Novell® Sentinel™

www.novell.com

5.1.3

Volume V : GUIDE D'INTÉGRATION DE PRODUITS TIERS

7 juillet 2006

Novell®

Avis juridique

Novell Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
États-Unis
www.novell.com

Documentation en ligne :
Pour accéder à la documentation en ligne relative aux produits Novell et pour obtenir des mises à jour, reportez-vous au site Novell, à l'adresse suivante : www.novell.com/documentation.

Marques Novell

Pour les marques Novell, reportez-vous à la liste des marques et marques de service Novell à l'adresse suivante : (http://www.novell.com/company/legal/trademarks/tmlist.html).

Marques tiers

Toutes les marques tiers sont la propriété de leurs détenteurs respectifs.

Avis juridique tiers

Sentinel 5 peut comprendre les technologies tierces suivantes :

- Apache Axis et Apache Tomcat, Copyright © 1999 à 2005, Apache Software Foundation. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://www.apache.org/licenses/.
- ANTLR : Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://www.antlr.org.
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous au site http://www.bouncycastle.org.
- Checkpoint : Copyright © Check Point Software Technologies Ltd.
- Concurrent, ensemble de programmes de service : Copyright © Doug Lea. Utilisé sans les classes CopyOnWriteArrayList et ConcurrentReaderHashMap.
- Crypto++ Compilation : Copyright © 1995-2003, Wei Dai, incorporant l'algorithme protégé par copyright mars.cpp par Brian Gladman et Sean Woods. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://www.eskimo.com/~weidai/License.txt.
- Crystal Reports Developer et Crystal Reports Server : Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991-2003.
- edpFTPj, sous licence Lesser GNU Public License. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, sous licence Lesser General Public License disponible à : 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 et/ou Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition : Copyright © Sun Microsystems, Inc. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

La plate-forme Java 2 peut également comprendre les produits tiers suivants :

- CoolServlets © 1999
- DES et 3xDES © 2000 par 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, une marque déposée ou une marque de Bigelow and Holmes
- Taligent, Inc.
- IBM, certaines parties étant disponibles à l'adresse suivante : http://oss.software.ibm.com/icu4j/

Pour obtenir plus d'informations sur ces technologies tiers et connaître les avis de non-responsabilité et les restrictions qui leur sont propres, reportez-vous à http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF) : Copyright © Sun Microsystems, Inc. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, accédez au site http://www.java.sun.com/products/javabeans/glasgow/jaf.html et cliquez sur Download (Télécharger) pour pouvoir afficher la licence correspondante (License).
- JavaMail : Copyright © Sun Microsystems, Inc. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, accédez au site http://www.java.sun.com/products/javamail/downloads/index.html et cliquez sur Download (Télécharger) pour pouvoir afficher la licence correspondante (License).
- Java Ace, par Douglas C. Schmidt et son groupe de recherche de Washington University et Tao (avec classes enveloppantes ACE) par Douglas C. Schmidt et son groupe de recherche de Washington University, University of California, Irvine et Vanderbilt University. Copyright © 1993-2005. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://www.cs.wustl.edu/~schmidt/ACE-copying.html et http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html.
- Java Authentication et Authorization Service Modules, sous licence Lesser General Public License. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://free.tagish.net/jaas/index.jsp.
- Java Network Launching Protocol (JNLP) : Copyright © Sun Microsystems, Inc. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, accédez au site http://www.java.sun.com/products/javawebstart/download-jnlp.html et cliquez sur Download (Télécharger) pour pouvoir afficher la licence correspondante (License).
- Java Service Wrapper : parties protégées par copyright comme suit : Copyright © 1999, 2004 Tanuki Software et Copyright © 2001 Silver Egg Technology. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE : Copyright © 2002-2005, JIDE Software, Inc.
- jTDS est concédé sous licence Lesser GNU Public License. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://jtds.sourceforge.net/.
- MDateSelector : Copyright © 2005, Martin Newstead, concédé sous licence Lesser General Public License. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://web.ukonline.co.uk/mseries.
- Monarch Charts : Copyright © 2005, Singleton Labs.

