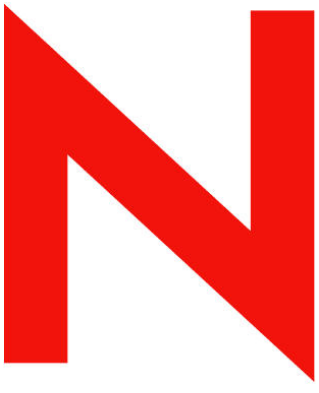
Novell® Sentinel™

5.1.3

7 de julho de 2006

www.novell.com

Volume V – GUIA DE INTEGRAÇÃO DE TERCEIROS DO SENTINEL



Novell®

Informações legais

A Novell, Inc. não faz representações ou garantias quanto ao conteúdo ou à utilização desta documentação e especificamente se isenta de quaisquer garantias de comercialização explícitas ou implícitas ou adequação a qualquer propósito específico.
Além disso, a Novell, Inc. reserva-se o direito de revisar esta publicação e fazer mudanças em seu conteúdo a qualquer momento,sem obrigação de notificar qualquer pessoa ou entidade sobre essas revisões ou mudanças.

A Novell, Inc. não representa nem garante nenhum software e especificamente se isenta de qualquer garantia explícita ou implícita de comercialização ou adequação a qualquer propósito específico. A Novell, Inc. reserva-se o direito de mudar qualquer parte do software da Novell a qualquer momento, sem ter a obrigação de notificar nenhuma pessoa ou entidade sobre tais mudanças.

Quaisquer produtos ou informações técnicas sob este Contrato estão sujeitos aos controles de exportação vigentes nos Estados Unidos e à legislação comercial de outros países. Você concorda em cumprir todos os regulamentos do controle de exportação e em obteras licenças ou a classificação necessárias para exportar, reexportar ou importar produtos finais. Você concorda em não exportar nem reexportar para entidades que constem nas listas atuais de exclusão de exportação dos Estados Unidos ou para qualquer país embargado ou com histórico de terrorismo, como especificam as leis de exportação norte-americanas. Você concorda em não utilizar os produtos finais em atividades proibidas, relacionadas a mísseis, equipamentos nucleares e armas químico-biológicas.Consulte o site www.novell.com/info/exports/ para obter mais informações sobre a exportação do software da Novell. A Novell não assumirá qualquer responsabilidade se você não obtiver as aprovações necessárias para exportação.

Copyright © 1999-2006 Novell, Inc. Todos os direitos reservados. Nenhuma parte desta publicação pode ser reproduzida, fotocopiada, armazenada em um sistema de recuperação ou transmitida sem o consentimento por escrito da Novell.

A Novell, Inc. possui os direitos de propriedade intelectual com relação à tecnologia utilizada no produto descrito neste documento. Em particular, e sem limitação, esses direitos de propriedade intelectual podem incluir uma ou mais patentes americanas listadas em http://www.novell.com/company/legal/patents/ e uma ou mais patentes adicionais ou pedidos de patentes pendentes nos EUA e em outros países.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EUA
http://www.novell.com

Documentação Online: Para acessar a documentação online deste produto e de outros produtos da Novell e obter atualizações,visite www.novell.com/documentation.

Marcas registradas da Novell

Para obter informações sobre as marcas registradas da Novell, consulte a lista Marcas registradas da Novell e marcas de serviços em (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiais de terceiros

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Informações legais de terceiros

O Sentinel 5 pode conter as seguintes tecnologias de terceiros:

- Apache Axis e Apache Tomcat, Copyright © 1999 a 2005, Apache Software Foundation. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.apache.org/licenses/
- ANTLR. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.antlr.org
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.bouncycastle.org.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, pacote de utilitários. Copyright © Doug Lea. Usado sem as classes CopyOnWriteArrayList e ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, incorporando o seguinte trabalho protegido por lei de direitos autorais: mars.cpp por Brian Gladman e Sean Woods. Para obter mais informações, isenções de responsabilidade e restrições, consulte 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, licenciado sob a Licença Pública GNU Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, licenciado sob a Licença Pública GNU Menos Restritiva, disponível em: 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/ou Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

  O Java 2 Platform também pode conter os seguintes produtos de terceiros:

  - CoolServlets © 1999
  - DES e 3xDES © 2000 por 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, uma marca comercial registrada ou marca registrada da Bigelow e Holmes
- Taligent, Inc.
- IBM, algumas partes disponíveis em: http://oss.software.ibm.com/icu4j/

Para obter mais informações sobre essas tecnologias de terceiros e suas isenções de responsabilidade e restrições associadas, consulte: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.java.sun.com/products/javabeans/glasgow/jaf.html e clique em download > license.
- JavaMail. Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.java.sun.com/products/javamail/downloads/index.html e clique em download > license.
- Java Ace, por Douglas C. Schmidt e seu grupo de pesquisa na Washington University e Tao (com agrupadores ACE) por Douglas C. Schmidt e seu grupo de pesquisa em Washington University, University of California, Irvine e Vanderbilt University. Copyright © 1993-2005.Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.cs.wustl.edu/~schmidt/ACE-copying.html e http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Java Authentication e Authorization Service Modules, licenciados sob a Licença Pública Geral Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://free.tagish.net/jaas/index.jsp.
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.java.sun.com/products/javawebstart/downloads-jnlp.html e clique em download > license.
- Java Service Wrapper. Partes protegidas por lei de direitos autorais da seguinte maneira: Copyright © 1999, 2004 Tanuki Software e Copyright © 2001 Silver Egg Technology. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE. Copyright © 2002 a 2005, JIDE Software, Inc.
- O jTDS é licenciado sob a Licença Pública GNU Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, licenciado sobre a Licença Pública Geral Menos Restritiva. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://web.ukonline.co.uk/mseries.
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Partes do código são protegidas por lei de direitos autorais por várias entidades, que se reservam todos os direitos. Copyright © 1989, 1991, 1992 por Carnegie Mellon University; Copyright © 1996, 1998 a 2000, the Regents of the University of California; Copyright © 2001 a 2003 Networks Associates Technology, Inc.; Copyright © 2001 a 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. e Copyright © 2003 a 2004, Sparta, Inc. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://net-snmp.sourceforge.net.
- The OpenSSL Project. Copyright © 1998-2004. the Open SSL Project. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://www.openssl.org.
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, antiga Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Licenciado sob a Licença de Software do Apache. Para obter mais informações, isenções de responsabilidade e restrições, consulte https://skinlf.dev.java.net/.
- Sonic Software Corporation. Copyright © 2003-2004. O software SSC contém software de segurança licenciado pela RSA Security, Inc.

- Tinyxml. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://grinninglizard.com/tinyxmldocs/index.html.
- SecurityNexus. Copyright © 2003 a 2006. SecurityNexus, LLC. Todos os direitos reservados.
- Xalan e Xerces, licenciados pela Apache Software Foundation Copyright © 1999-2004. Para obter mais informações, isenções de responsabilidade e restrições, consulte http://xml.apache.org/dist/LICENSE.txt.
- yWorks. Copyright © 2003 a 2006, yWorks.

NOTA: A partir da publicação desta documentação, os links acima se tornaram ativos. Caso você descubra que quaisquer dos links acima foram desfeitos ou que as páginas da Web vinculadas estão inativas, contate a Novell, Inc. no endereço 404 Wyman Street, Suite 500, Waltham, MA 02451 EUA.

Índice analítico

1 Integração do Remedy **1-1**

Configuração ... 1-2
Fluxo de dados do Remedy para o Sentinel ... 1-6
Instalando o Sentinel ... 1-10
Configuração do fluxo de dados do Remedy para o Sentinel ... 1-11

2 Operações do Suporte Técnico do Remedy **2-1**

Operações do Suporte Técnico do Remedy ... 2-1
Redefinindo manualmente as configurações da interface do Remedy ... 2-2
Configurações do Remedy ... 2-2
Redefinindo a senha do Remedy ... 2-2

3 Instalando o HP OpenView Service Desk para Windows **3-1**

Requisitos do sistema ... 3-1
Instalação ... 3-2
Configurando o HP OpenView Service Desk ... 3-3
Habilitando a Interface (bidirecional) do Service Desk para o Sentinel ... 3-4

4 Integração do HP OpenView Service Desk **4-1**

HP OpenView Service Desk ... 4-1
Enviando Incidentes para o HP OpenView Service Desk ... 4-2
HP OpenView Service Desk Client ... 4-4
HP OpenView Service Desk – Interface Bidirecional ... 4-5
Redefinindo manualmente as configurações da Interface do HP OpenView Service Desk ... 4-6

Prefácio

A documentação técnica do Sentinel consiste no guia de referência e operação para finalidade geral. Essa documentação é destinada aos profissionais de segurança da informação. O texto foi desenvolvido para ser usado como fonte de referência sobre o Sistema de Gerenciamento de Segurança Empresarial do Sentinel. A documentação adicional está disponível no portal do Sentinel na Web.

A documentação técnica do Sentinel está dividida em cinco volumes. São eles:

- Volume I – Guia de Instalação do Sentinel™ 5
- Volume II – Guia do Usuário do Sentinel™ 5
- Volume III – Guia do Usuário do Assistente do Sentinel™ 5
- Volume IV – Guia de Referência do Usuário do Sentinel™ 5
- Volume V – Guia de Integração de Terceiros do Sentinel™

Volume I – Guia de Instalação do Sentinel

Este guia explica como instalar:

- Sentinel Server
- Console do Sentinel
- Mecanismo Sentinel Correlation
- Crystal Reports do Sentinel
- Construtor de Coletor Assistente
- Gerenciador de Coletor Assistente
- Consultor

Volume II – Guia do Usuário do Sentinel

Este guia aborda o seguinte:

- Operação do Console do Sentinel
- Recursos do Sentinel
- Arquitetura do Sentinel
- Comunicação do Sentinel
- Avaliação de vulnerabilidade
- Monitoramento de eventos
- Filtragem de eventos
- Correlação de eventos
- Gerenciador de Dados do Sentinel
- Configuração de Eventos para Relevância Comercial
- Serviço de Mapeamento
- Geração de relatórios de histórico
- Gerenciamento de Host do Assistente
- Incidentes
- Casos
- Gerenciamento de usuários
- Workflow

Volume III – Guia do Usuário do Assistente

Este guia aborda o seguinte:

- Operação do Construtor de Coletor do Assistente
- Gerenciador de Coletor Assistente
- Coletores
- Gerenciamento de Host do Assistente
- Construção e manutenção de coletores

Volume IV – Guia de Referência do Usuário do Sentinel

Este guia aborda o seguinte:

- Linguagem de criação de scripts do Assistente
- Comandos de análise do Assistente
- Funções do administrador do Assistente
- Metatags do Assistente e do Sentinel
- Permissões de usuário
- Mecanismo de correlação do Sentinel
- Opções da linha de comando de correlação
- Esquema do banco de dados do Sentinel

