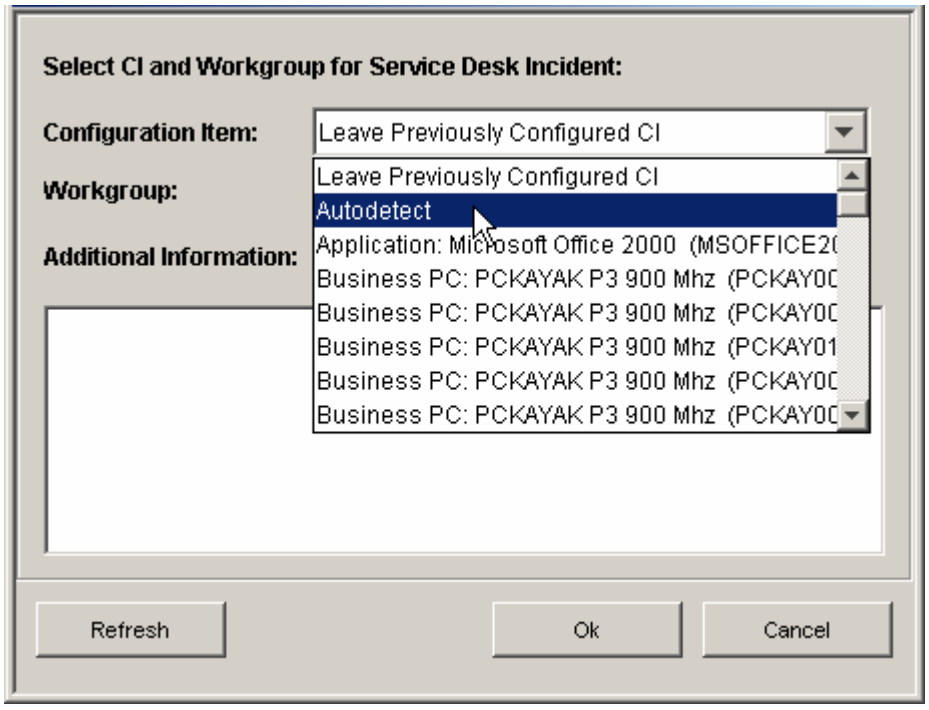
Invio di un caso a HP OpenView Service Desk

1. Fare clic sulla scheda *Casi*.
2. Nel riquadro di navigazione espandere la cartella *Visualizzazioni casi*, quindi evidenziare *Gestione visualizzazione caso*.

   NOTA: se si è già impostato un caso per un altro sistema esterno, non è possibile modificarlo.

3. Espandere una delle visualizzazioni di casi, quindi fare doppio clic sul caso desiderato. Il caso verrà aperto.
4. Fare clic sul pulsante *HP SD*.

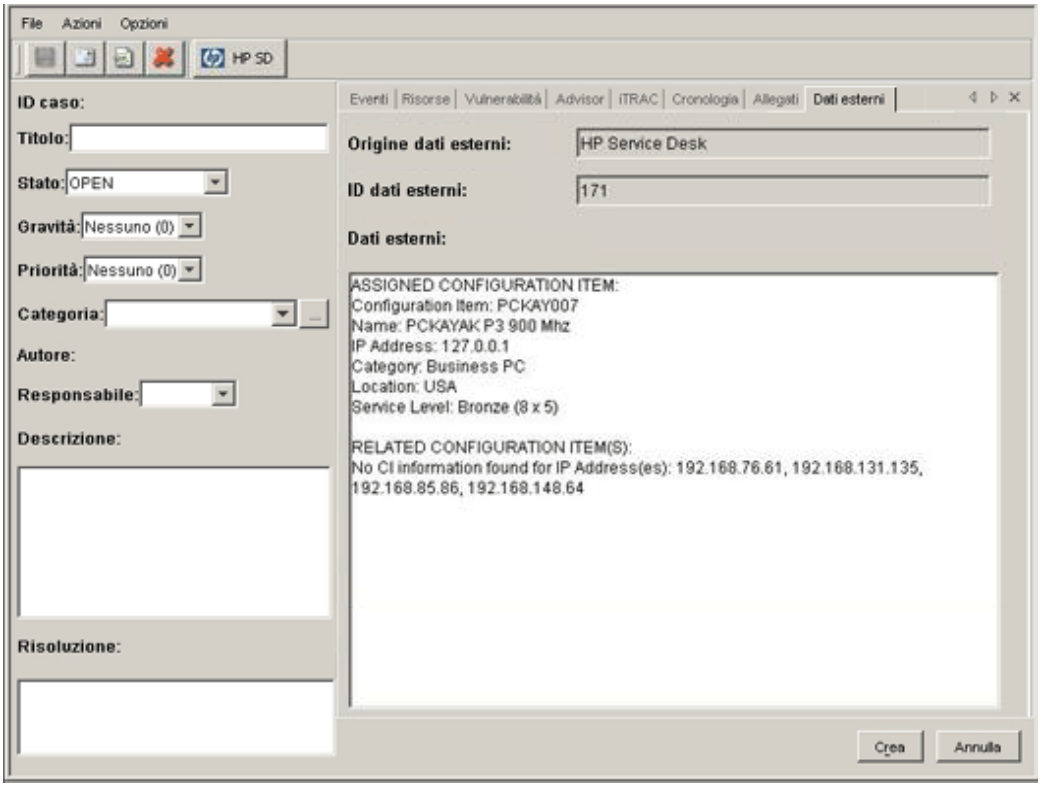
5. Verrà visualizzata la finestra Invia caso a *HP OpenView Service Desk*. Nel menu a discesa *Send To Service Desk* (*Invia a Service Desk*) è disponibile l'elenco di selezione degli elementi di configurazione che include quelli richiesti da HP Service Desk.