- Net-SNMP : certaines parties du code sont protégées par copyright par diverses entités, qui se réservent tous les droits. Copyright © 1989, 1991, 1992 par Carnegie Mellon University ; Copyright © 1996, 1998 à 2000, the Regents of the University of California ; Copyright © 2001 à 2003 Networks Associates Technology, Inc. ; Copyright © 2001 à 2003, Cambridge Broadband, Ltd. ; Copyright © 2003 Sun Microsystems, Inc. et Copyright © 2003 à 2004, Sparta, Inc. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://net-snmp.sourceforge.net.
- The OpenSSL Project : Copyright © 1998-2004, The Open SSL Project. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://www.openssl.org.
- Oracle Help pour Java : Copyright © 1994-2006, Oracle Corporation.
- RoboHELP Office : Copyright © Adobe Systems Incorporated, anciennement Macromedia.
- Skin Look and Feel (SkinLF) : Copyright © 2000-2006 L2FProd.com. Concédé sous licence Apache Software. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à https://skinlf.dev.java.net/.
- Sonic Software Corporation : Copyright © 2003-2004. Le logiciel SSC contient un logiciel de sécurité concédé sous licence par RSA Security, Inc.
- Tinyxml : pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://grinninglizard.com/tinyxmldocs/index.html.
- SecurityNexus : Copyright © 2003-2006, SecurityNexus, LLC. Tous droits réservés.
- Xalan et Xerces, chacun concédé sous licence par Apache Software Foundation Copyright © 1999-2004. Pour obtenir plus d'informations et connaître les avis de non-responsabilité et les restrictions, reportez-vous à http://xml.apache.org/dist/LICENSE.txt.
- yWorks : Copyright © 2003-2006, yWorks.

REMARQUE : lors de la publication de cette documentation, les liens ci-dessus étaient actifs. Si l'un de ces liens est rompu ou que les pages Web liées sont inactives, veuillez contacter Novell Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Sommaire

1 Intégration à Remedy **1-1**

Configuration 1-2
Flux de données Remedy vers Sentinel 1-7
Installation de Sentinel 1-10
Configuration des flux de données Remedy vers Sentinel 1-11

2 Opérations liées à Remedy Help Desk **2-1**

Opérations liées à Remedy Help Desk 2-1
Reconfiguration manuelle des paramètres de l'interface Remedy 2-2
Paramètres Remedy 2-2
Modification du mot de passe Remedy 2-2

3 Installation de HP OpenView Service Desk pour Windows **3-1**

Configuration système requise 3-2
Installation 3-2
Configuration de HP OpenView Service Desk 3-3
Activation de l'interface Service Desk - Sentinel (bi-directionnelle) 3-5

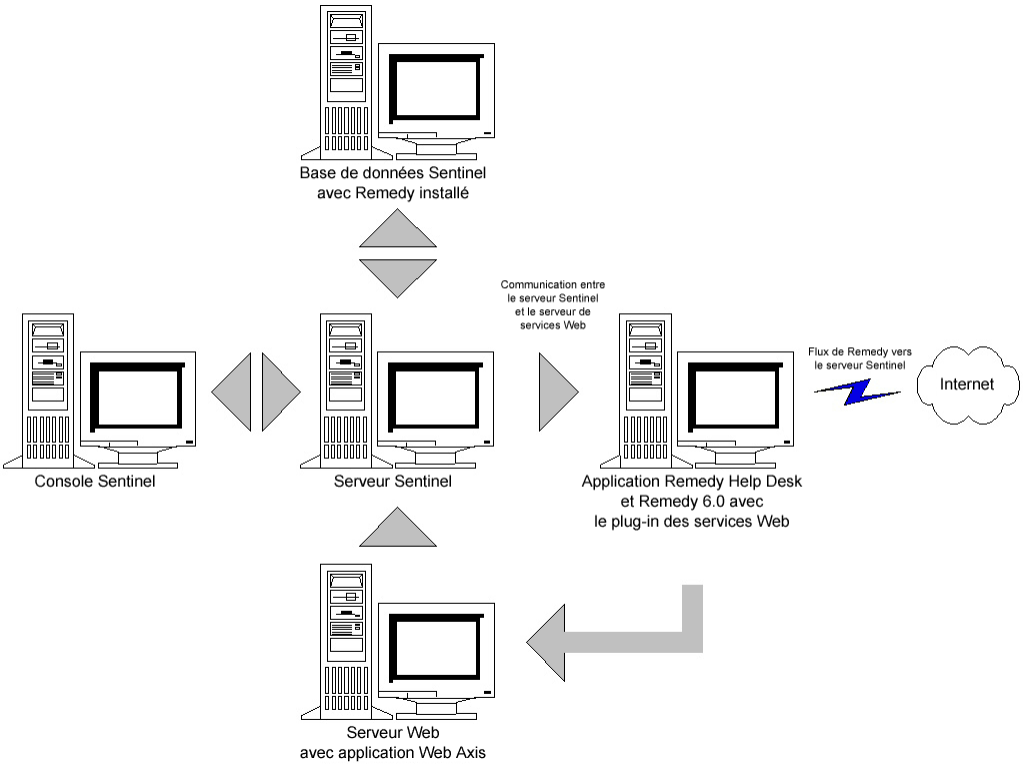
4 Intégration de HP OpenView Service Desk **4-1**