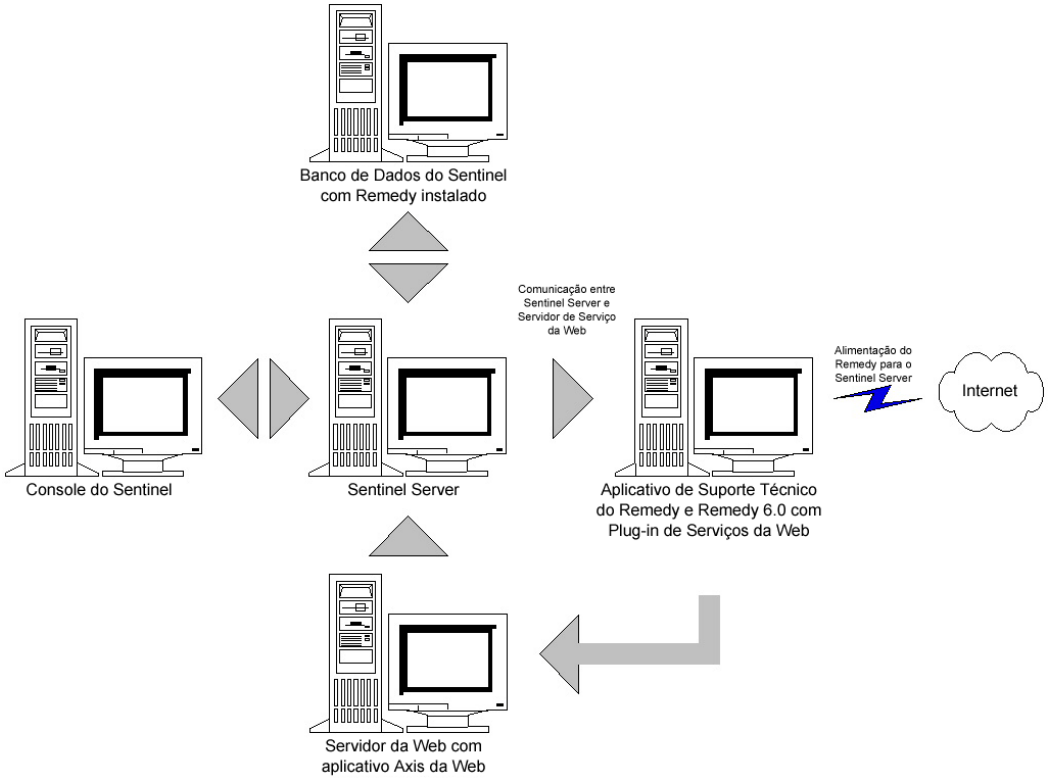
Volume V – Guia de Integração de Terceiros do Sentinel

- Remedy
- Operações do HP OpenView
- Suporte técnico HP

1 Integração do Remedy

É possível usar a integração do Remedy para o Sentinel v4.2 ou v5 para criar aplicativos de workflow integrados ao Sistema de Comunicação de Problemas do Remedy e ao sistema Sentinel. Estes são os principais recursos da integração do Remedy:

- Capacidade de criar um novo caso no Suporte Técnico do Remedy com base em um incidente no Sentinel.
- Capacidade de atualizar um caso relacionado no Suporte Técnico quando um incidente é atualizado no Sentinel.
- Capacidade de atualizar um incidente no Sentinel quando um caso relacionado é atualizado no Suporte Técnico.



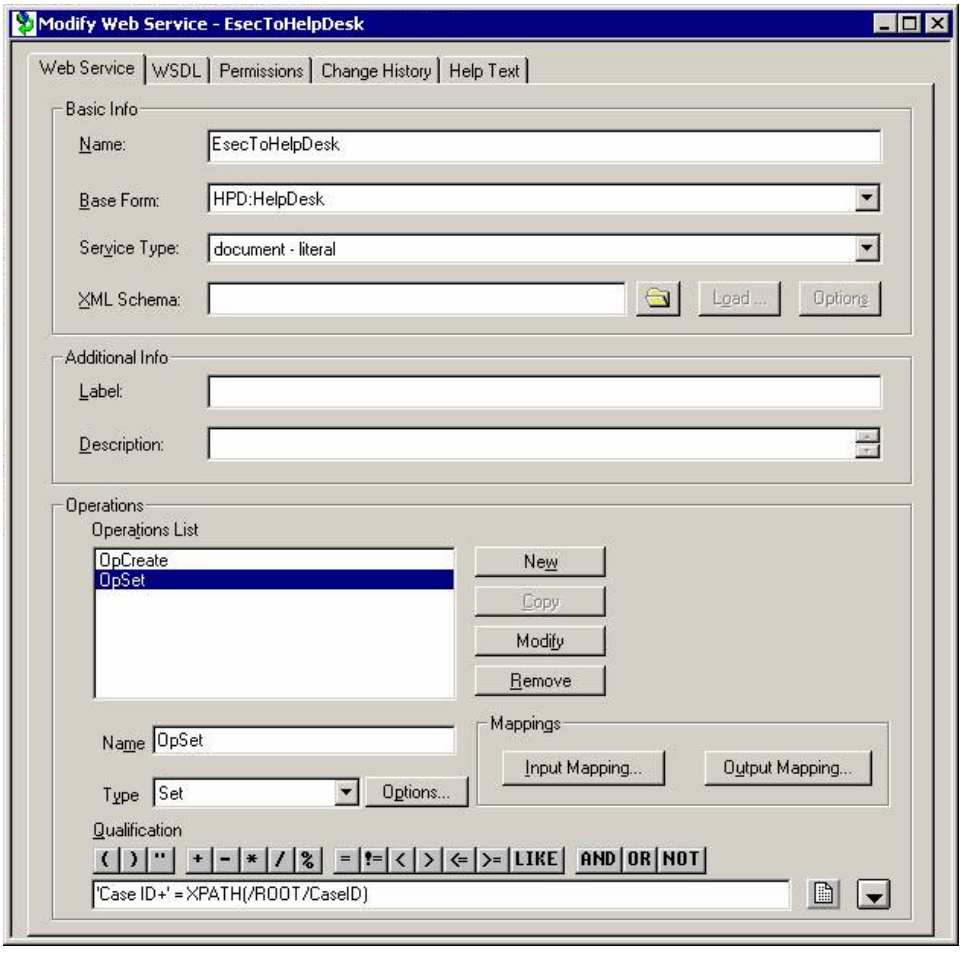
Configuração

Para mudar o formulário Caso do Suporte Técnico do Remedy

1. Efetue login em *Administrador do Remedy* > *Formulários*, clique duas vezes em *Suporte Técnico HPD*.
2. Para suportar a integração com o Sentinel, é necessário adicionar ao formulário Caso do Suporte Técnico um campo de caractere (EsecIncidentId) e um campo de pool de anexos (Pool de Anexos). Essas entradas de campo serão usadas para adicionar anexos de incidentes ao formulário.
3. Para adicionar o campo de caractere EsecIncidentId:
   - Clique no botão “Novo Campo de Caractere” e coloque-o em um local do formulário.
   - Na guia Exibir, defina um rótulo.
   - Na guia Banco de Dados, no campo Nome, defina o nome como EsecIncidentID.
4. Para adicionar o campo de caracteres Pool de Anexos com os três seguintes campos: EsecEvents, EsecVuln e EsecAdv.
   - Clique no botão *Criar Pool de Anexos*.
   - Na guia Exibir, no campo de rótulo, digite um nome de rótulo (ex: anexos do esec).
   - Sob Campos de Anexos, em “Inserir Rótulo de Campo de Anexos”, digite:
     - EsecEvent e clique em Adicionar.
     - EsecVuln e clique em Adicionar.
     - EsecAdv e clique em Adicionar.
5. Clique em *Gravar*.

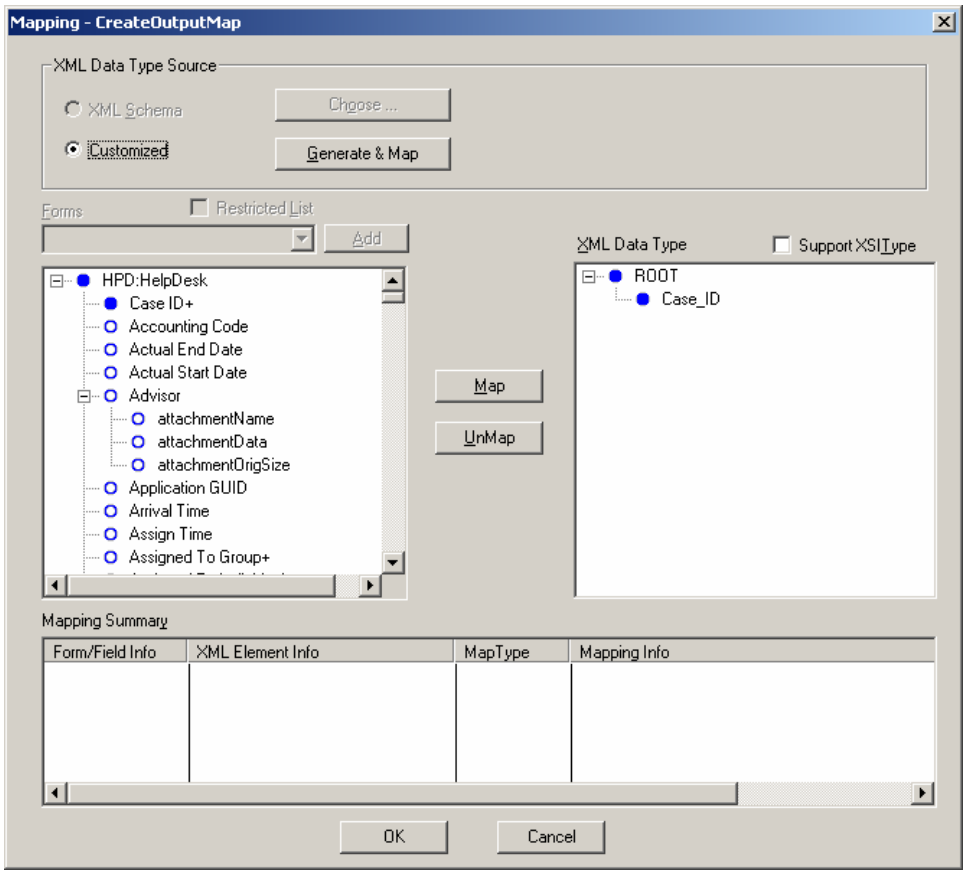
Criando o serviço Web

1. No Administrador do Remedy, no painel de navegação, realce *Serviços Web*. Clique o botão direito do mouse em *Novos Serviços Web* e clique na guia *Serviços Web*.