In questo elenco è inoltre disponibile l'opzione *Rilevamento automatico*. Se è selezionata, Sentinel tenterà di utilizzare l'indirizzo IP di destinazione degli eventi associati al caso di Sentinel in modo da determinare automaticamente l'elemento di configurazione Service Desk correlato.

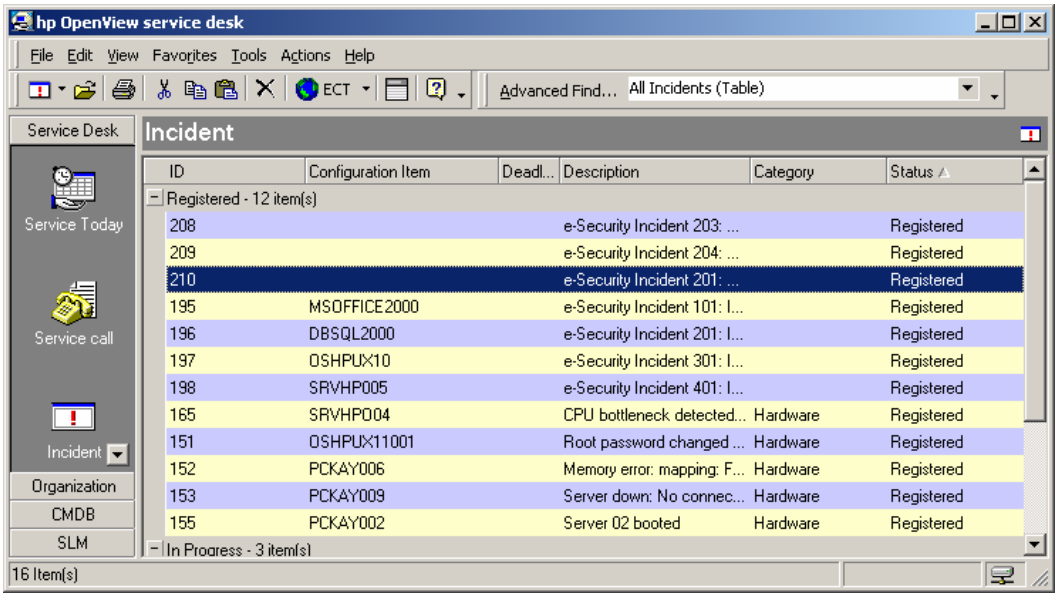
6. (Facoltativo) Nella finestra di dialogo *Send To Service Desk* (*Invia a Service Desk*) è disponibile l'elenco di selezione Gruppo di lavoro che include i gruppi di lavoro richiesti da HP Service Desk.
7. Fare clic su OK. Il caso verrà inoltrato a *HP OpenView Service Desk*.

NOTA: per aggiornare il caso di Sentinel visualizzato, utilizzare la scheda Dati esterni. Nella scheda Dati esterni vengono visualizzati l'ID del caso di Service Desk e il relativo elemento di configurazione a cui è assegnato il caso di Service Desk.