HP OpenView Service Desk 4-1
Envoi d'incidents à HP OpenView Service Desk 4-2
Client HP OpenView Service Desk 4-5
HP OpenView Service Desk – Interface bi-directionnelle 4-7
Reconfiguration manuelle des paramètres de l'interface HP OpenView Service Desk 4-7

1 Intégration à Remedy

Vous pouvez intégrer Remedy à Sentinel v4.2 ou v5 pour créer des applications de workflow entre le système de tickets de dépannage Remedy et le système Sentinel. Les principales caractéristiques de cette intégration sont les suivantes :

- Possibilité de créer un cas dans Remedy Help Desk suite à un incident survenu dans Sentinel
- Possibilité de mettre à jour un cas associé dans Remedy Help Desk lors de la mise à jour d'un incident Sentinel
- Possibilité de mettre à jour un incident Sentinel lors de la mise à jour d'un cas associé dans Remedy Help Desk



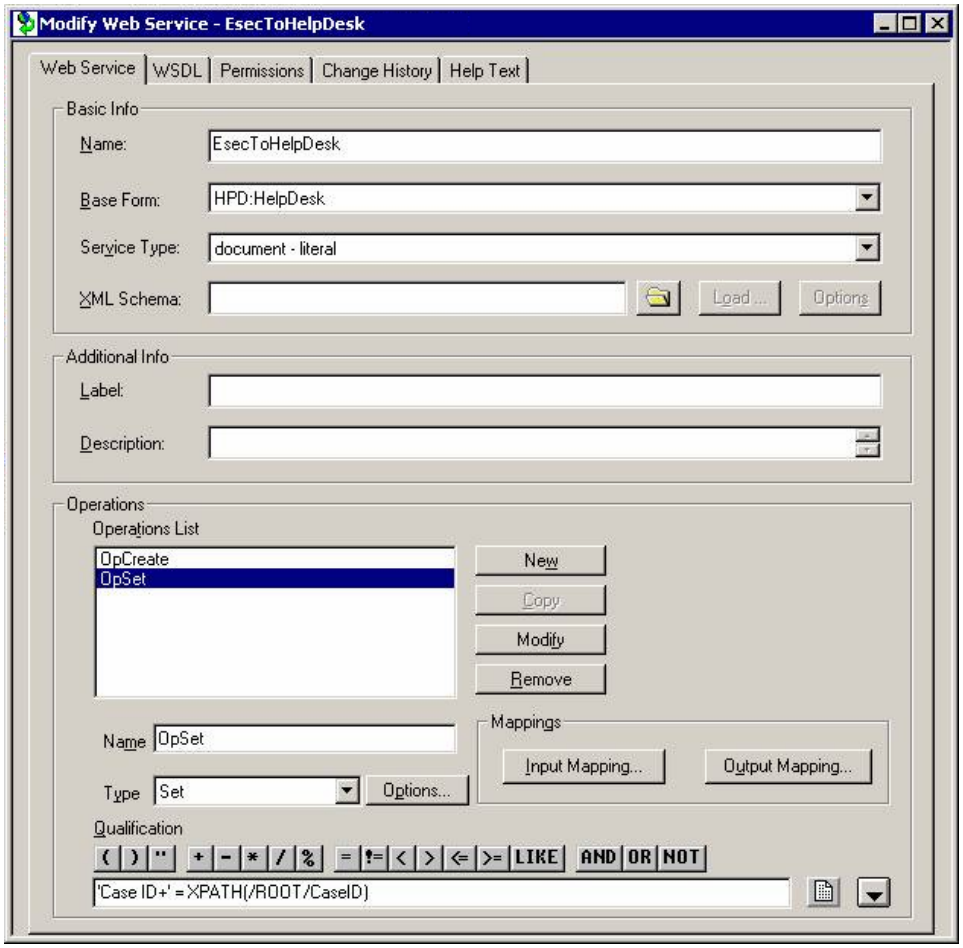
Configuration

Pour modifier le formulaire Remedy Help Desk Case (Cas Remedy Help Desk)