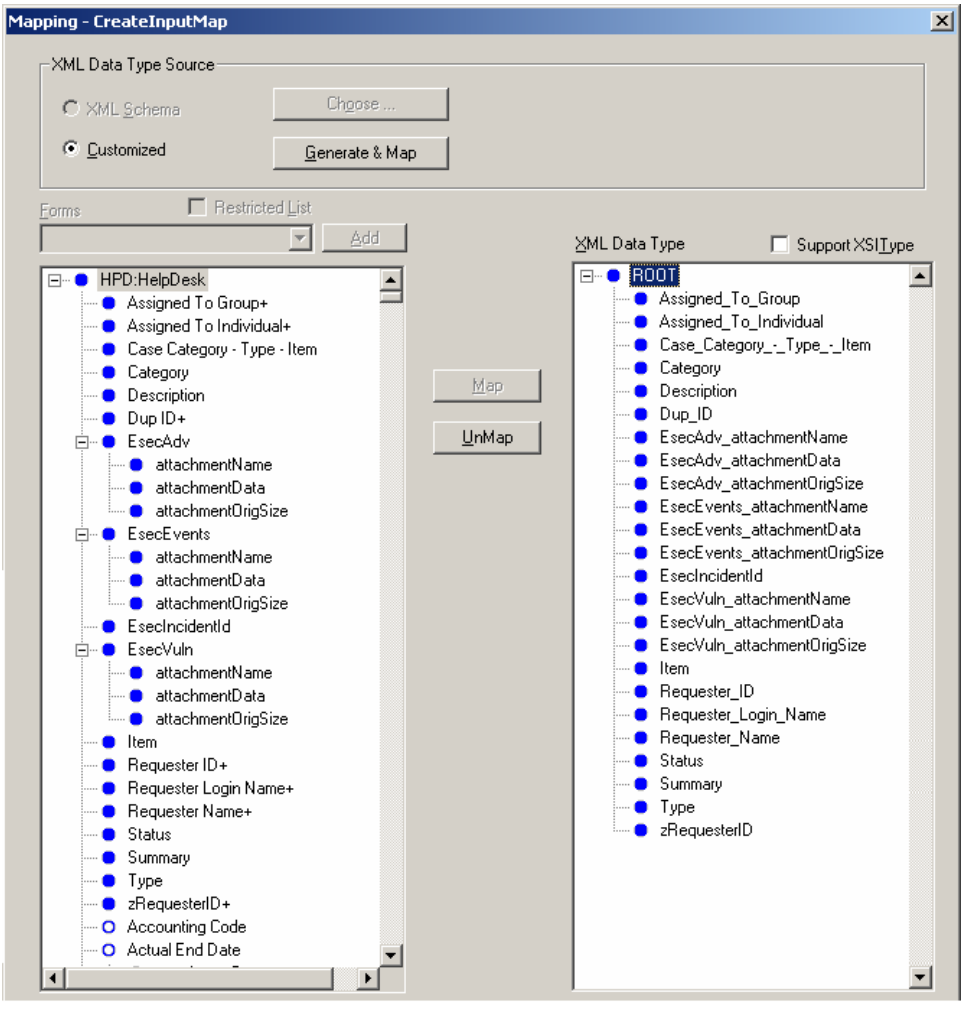
2. Usando o Caso do Suporte Técnico como um formulário de base, crie um Serviço Web chamado *EsecToHelpDesk* e selecione Formulário de Base do Suporte Técnico HPD.
3. Realize estas duas operações para o serviço Web:
   - opCreate
   - opSet

   removendo as outras operações.
4. Selecione OpCreate e clique no botão Mapeamento de Saída. Faça com que a tela corresponda à ilustração a seguir.


Mapping - CreateOutputMap
XML Data Type Source
XML Schema
Customized
Choose ...
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

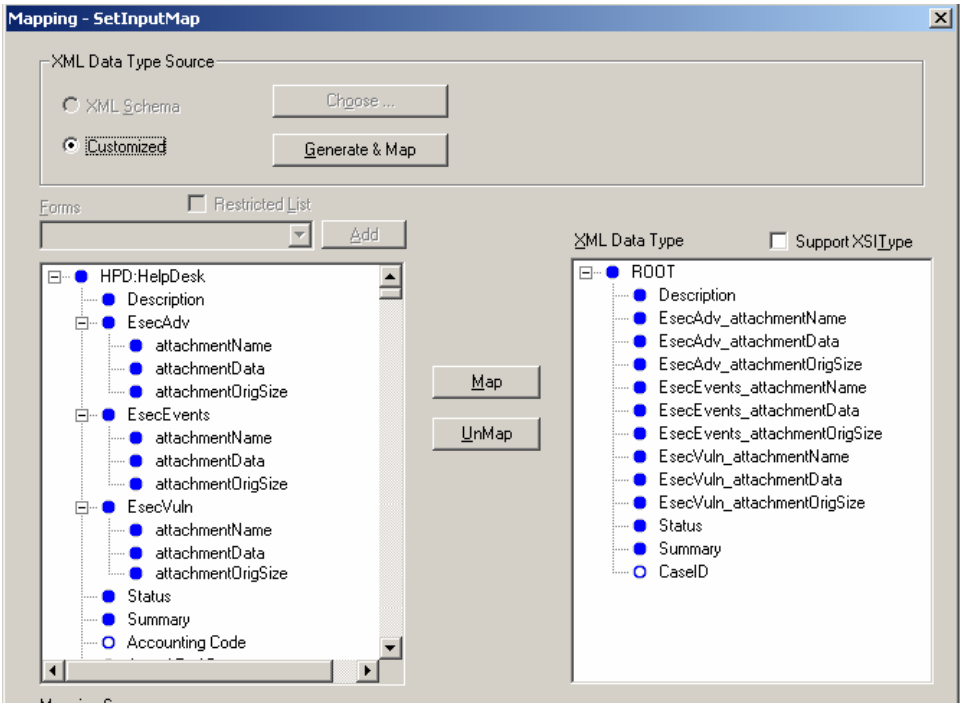
Selecione o botão Mapeamento de Entrada para opCreate. Faça com que a tela corresponda à ilustração a seguir.

NOTA: Para remover um item, realce-o > *clique o botão direito do mouse* > *cortar*.

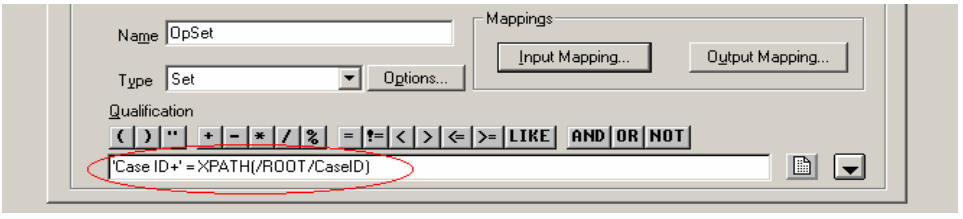


Clique em *Gravar*.

Selecione o botão Mapeamento de Entrada para opSet. Faça com que a tela corresponda à ilustração a seguir.



Não há mapeamento de saída para opSet. Para opSet, é necessário especificar uma qualificação:



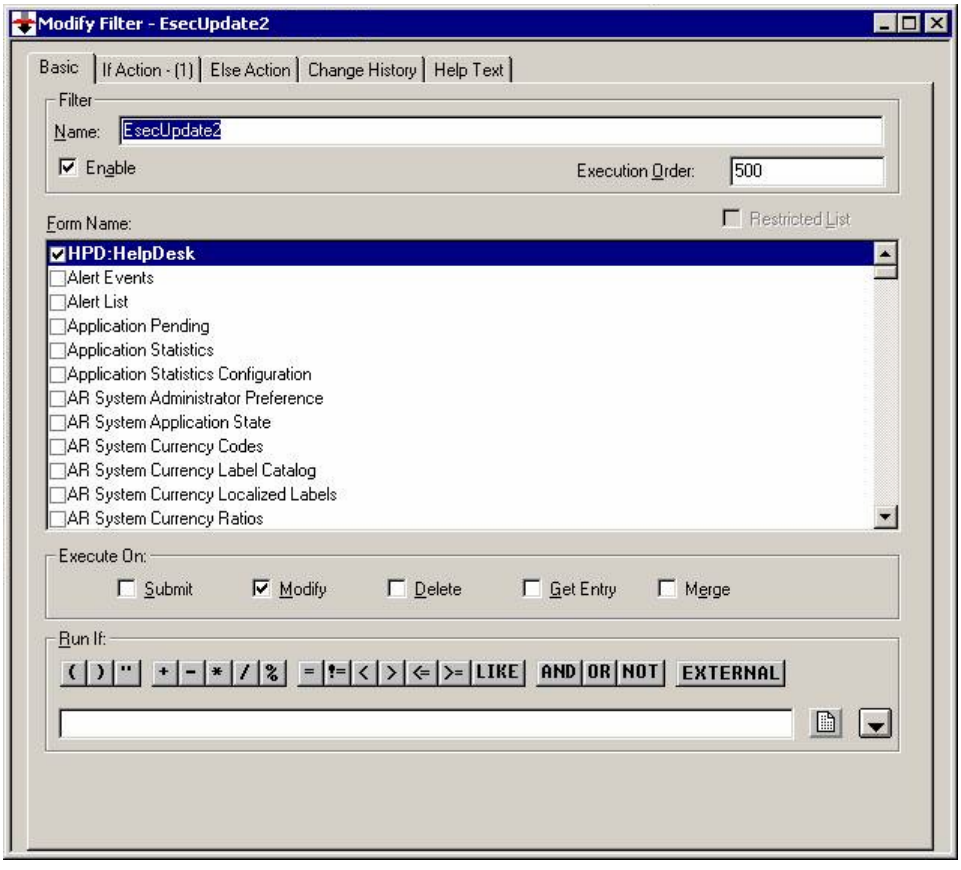
5. Vá para a guia Permissões e mova o serviço para Público, movendo essa opção da esquerda para a direita. Clique em *Gravar*.

Fluxo de dados do Remedy para o Sentinel

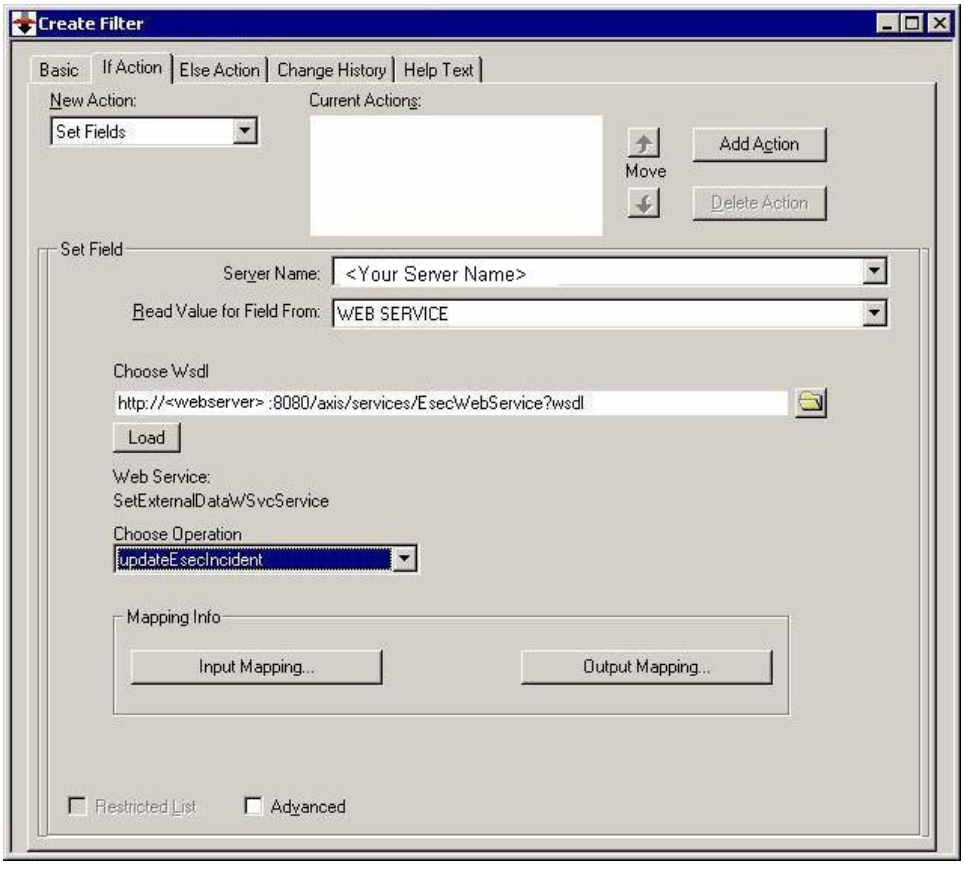
Para que o Serviço Web do Sentinel possa ser acessado, é necessário que haja um servidor Web com o aplicativo Web Axis em execução no momento da inicialização do Sentinel Server.