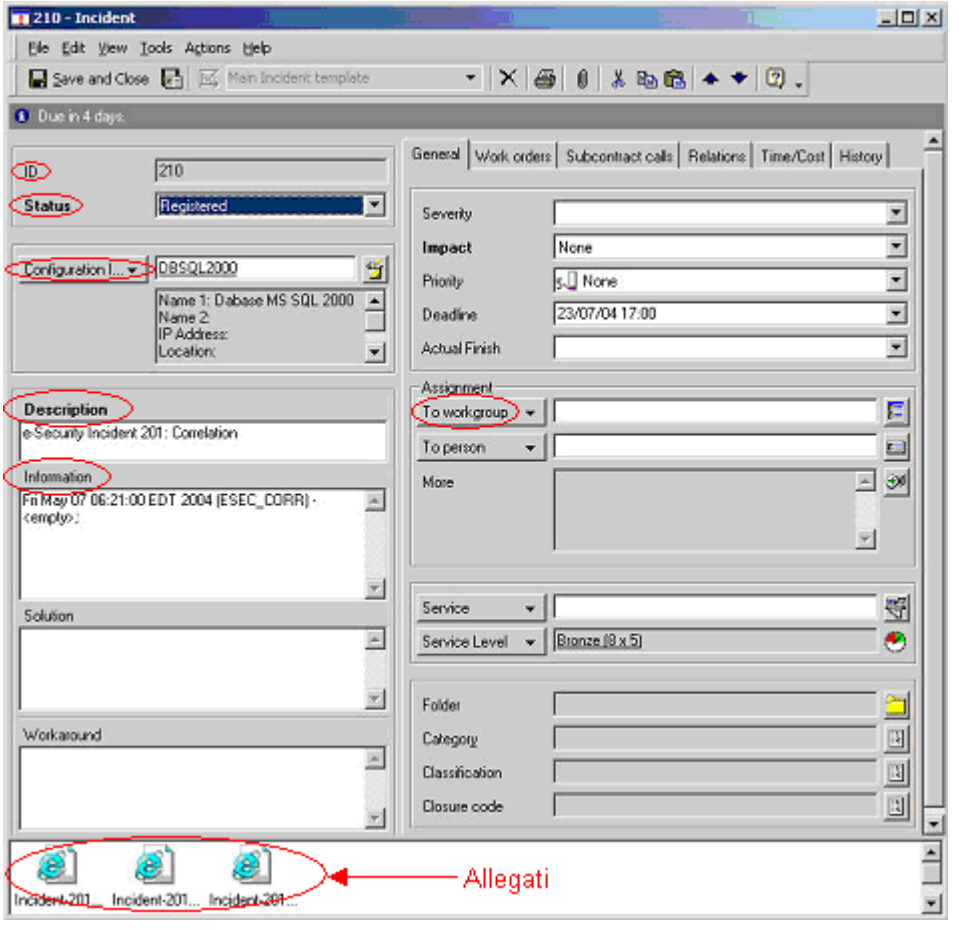
HP OpenView Service Desk Client

Il caso, una volta inviato a HP OpenView Service Desk, viene visualizzato in HP OpenView Service Desk Client in cui viene elencato in base all'ID dei dati estesi anziché in base al numero di ID del caso.



Fare doppio clic su un caso per visualizzarne i dettagli.

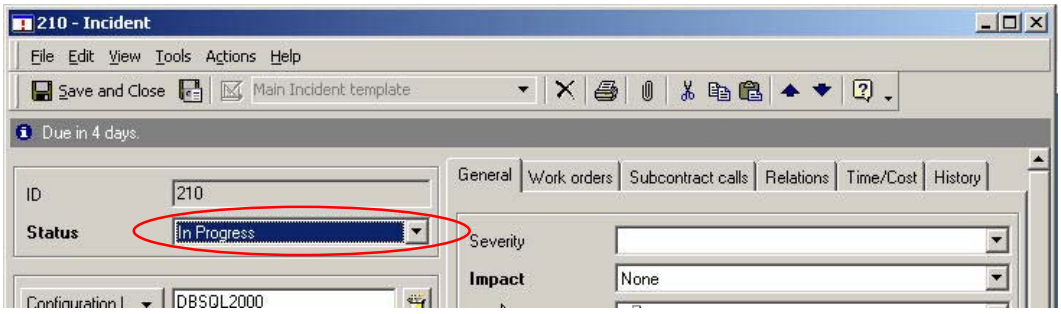
- ID dell'origine estesa
- Stato
- Elemento di configurazione
- Descrizione
- Informazioni
- Gruppo di lavoro
- Informazioni sugli eventi (allegato)
- Informazioni sulla vulnerabilità (allegato)
- Informazioni di Advisor (allegato)