1. Connectez-vous à *Remedy Administrator* > *Forms* (Formulaires), double-cliquez sur *HPD HelpDesk*.
2. Afin que l'intégration avec Sentinel puisse être prise en charge, vous devez ajouter deux champs de caractères au formulaire Help Desk Case : EsecIncidentId et Attachment Pool (Pool de pièces jointes). Ces entrées de champs permettront d'ajouter les incidents au formulaire sous forme de pièces jointes.
3. Pour ajouter le champ de caractères EsecIncidentId
   - Cliquez sur le bouton New Character Field (Nouveau champ de caractères) et placez-le sur le formulaire.
   - Sous l'onglet Display (Affichage), définissez une étiquette.
   - Sous l'onglet Database (Base de données), dans le champ Name (Nom), définissez le nom sur EsecIncidentID.
4. Pour ajouter le champ de caractères Attachment Pool (Pool de pièces jointes) avec les trois champs suivants : EsecEvents, EsecVuln et EsecAdv
   - Cliquez sur le bouton *Create Attachment Pool* (Créer pool de pièces jointes).
   - Sous l'onglet Display (Affichage), entrez un nom d'étiquette dans le champ correspondant (par ex. : pièces jointes esec).
   - Sous Attach Fields (Attacher champs), dans la zone Enter Attachments Field Label (Entrez l'étiquette des champs relatifs aux pièces jointes), entrez :
     - EsecEvent et cliquez sur Add (Ajouter).
     - EsecVuln et cliquez sur Add (Ajouter).
     - EsecAdv et cliquez sur Add (Ajouter).
5. Cliquez sur *Save* (Enregistrer).

Pour créer le service Web

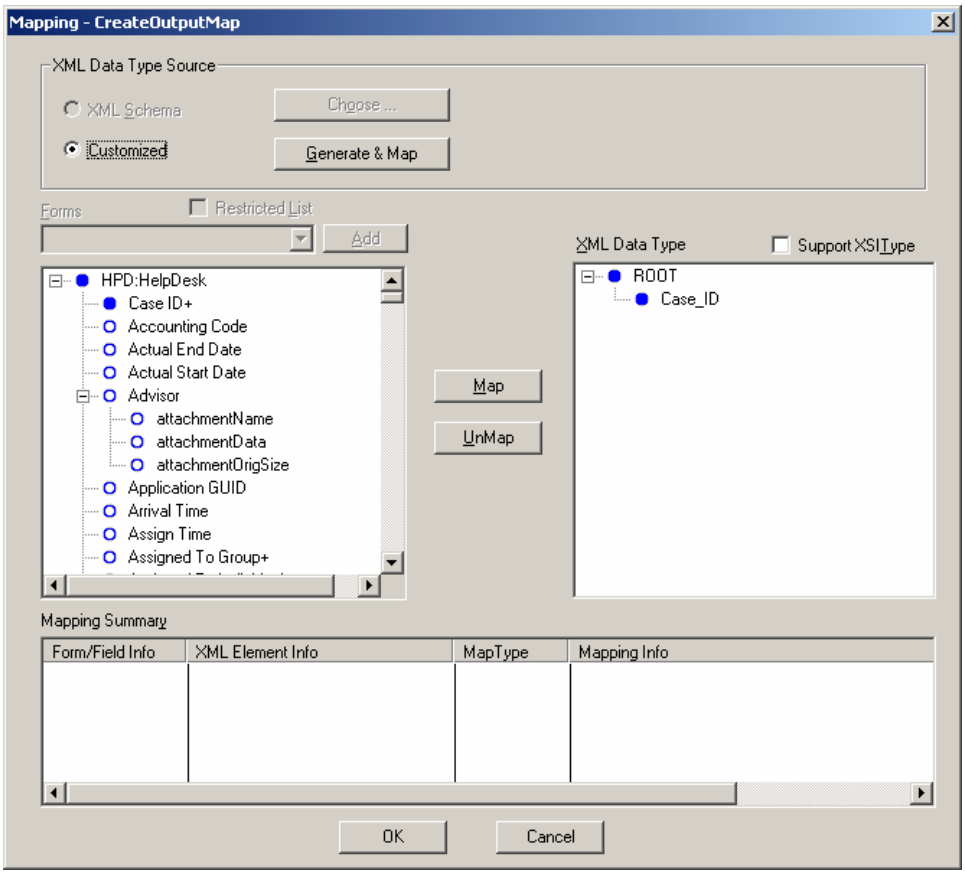
1. Dans Remedy Administrator, mettez en surbrillance *Web Services* (Services Web) dans le volet de navigation. Cliquez avec le bouton droit sur *New Web Services* (Nouveaux services Web) et cliquez sur l'onglet *Web Services* (Services Web).