Fluxo de dados do Remedy para o Sentinel

1. No Administrador do Remedy, realce Filtros e clique o botão direito do mouse em *Adicionar Filtro*.
2. Crie um filtro para o formulário Caso do Suporte Técnico que seja executado em um evento modificado. Verifique se a tela corresponde à ilustração a seguir.

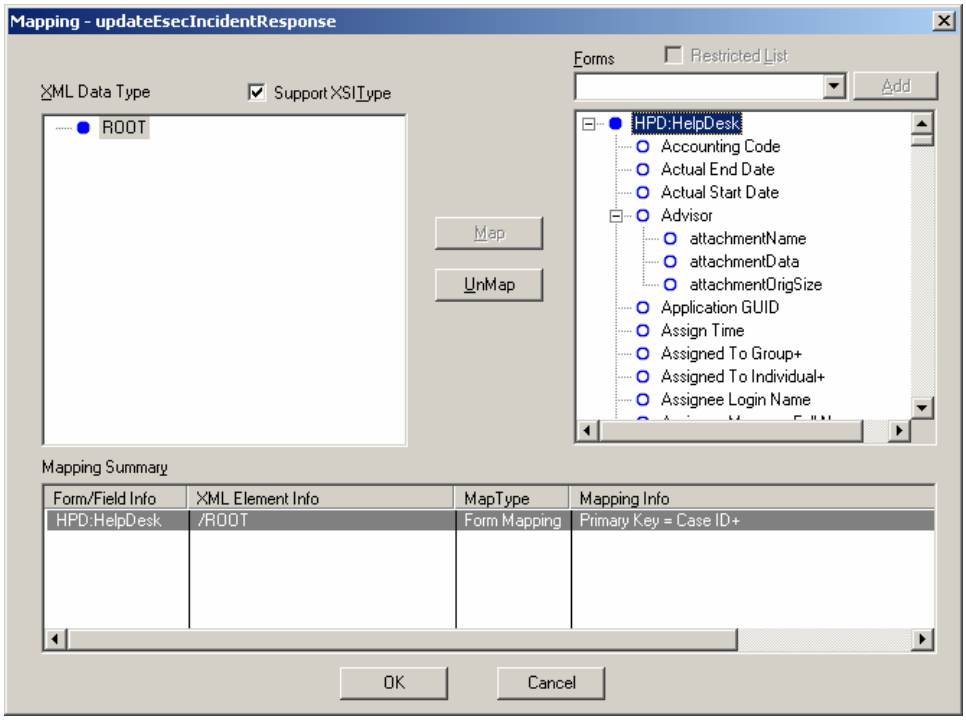


3. Na guia *Ação Se*, no menu suspenso *Nova Ação*, selecione a ação *Definir campo*, no painel *Definir Campo*, selecione *SERVIÇO WEB* e forneça o URL do Serviço Web do Sentinel (http://<IP do servidor Web ou nome DNS>:8080/axis/services/EsecWebService?wsdl).



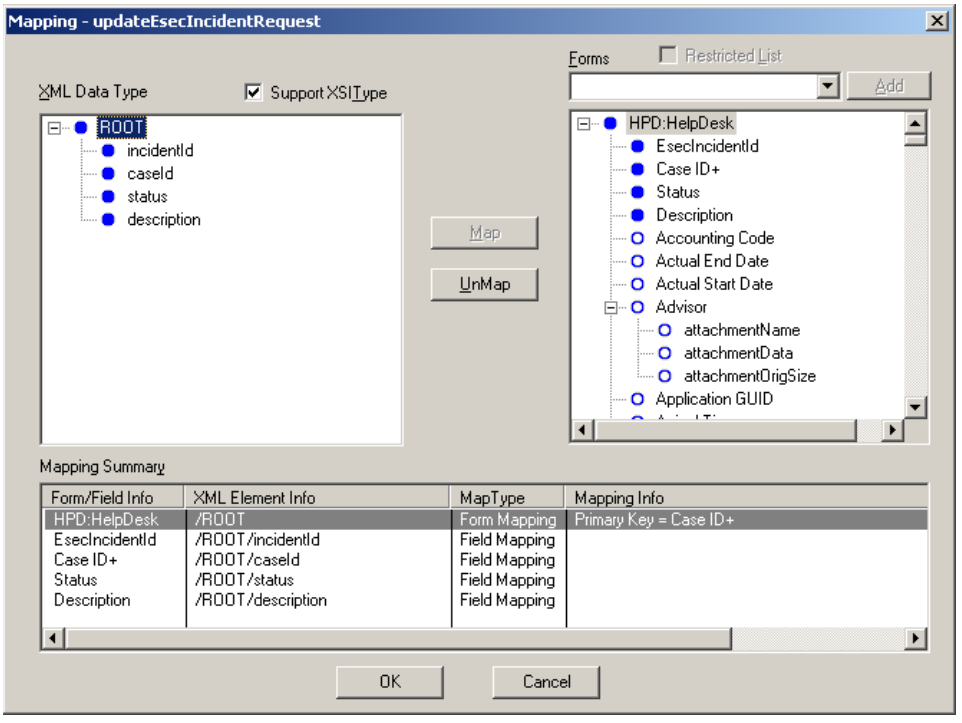
4. No menu suspenso *Escolher Operação*, selecione o método *updateEsecIncident* e defina o mapeamento de Entrada e de Saída.

Clique no botão Mapeamento de Saída. Faça com que a tela corresponda à ilustração a seguir.



Clique no botão Mapeamento de Entrada. Faça com que a tela corresponda à ilustração a seguir.

NOTA: Para definir seu Mapa, selecione um item à esquerda (p.ex., incidentId), selecione um item à direita (p.ex., EsecIncidentId) e clique no botão Mapear.



NOTA: Após a instalação, sempre que você gravar uma mudança no formulário Caso do Suporte Técnico, ela será submetida a um serviço do Sentinel.

5. Clique em *Gravar*.

Instalando o Sentinel

Ao instalar o Sentinel com o Remedy, você precisará ter uma conta no Remedy. Nessa conta, você será solicitado a fornecer as informações a seguir.

NOTA: Você deve ter a permissão Integração do Remedy.

- Nome de Usuário
- Senha
- Nome do Solicitante
- ID do Solicitante
- Login do Solicitante
- Nome do Grupo (pode ser deixado em branco)
- Nome Individual (pode ser deixado em branco)
- Nome do Servidor
- Nome do Serviço

Para o fluxo de dados do Remedy para o Sentinel, você será solicitado a fornecer:

- Servidor Web do Sentinel (<nome da máquina:porta>)
- Nome de Usuário do Sentinel (como esecadm)
- ID de Usuário do Sentinel
- UUID do Sentinel
- ID de Bloqueio do Sentinel (normalmente definido como 1 ou 2, é....

Instalando o Sentinel

1. Selecione integração do Remedy durante a instalação.
2. Tenha as informações acima disponíveis durante o processo de instalação.

Configuração do fluxo de dados do Remedy para o Sentinel

Se você for usar a Integração de Terceiros (Integração do Remedy), será recomendável fazer a instalação e a configuração na seguinte ordem:

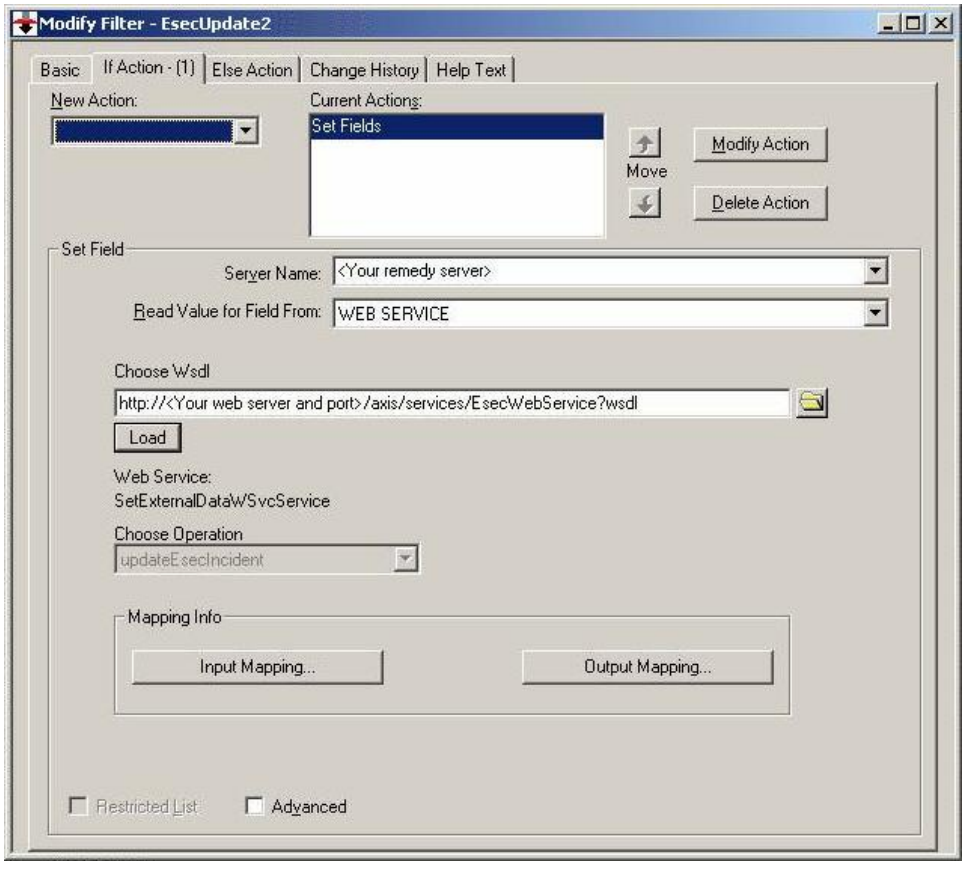
- Instale o Aplicativo de Suporte Técnico do Remedy e o Remedy 6.0 com o Plug-in de Serviços Web
- Configure novos Filtros e serviços Web no Aplicativo de Ajuda do Remedy.
- Instale o Sentinel

Para estabelecer o fluxo de dados do Remedy para o Sentinel, você deve:

- Para que o Serviço Web do Sentinel possa ser acessado, é necessário que haja um servidor Web com o aplicativo Web Axis em execução antes da inicialização do Sentinel Server.
- Copie todos os arquivos jar da localização a seguir do Sentinel Server para <aplicativo web axis>\webclient\lib.
  - %ESEC_HOME%\lib
  - %ESEC_HOME%\sentinel\console
  - %ESEC_HOME%\communicator (somente na v4.2)
- Copie os arquivos configuration.xml e .keystore do Sentinel Server para uma localização de sua preferência no servidor Web. Esses arquivos estão localizados em %ESEC_HOME%.
  - Edite o arquivo configuration.xml no servidor Web de modo que aponte para o arquivo .keystore.
  - Adicione a seguinte opção JVM ao servidor Web:

    ```
    Dcom.esecurity.configurationfile=<caminho do arquivo
       configuration.xml>\configuration.xml
    ```

- Você deve criar um filtro para o formulário Caso do Suporte Técnico que seja executado em um evento "Modificado". Esse filtro chama o servidor Web do Sentinel.