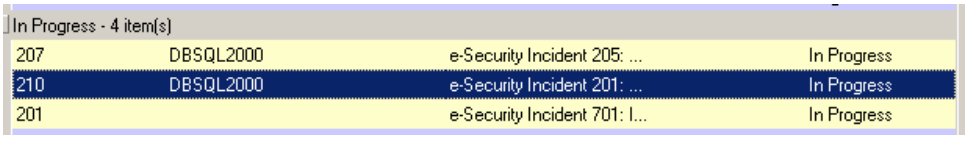
HP OpenView Service Desk – Interfaccia bidirezionale

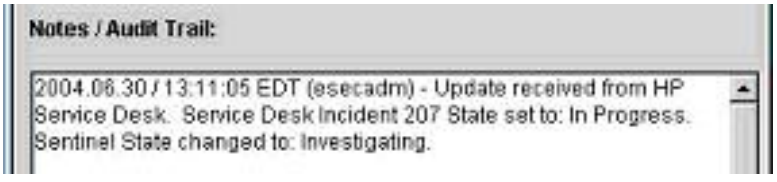
Se questa opzione è abilitata (vedere la Guida all'installazione di Sentinel) in Sentinel si riceverà una notifica da Service Desk ogni volta che lo stato di un caso originato da Sentinel viene modificato da un utente di Service Desk. Ciò consente agli utenti di Sentinel di tenere traccia dello stato corrente di ogni caso inviato tramite Service Desk.

Se si attiva una visualizzazione dei dettagli, la si modifica e la si salva la visualizzazione indicherà lo stato in corso.



È possibile visualizzare questo aggiornamento in HP OpenView Service Desk Client e nella finestra Caso della console di Sentinel.





Riconfigurazione manuale delle impostazioni di interfaccia di HP OpenView Service Desk

Durante la prima installazione di HP OpenView Service Desk Interface di terze parti, le impostazioni Service Desk e OpenView vengono memorizzate nel file das_query.xml. Per modificare queste impostazioni al termine dell'installazione, consultare le informazioni riportate in questa sezione del documento.

Impostazioni di HP OpenView Service Desk

Le impostazioni di HP OpenView Service Desk vengono memorizzate nel file das_query.xml incluso nel componente HpServiceDeskService come illustrato di seguito:

- server: impostato sul nome host e/o indirizzo IP di Service Desk Server.
- username (nome utente): impostato sul nome utente di Service Desk Server.
- password: impostata sulla password cifrata di Service Desk Server mediante l'utility descritta nella sezione Reimpostazione delle password di HP Open View.
- attachment_path (percorso_allegato): impostato automaticamente sulla directory per gli allegati di terze parti .
- ftp_server (server_ftp): impostato sul nome host e/o l'indirizzo IP del server FTP utilizzati da Service Desk per gli allegati.
- ftp_username (nome utente_ftp): impostato sul nome utente FTP utilizzato da Service Desk per gli allegati.
- ftp_password (password_ftp): impostata sulla password cifrata dell'utente FTP (utilizzata da Service Desk per gli allegati) mediante l'utility descritta nella sezione Reimpostazione delle password di HP Open View.
- ftp_user_home (home_utente_ftp): impostata sul percorso completo della directory dell'utente FTP.
- attachment.events: impostata su yes (sì) per indicare che verrà utilizzato l'allegato degli eventi.

- attachment.events.filename: il nome file utilizzato per i file con gli allegati degli eventi.
- attachment.vuln: impostata su yes (sì) per indicare che verrà utilizzato l'allegato delle vulnerabilità.
- attachment.vuln.filename: il nome file utilizzato per i file con gli allegati della vulnerabilità.
- attachment.adv.attack: impostata su yes (sì) per indicare che verrà utilizzato l'allegato con gli attacchi di Advisor.
- attachment.adv.attack.filename: il nome file utilizzato per i file con gli allegati degli attacchi di Advisor.

Reimpostazione delle password di HP OpenView

Le password di HP OpenView vengono memorizzate in formato cifrato nel file das_query.xml file. Per reimpostare le password memorizzare in questo file, è quindi necessario utilizzare l'utility descritta di seguito.

Per reimpostare le impostazioni di interfaccia di HP OpenView Service Desk

8. Passare alla directory %ESEC_HOME%/sentinel/bin/
9. Immettere:

```
extconfig -n das_query.xml [-s password_sd] [-f
   password_ftp_sd]
```

   - -s corrisponde alla password del server di HP OpenView Service Desk
   - -f corrisponde alla password del server FTP che verrà utilizzato da Service Desk per gli allegati.