2. En prenant comme base le formulaire Help Desk Case, créez un service Web appelé *EsecToHelpDesk* et sélectionnez HPD HelpDesk dans le champ Base Form (Formulaire de base).
3. Créez les deux opérations suivantes pour ce service Web :
   - opCreate
   - opSet

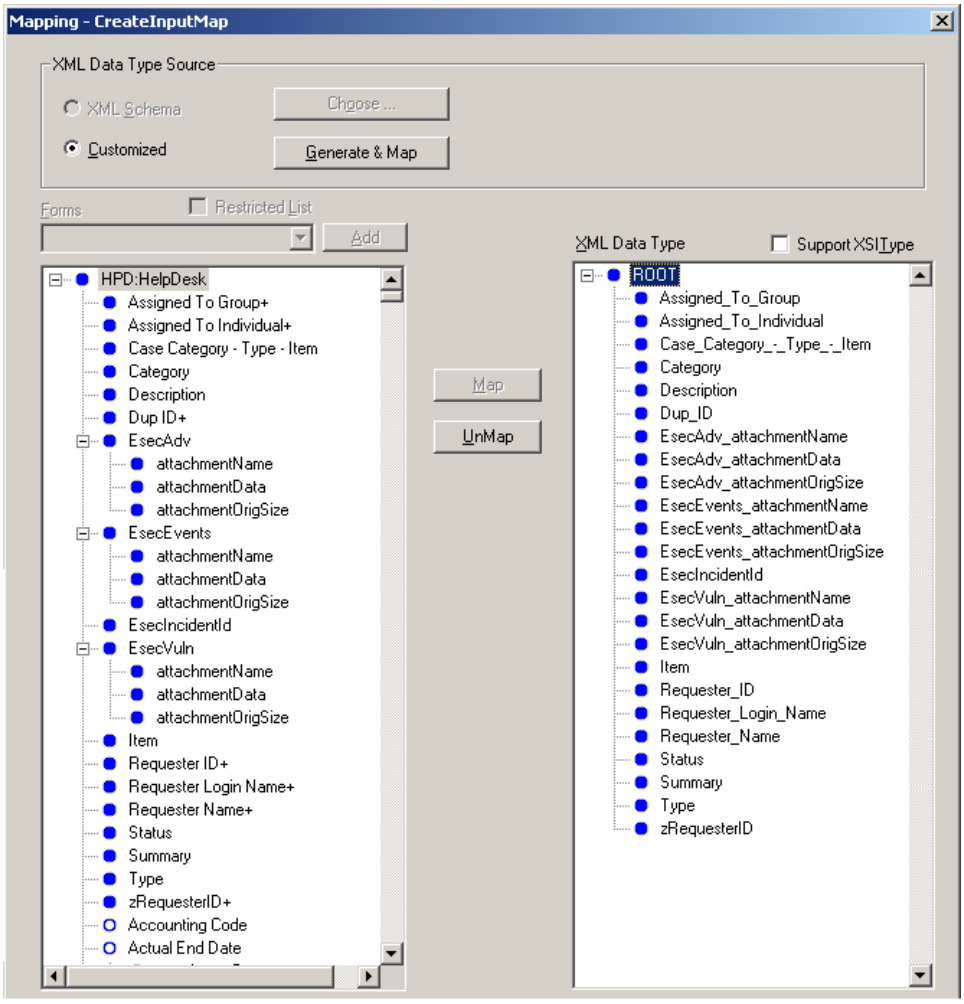
   et supprimez toute autre opération.

4. Sélectionnez OpCreate et cliquez sur le bouton Output Mapping (Assignation de sortie). Votre écran doit correspondre à l'illustration suivante.



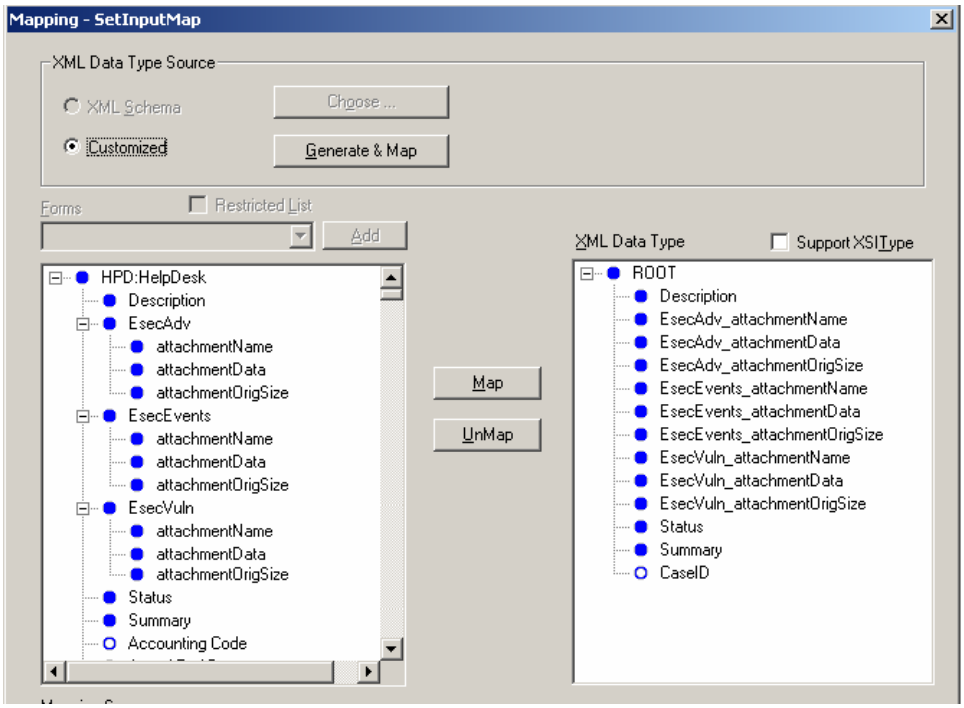
Sélectionnez le bouton Input Mapping (Assignation d'entrée) pour l'opération opCreate. Votre écran doit correspondre à l'illustration suivante.