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 Operações do Suporte Técnico do Remedy

Suporte Técnico do Remedy É possível usar a integração do Remedy para criar aplicativos de workflow. Estes são os recursos da integração do Remedy:

- Capacidade de criar um novo caso no Suporte Técnico do Remedy com base em um incidente no Sentinel.
- Capacidade de atualizar um incidente no Sentinel quando um caso relacionado é atualizado no Suporte Técnico.
- Capacidade de atualizar um incidente no Sentinel quando um Caso relacionado é atualizado no Suporte Técnico.

Operações do Suporte Técnico do Remedy

Como enviar um Incidente para o Suporte Técnico do Remedy (v5.0.1 e posterior)

1. Clique na guia *Incidentes*.
2. No painel de navegação, expanda a pasta *Visões de Incidente* e realce *Gerenciador de Visão de Incidente*.

   NOTA: Se já houver um conjunto de incidentes para outro sistema externo, não será possível mudá-lo.

3. Expanda umas das telas de incidentes e clique duas vezes no seu incidente. O incidente será aberto.
4. Clique no botão *Remedy*.

O Incidente será atualizado com a guia Dados Externos e o botão Remedy.

Como atualizar um Incidente para o Suporte Técnico do Remedy (v5.0.1 e posterior)

1. Clique na guia *Incidentes*.
2. Expanda o painel de navegação à esquerda e clique duas vezes em um incidente que esteja definido para o Suporte Técnico do Remedy.
3. Clique no botão *Remedy* no Incidente. Será adicionada uma anotação na guia Externo.

Redefinindo manualmente as configurações da interface do Remedy

Durante a instalação inicial da Interface do Suporte Técnico do Remedy, as configurações do Remedy são armazenadas no arquivo das_query.xml. Use as informações contidas nesta seção da documentação se precisar modificar essas configurações após a instalação.

Configurações do Remedy

As configurações do Remedy são armazenadas no arquivo das_query.xml sob o componente RemedyARServerService, da seguinte maneira:

Redefinindo a senha do Remedy

As senhas do Remedy são armazenadas em formato criptografado no arquivo das_query.xml. Portanto, se você precisar redefinir as senhas armazenadas nesse arquivo, deverá usar o utilitário descrito abaixo.

Para redefinir a senha da interface do Remedy

1. cd %ESEC_HOME%/sentinel/bin/
2. Digite:

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

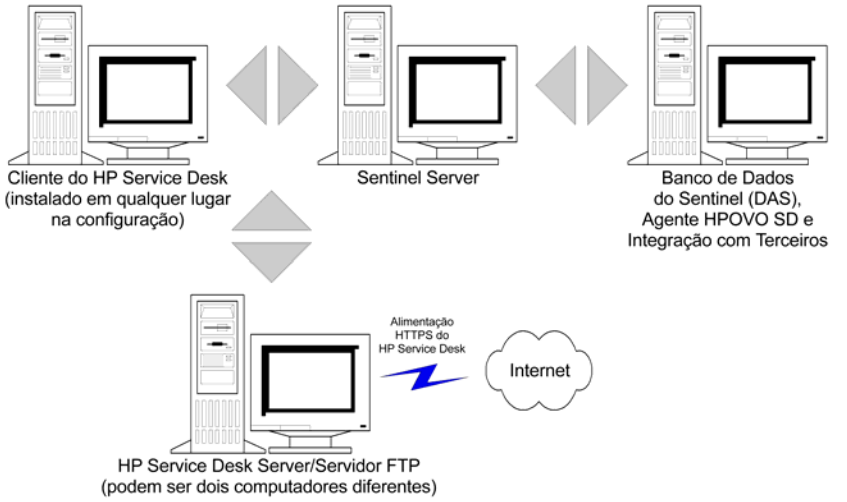
   - -r é a senha do Remedy

3 Instalando o HP OpenView Service Desk para Windows

A integração bidirecional do Sentinel com o HP OpenView Service Desk, que é licenciado separadamente, fornece novos recursos importantes ao Console do Sentinel. O Sentinel aproveita os recursos do Gerenciamento de Bens do HP OpenView Service Desk para fornecer informações referenciais para ajudar na resposta a ameaças e ataques de segurança. Esses novos recursos fornecem a capacidade de:

- Enviar Incidente(s) para o HP Service Desk (SD)
- Anexar Evento(s) a um Incidente do HP SD
- Anexar Informações de Vulnerabilidade a um Incidente do HP SD
- Consultar e Preencher informações de Item de Configuração (Bem) no SD e no Incidente do Console do Sentinel
- Integração das Viagens de Ida e Volta: O SD envia atualizações para a Novell e a Novell envia atualizações para o SD
- Atualizar o Status de Incidentes do SD no Console do Sentinel da Novell
- Atualizar o Status de Incidentes do Sentinel no HP SD

A seguir está uma configuração de instalação típica. Sua configuração pode ser diferente.



Requisitos do sistema

Para obter os requisitos de hardware e software do HP OpenView Service Desk Client, do HP OpenView Service Desk Server e do HP OpenView Service Desk Server, consulte o Guia de Instalação do HP OpenView Service Desk.

O Sentinel suporta as seguintes versões do HP OpenView Service Desk:

- HP OpenView Service Desk Server - Versão 4.5 com Service Pack 8 (4.5.0588.0802 SP 8)
- HP OpenView Service Desk Client - Versão 4.5 com Service Pack 8
- HP OpenView Service Desk Agent - Versão 4.5 com Service Pack 8
- Sentinel 4.2.1.8 ou 4.2.1.15 para Windows
- Qualquer Servidor FTP de terceiros

O HP OpenView Service Desk Server e o HP OpenView Service Desk Client devem ser instalados em uma máquina a ser designada como o Service Desk Server. Consulte o Guia de Instalação do HP OpenView Service Desk para obter ajuda sobre como instalar o Service Desk.

Para habilitar essa interface bidirecional, um HP OpenView Agent deve ser instalado na mesma máquina em que o das_cmd.bat estiver instalado. A interface bidirecional permite que o HP Service Desk notifique o Sentinel sempre que o Status de um Incidente originado do Sentinel for mudado por um usuário do Service Desk. Esses incidentes devem originar-se do Console do Sentinel.

Para que o Service Desk gerencie anexos, um servidor FTP deve ser instalado (normalmente no Service Desk Server) e o Service Desk deve ser configurado para se comunicar com ele. É possível usar qualquer servidor FTP de terceiros. Consulte o Guia de Instalação do servidor FTP para obter ajuda sobre como instalar esse servidor.

Instalação

Se você também for instalar o HP OpenView Operations, é recomendável instalá-lo antes do HP OpenView Service Desk.

NOTA: Durante a instalação inicial da Interface de Terceiros do HP OpenView Service Desk, as configurações do Service Desk e do OpenView são armazenadas no arquivo das_query.xml. Para mudar qualquer uma dessas configurações (como o nome do usuário ou a senha), consulte *Operação - HP OpenView e Service Desk para Windows 2000.*

É recomendável fazer a instalação na seguinte ordem:

- FTP Server

NOTA: Consulte o Guia de Instalação do servidor FTP para obter ajuda sobre como instalar esse servidor.

- HP OpenView Service Desk Server com Service Pack 8 – pode ser o mesmo que o servidor FTP
- HP OpenView Service Desk Client com Service Pack 8
- HP OpenView Service Desk Agent com Service Pack 8 (para habilitar essa interface bidirecional) – deve estar na mesma máquina em que o DAS está instalado.

NOTA: Consulte o Guia de Instalação do HP OpenView Service Desk para obter ajuda sobre como instalar o software HP OpenView Service Desk.

- Instale a Integração de Terceiros do Sentinel
  - HP OpenView Service Desk

NOTA: Para obter informações de instalação, consulte as Notas de Versão do Sentinel v4.2.1.8 e o Guia de Instalação do Sentinel v4.2 para Windows e Solaris.

Configurando o HP OpenView Service Desk

A configuração do HP OpenView Service Desk é realizada por meio do Service Desk Client. Antes de modificar a configuração do HP Service Desk para que ele se comunique com o Servidor FTP, tenha as seguintes informações disponíveis:

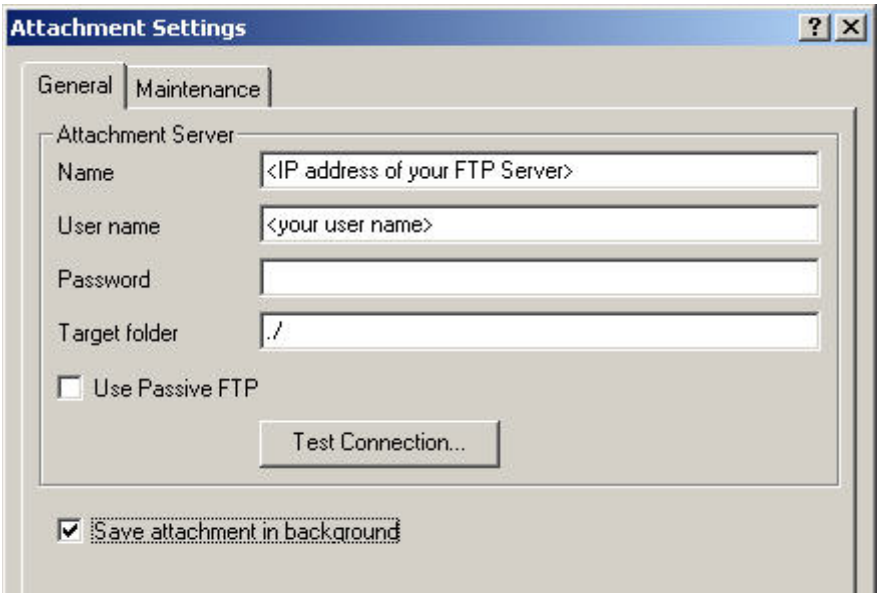
- Nome – endereço IP do Servidor FTP
- Nome de Usuário/Senha – qualquer usuário definido no Servidor FTP
- Pasta de Destino – recomenda-se digitar "./". Essa ação coloca seu diretório de FTP no diretório de FTP atual.
- Desmarque 'Usar FTP Passivo'
- Marque “Gravar anexo em segundo plano”

NOTA: Para obter mais informações e as etapas de configuração detalhadas, consulte a seção Tarefas de pós-instalação do Guia de instalação do HP OpenView Service Desk.