REMARQUE : pour supprimer un élément, mettez-le en surbrillance, cliquez avec le bouton droit dessus et sélectionnez *Cut* (Couper).

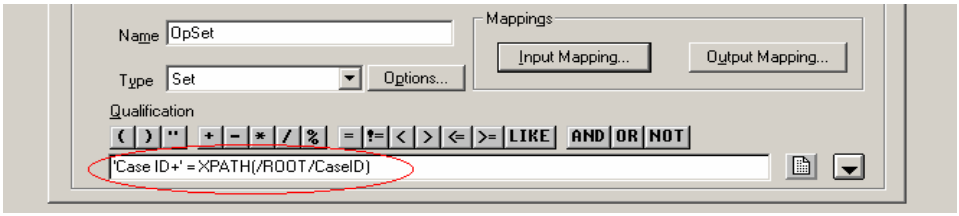


Cliquez sur *Save* (Enregistrer).

Sélectionnez le bouton Input Mapping (Assignation d'entrée) pour l'opération opSet. Votre écran doit correspondre à l'illustration suivante.



L'opération opSet ne comporte pas d'assignation de sortie, mais nécessite que vous spécifiiez le champ Qualification :



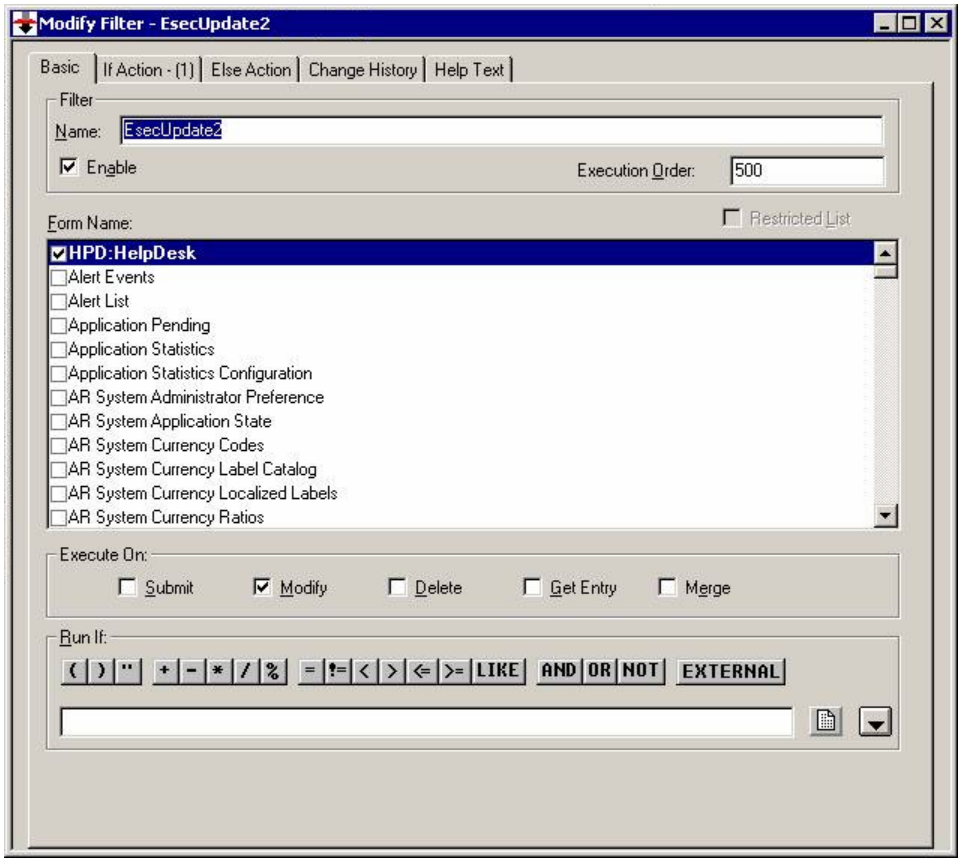
5. Accédez à l'onglet Permissions (Autorisations) et définissez le service sur Public en déplaçant Public de la gauche vers la droite. Cliquez sur *Save* (Enregistrer).