Para definir Configurações de Anexos

1. Inicie o HP Service Desk Client.
2. Clique em *Ferramentas* > *Sistema*.
3. Clique em *Painel do Sistema* no painel de navegação à esquerda.
4. Clique duas vezes em *Configurações de Anexo*. Digite:
   - Nome – endereço IP do Servidor FTP
   - Nome de Usuário/Senha – qualquer usuário definido no Servidor FTP
   - Pasta de Destino – recomenda-se digitar "./". Essa ação coloca seu diretório de FTP no diretório de FTP atual.
   - Desmarque *Usar FTP Passivo*
   - Marque *Gravar anexo em segundo plano*

NOTA: Para obter mais informações e as etapas de configuração detalhadas, consulte a seção Tarefas de pós-instalação do Guia de instalação do HP OpenView Service Desk.



5. Clique em *Testar Conexão*.
6. Clique em *Aplicar* e, em seguida, em *OK*.

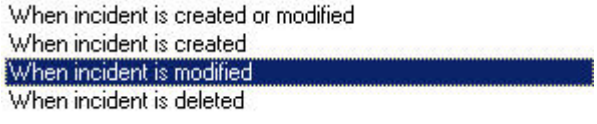
Habilitando a Interface (bidirecional) do Service Desk para o Sentinel

Esta opção permite que o HP Openview Service Desk notifique o Sentinel sempre que o Status de um Incidente originado do Sentinel for mudado por um usuário do Service Desk. Desse modo, você pode monitorar o estado atual de cada Incidente que tenha sido enviado anteriormente ao HP OVO OpenView Service Desk.

Para habilitar esse recurso, é necessário instalar um HP OpenView Service Agent na mesma máquina em que o Sentinel (das_cmd.bat) está instalado. Desse modo, o HP Service Desk poderá executar o utilitário das_cmd do Sentinel.

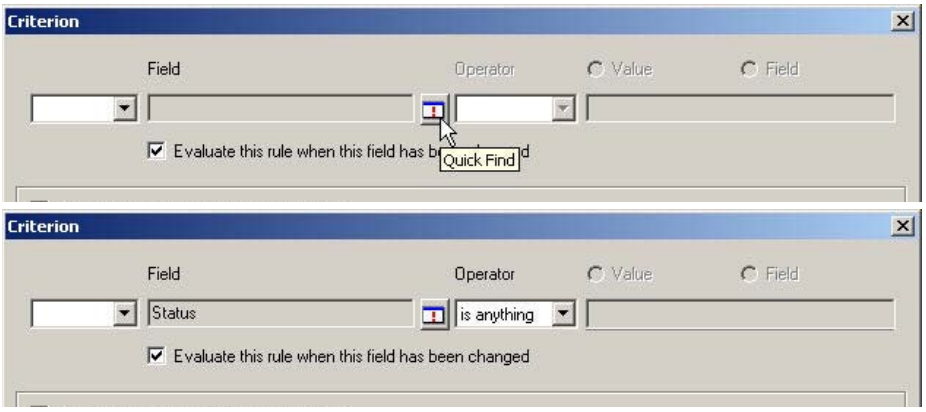
Habilitando a interface bidirecional

1. Inicie o Service Desk Client.
2. Abra o Console do Administrador selecionando *Ferramentas* > *Sistema*.
3. Clique em Lógica Comercial no painel de navegação à esquerda.
4. Clique duas vezes em *Regras Comerciais*.
5. Clique duas vezes em *Incidente*. Será exibida a janela de lista Regras de Banco de Dados.
6. Clique o botão direito do mouse no painel Regras de Banco de Dados > *Nova Regra de Banco de Dados*.
7. Realce *Quando o incidente é modificado* e clique em *Avançar*.



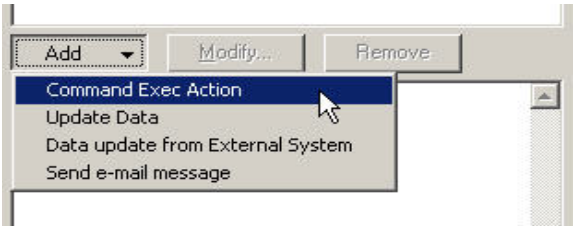
8. Clique no botão *Condição...*
9. Clique no botão *Adicionar Critério...*

10. Clique no botão *Localização Rápida*, selecione *Status* e, em seguida, selecione *é qualquer item* no campo de operador.



Clique em *OK* e em *OK* novamente.

11. Clique em *Adicionar*. Selecione *Ação de Execução de Comando*.



12. Adicione uma nova “Ação de Execução de Comando", de modo que o script “das_cmd.bat” seja executado no Sentinel Server sempre que a regra for avaliada.

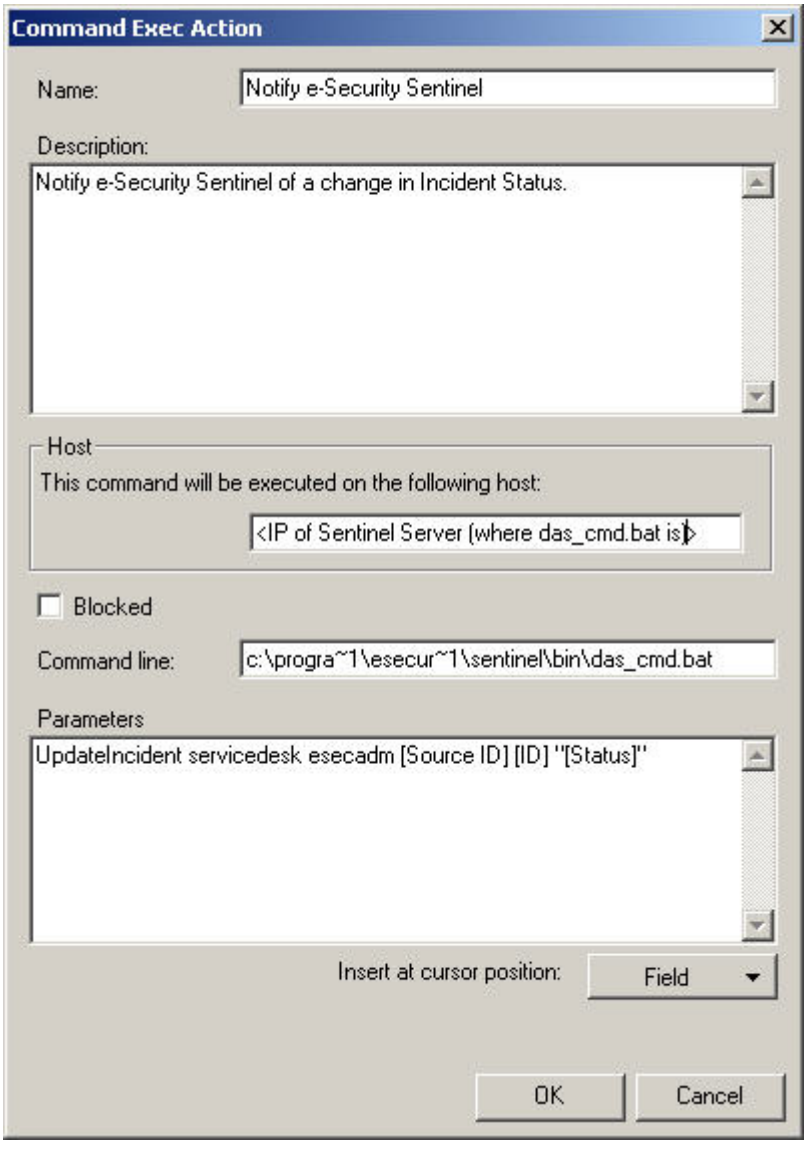
    Ao configurar a ação, especifique o nome (ou endereço IP) do Sentinel Server (máquina em que o das_cmd.bat está localizado) como o “Host”. Especifique também o caminho completo do arquivo "das_cmd.bat" do Sentinel Server na “Linha de Comando”, como:

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

NOTA: Você deve usar a convenção de nomeação do DOS 8.3 para especificar os nomes de diretório com espaços. Por exemplo, use “progra~1” em vez de “Arquivos de Programa”.

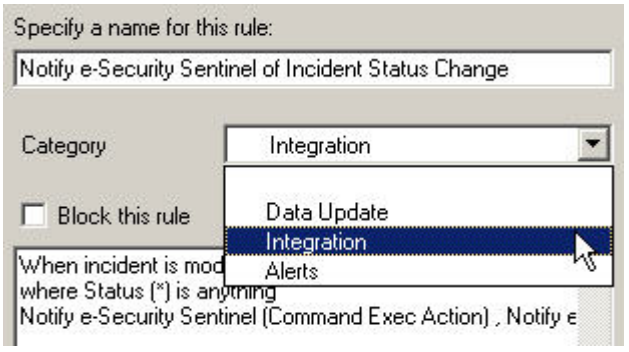
Por fim, especifique a ação “Parâmetros” como:

```
UpdateIncident servicedesk esecadm [ID da Origem] [ID]
   "[Status]"
```



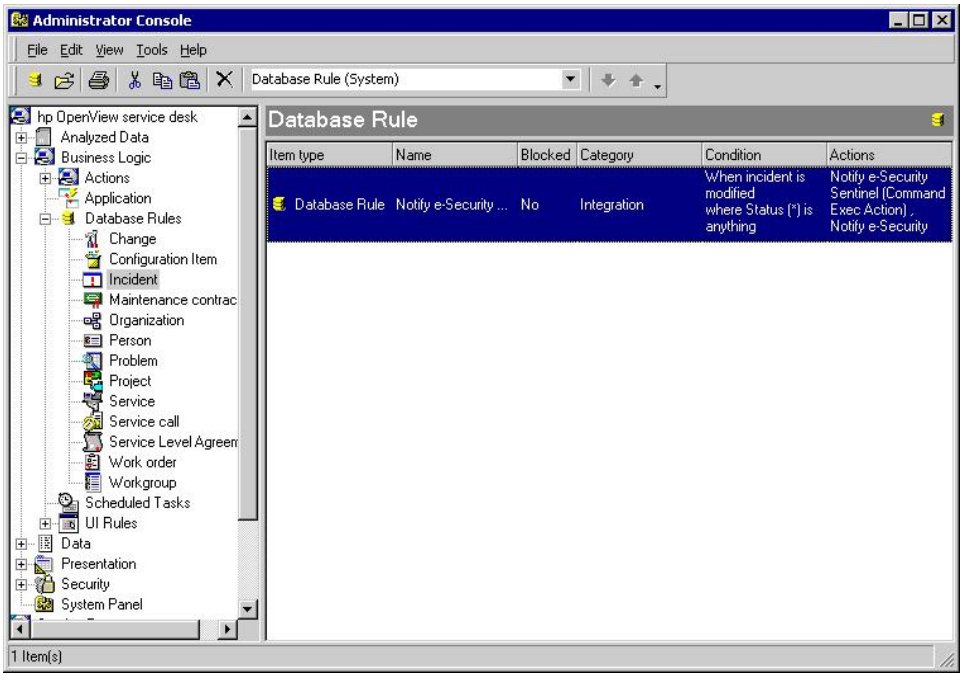
Atribua o nome desejado com uma descrição à nova Regra de Banco de Dados. Clique em *OK* e, em seguida, em *Avançar*.