Flux de données Remedy vers Sentinel

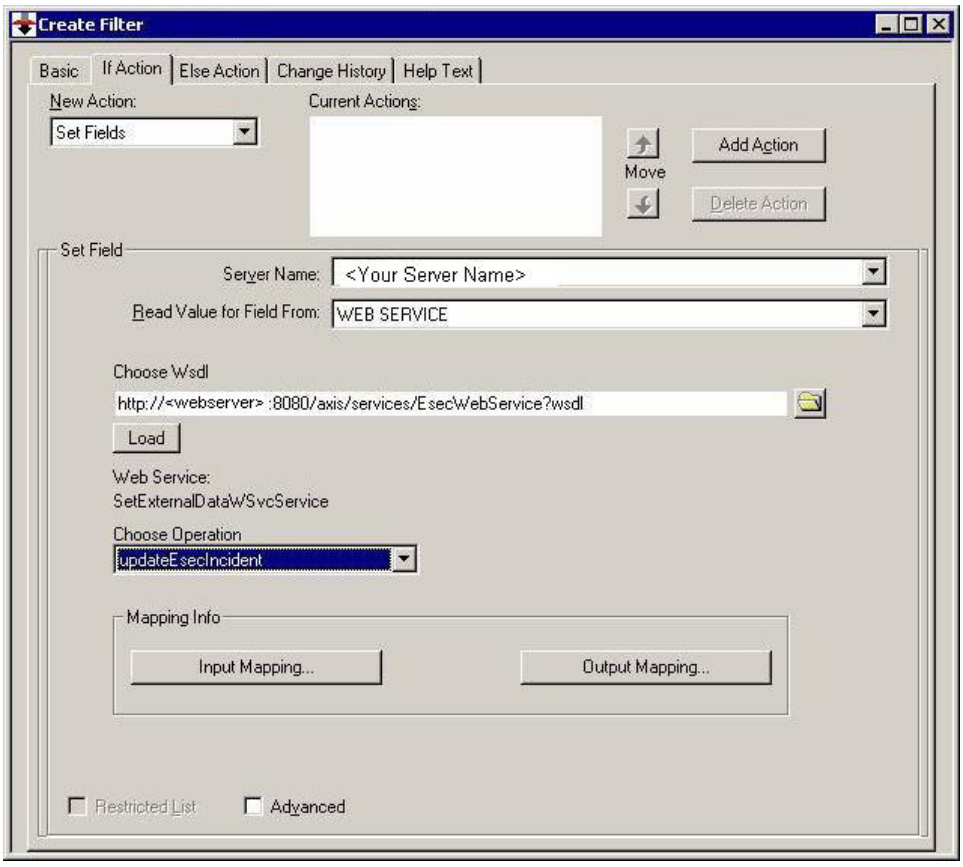
Pour que le service Web Sentinel soit accessible, l'application Axis Web doit être en cours d'exécution sur votre serveur Web lors du démarrage du serveur Sentinel.

Flux de données Remedy vers Sentinel

1. Dans Remedy Administrator, mettez en surbrillance Filters (Filtres) et cliquez avec le bouton droit sur *Add Filter* (Ajouter filtre).
2. Créez un filtre pour le formulaire Help Desk Case qui sera exécuté lors d'un événement de modification. Assurez-vous que votre écran corresponde bien à l'illustration suivante.