13. No campo Categoria, selecione Integração e especifique um nome para essa regra. Não selecione *Bloquear esta regra*.



Clique em *Concluir*.

14. Após a conclusão da nova Regra de Banco de Dados, uma nova regra deverá ser relacionada na lista Regra de Banco de Dados.



4 Integração do HP OpenView Service Desk

O HP OpenView Service Desk para Sentinel permite que você envie eventos de qualquer tela que exiba incidentes e eventos para.

HP OpenView Service Desk

A integração entre o Sentinel e o HP OpenView Service Desk proporciona um recurso adicional de gerenciamento de bens. Esse recurso adicional de gerenciamento de bens permite:

- Enviar Incidente(s) para o HP Service Desk (SD)
  - Anexar Evento(s) a um Incidente do HP SD
  - Anexar Informações de Vulnerabilidade a um Incidente do HP SD
  - Anexar Informações do Consultor a um Incidente do HP SD
  - Consultar e Preencher informações de Item de Configuração (Bem) no Console de Controle do Sentinel
- Atualizar o Status de Incidentes do SD no Console de Controle do Sentinel
- Atualizar o Status de Incidentes do Sentinel no HP SD

As informações de Incidentes do Sentinel enviadas ao HP OpenView Service Desk incluem:

- ID de Incidente do Sentinel
- Estado
- Título
- Anotações/Histórico
- Eventos (anexo)
- Informações de Vulnerabilidade (anexo)
- Informações do Consultor (anexo)

Durante o envio ou o recebimento de informações do HP OpenView Service Desk, ocorrem a conversão e o mapeamento automáticos de estado e status.

A conversão e o mapeamento do Estado do Sentinel para o Status do Service Desk são os seguintes:

Estado do Sentinel	Status do Service Desk
Aberto	Registrado
Confirmado	Aguardando
Designado	Informado
Investigando	Em Andamento
Falso Positivo	Fechado
Verificado	Concluído
Aprovado	Em Andamento
Fechado	Fechado

A conversão e o mapeamento do Status do Service Desk para o Estado do Sentinel são os seguintes:

Status do Service Desk	Estado do Sentinel
Registrado	Aberto
Em Andamento	Investigando
Aguardando	Confirmado
Concluído	Verificado
Informado	Atribuído
Fechado	Fechado

Enviando Incidentes para o HP OpenView Service Desk

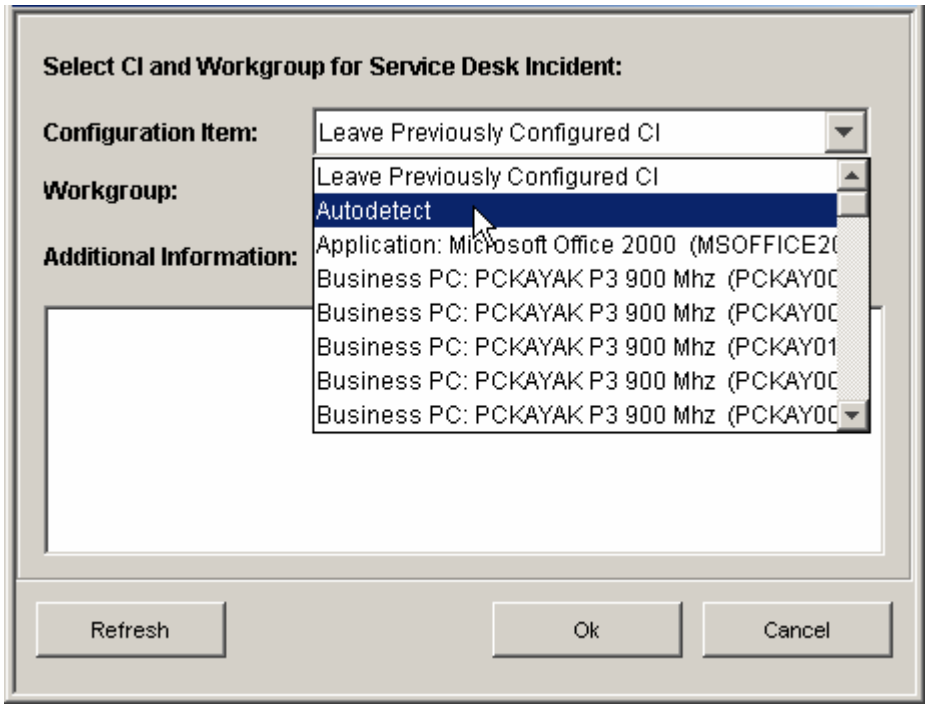
Como enviar um Incidente ao HP OpenView Service Desk

1. Clique na guia *Incidentes*.
2. No painel de navegação, expanda a pasta *Visões de Incidente* e realce *Gerenciador de Telas de Incidentes*.

   NOTA: Se já houver um conjunto de incidentes para outro sistema externo, não será possível mudá-lo.

3. Expanda umas das telas de incidentes e clique duas vezes no seu incidente. O incidente será aberto.
4. Clique no botão *HP SD*.

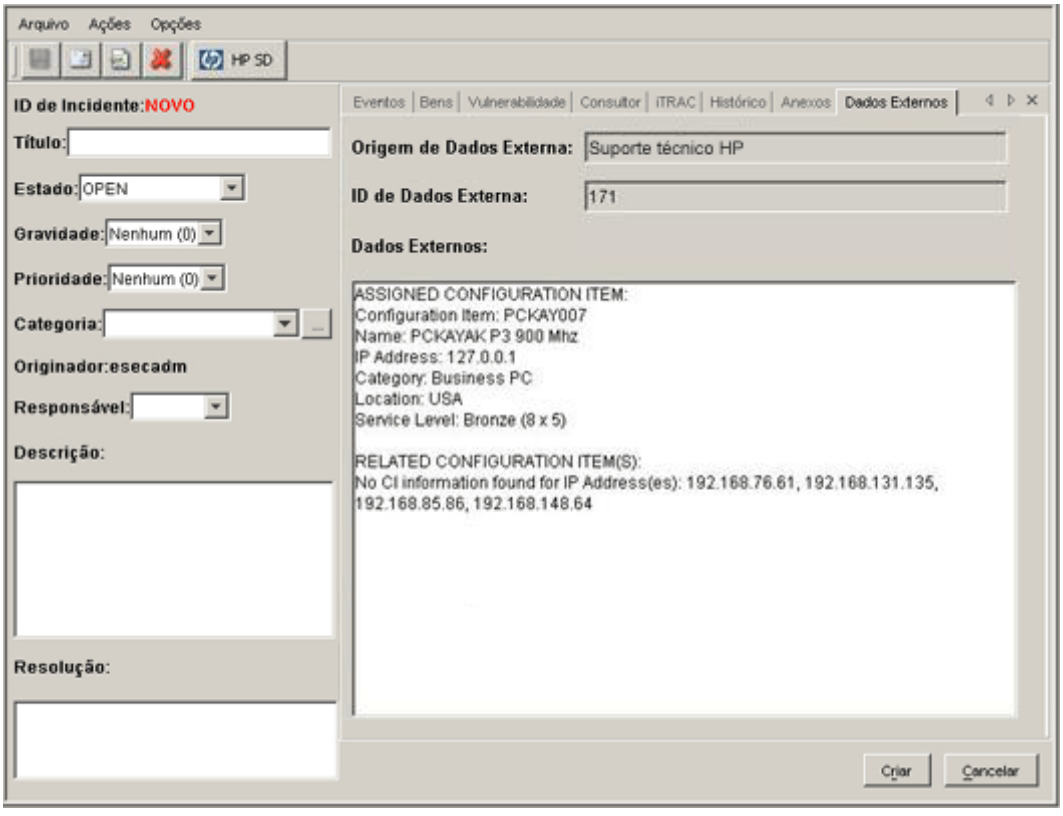
5. Será exibida a janela *Enviar Incidente ao HP Service Desk*. O menu suspenso *Enviar para Service Desk* fornece uma lista de seleção de Itens de Configuração, que é preenchida com os Itens de Configuração consultados no HP Service Desk.



A opção *Detectar Automaticamente* está disponível na lista de seleção de Itens de Configuração. Se você selecionar *Detectar Automaticamente*, o Sentinel tentará usar os endereços IP de Destino dos Eventos associados ao Incidente do Sentinel para determinar automaticamente o IC relacionado ao Service Desk.

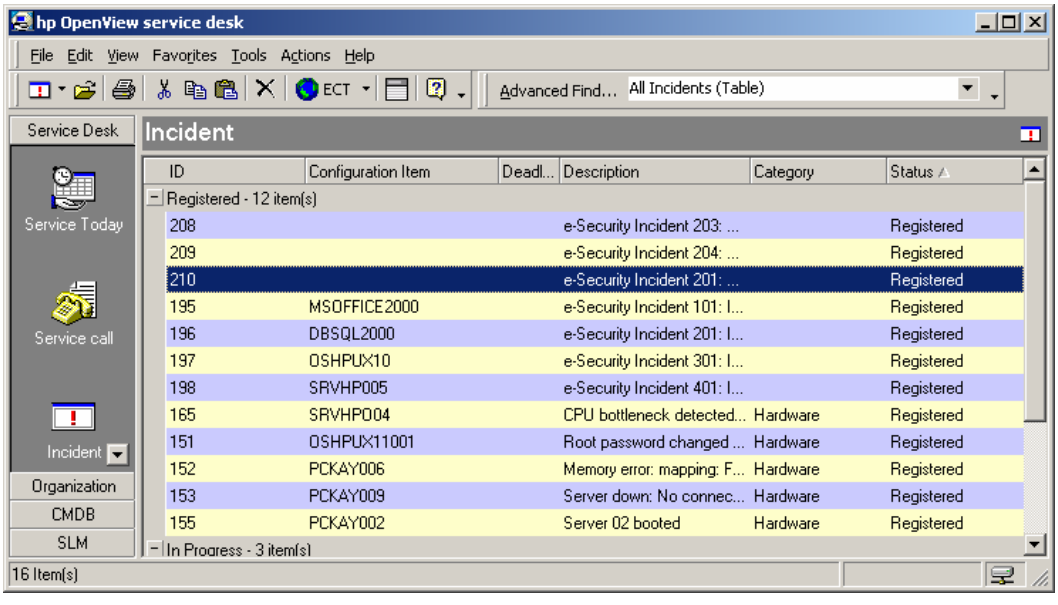
6. (opcional) A caixa de diálogo *Enviar para Service Desk* também fornece uma lista de seleção de Grupos de Trabalho, que é preenchida com os Grupos de Trabalho consultados no Service Desk.
7. Clique em *OK* para que o incidente seja encaminhado ao *HP OpenView Service Desk*.

NOTA: A exibição do Incidente do Sentinel é atualizada com a guia Dados Externos. Essa guia indica o ID do Incidente de Service Desk e o Item de Configuração de Service Desk ao qual foi atribuído o novo Incidente de Service Desk.



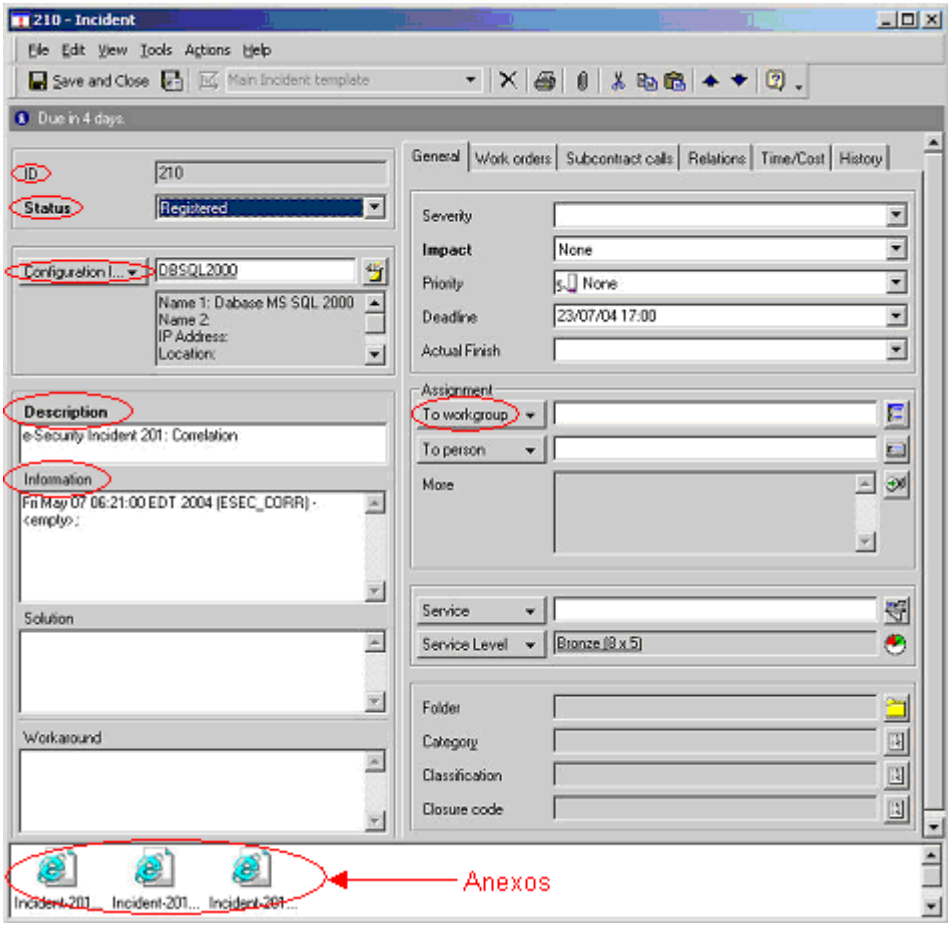
HP OpenView Service Desk Client

Depois que um incidente for enviado ao HP OpenView Service Desk, o incidente será exibido no HP OpenView Service Desk Client. No Service Desk Client, o incidente é relacionado pelo ID de Dados Estendidos, e não pelo número de ID do Incidente.



Clique duas vezes em um incidente e a tela de detalhes desse incidente será exibida.

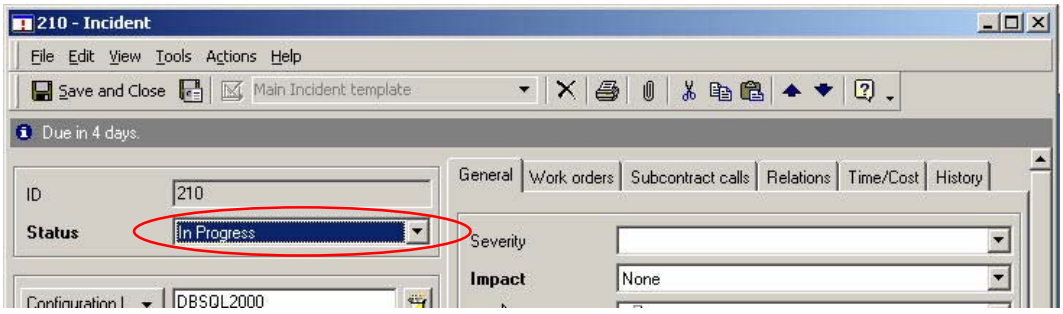
- ID de Origem Estendida
- Status
- Item de Configuração
- Descrição
- Informações
- Grupo de Trabalho
- Informações sobre eventos (anexo)
- Informações sobre Vulnerabilidade (anexo)
- Informações do Consultor (anexo)



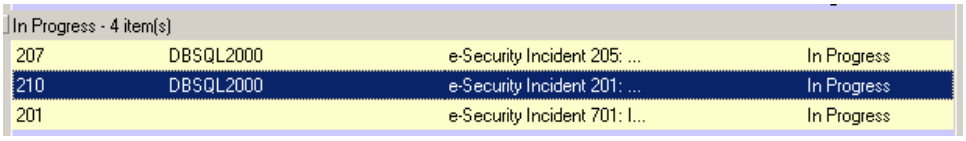
HP OpenView Service Desk – Interface Bidirecional

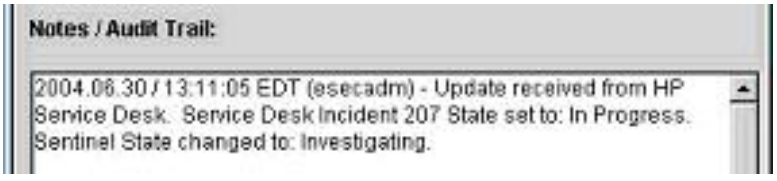
Se esta opção for habilitada, (consulte o Guia de Instalação do Sentinel), o Service Desk notificará o Sentinel sempre que o Status de um Incidente originado do Sentinel for mudado por um usuário do Service Desk. Desse modo, os usuários do Sentinel poderão monitorar o estado atual de cada Incidente enviado ao Service Desk.

Se você ativar uma tela de detalhes, mude-a e grave-a; essa tela de detalhes indicará o status "em andamento".



Também é possível ver essa atualização no HP OpenView Service Desk Client e na janela Incidente do Console do Sentinel.





Redefinindo manualmente as configurações da Interface do HP OpenView Service Desk

Durante a instalação inicial da Interface de Terceiros do HP OpenView Service Desk, as configurações do Service Desk são armazenadas no arquivo das_query.xml.Use as informações contidas nesta seção da documentação se precisar modificar essas configurações após a instalação.

Configurações do HP OpenView Service Desk

As configurações do HP OpenView Service Desk são armazenadas no arquivo das_query.xml no componente HpServiceDeskService, da seguinte maneira:

- servidor - Definido como o nome de host/endereço ip do Service Desk Server.
- nome de usuário - Definido como o nome de usuário do Service Desk Server.
- senha - Definida como a senha criptografada do Service Desk Server, por meio do utilitário descrito na seção Redefinindo as senhas do HP OpenViews.
- alpattachment_path - Definido automaticamente como o diretório "attach" de terceiros.
- ftp_server - Definido como o nome de host/endereço ip do Servidor FTP (esse Service Desk será usado para anexos).
- ftp_username - Definido como o nome de usuário de FTP (esse Service Desk será usado para anexos).
- ftp_password - Definido como a senha criptografada do usuário FTP (esse Service Desk será usado para anexos), por meio do utilitário descrito na seção Redefinindo as senhas do HP OpenViews.
- ftp_user_home - Definido como o caminho completo de diretório do usuário de FTP.
- attachment.events - Definido como "sim" para indicar que o anexo de Eventos será usado.
- attachment.events.filename - O nome de arquivo usado para arquivos do anexo de Evento.

- attachment.vuln - Definido como "sim" para indicar que o anexo de Vulnerabilidade será usado.
- attachment.vuln.filename - O nome de arquivo usado para arquivos de anexo de Vulnerabilidade.
- attachment.adv.attack - Definido como "sim" para indicar que o anexo de Ataque ao Consultor será usado.
- attachment.adv.attack.filename - O nome de arquivo usado para arquivos de anexo de Ataque ao Consultor.

Redefinindo as senhas do HP OpenView

As senhas do HP OpenView são armazenadas em formato criptografado no arquivo das_query.xml. Portanto, se você precisar redefinir as senhas armazenadas nesse arquivo, deverá usar o utilitário descrito abaixo.

Para redefinir as configurações da interface do HP OpenView Service Desk

1. cd %ESEC_HOME%/sentinel/bin/
2. Digite:

```
extconfig -n das_query.xml [-s senha__do_sd] [-f
   senha_de_ftp_do_sd
```

   - -s é a senha de servidor do HP OpenView Service Desk
   - -f é a senha do servidor FTP (servidor FTP que o Service Desk usará para anexos)

HP - Service Desk 4-1
HP OpenView Service Desk 3-1, 4-1
configurando para o servidor FTP 3-3
enviando um Incidente (v5.0) 4-2
instalação 3-2
para definir configurações de anexos 3-3
HP SD 4-1
HP Service Desk 3-1, 4-1
configurando para o Servidor FTP 3-3
enviando um Incidente (v5.0) 4-2
instalação 3-2
para definir configurações de anexos 3-3
HP-OVO 4-1
instalação
HP OpenView Service Desk 3-2
Sentinel 1-10
instalando o Sentinel 1-10
interface bidirecional
HP OpenView Service Desk 3-4
Operações do HP-OpenView 4-1
Remedy 1-1
Suporte Técnico do Remedy 2-1
Configuração de incidentes (v5.0.1 e posterior) 2-1
criando o serviço Web 1-2
enviando um incidente ao Suporte Técnico do Remedy (v5.0.1 e posterior) 2-1
fluxo de dados 1-6
fluxo de dados - mapeamento de entrada 1-9
fluxo de dados - mapeamento de saída 1-9
instalando o Sentinel 1-10
mudando o formulário de casos 1-2
opCreate - entrada 1-5
opCreate - saída 1-3
opSet - entrada 1-6