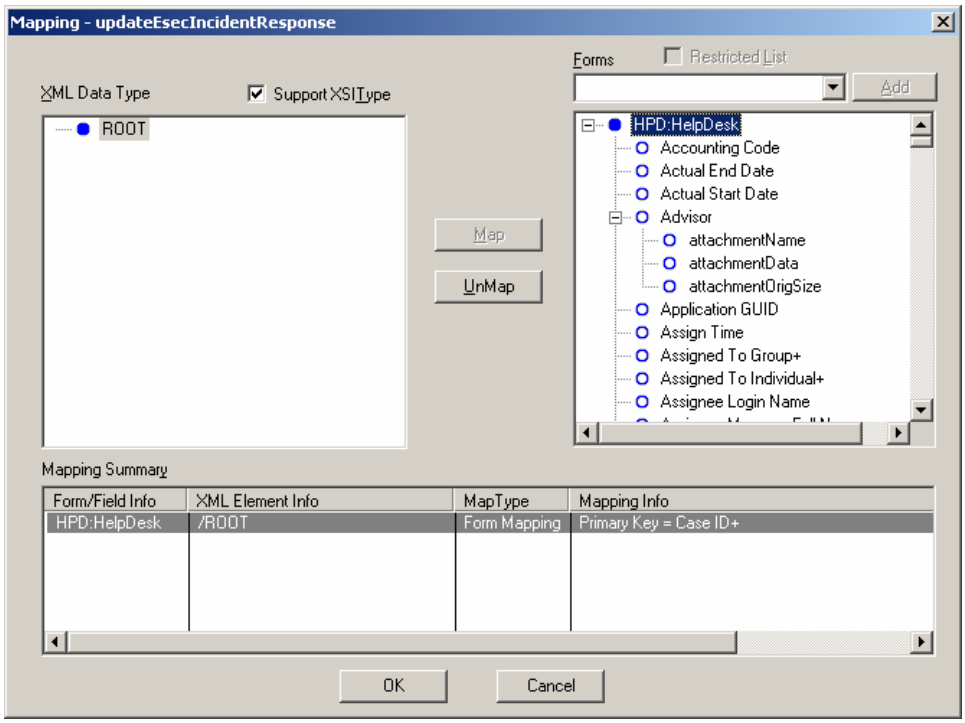


3. Sous l'onglet *If Action* (Action If), dans le menu déroulant *New Action* (Nouvelle action), sélectionnez l'action *Set Field* (Définir champ). Dans la section *Set Field*, sélectionnez *WEB SERVICE* (SERVICE WEB) et indiquez l'URL du service Web Sentinel (http://<Nom DNS ou adresse IP du serveur Web>:8080/axis/services/EsecWebService?wsdl).



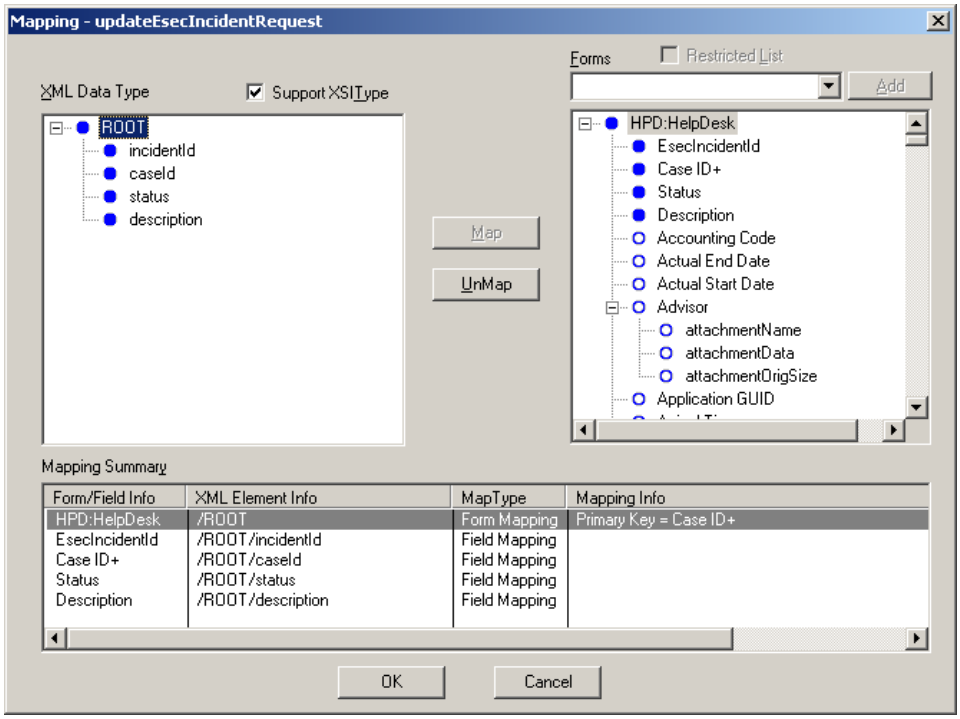
4. Dans le menu déroulant *Choose Operation* (Choisir opération), sélectionnez la méthode *updateEsecIncident* et définissez les assignations d'entrée et de sortie.

Cliquez sur le bouton Output Mapping (Assignation de sortie). Votre écran doit correspondre à l'illustration suivante.



Cliquez sur le bouton Input Mapping (Assignation d'entrée). Votre écran doit correspondre à l'illustration suivante.

REMARQUE : pour définir l'assignation, sélectionnez un élément dans le cadre de gauche (incidentId), sélectionnez un élément dans le cadre de droite (EsecIncidentId) et cliquez sur le bouton Map (Assigner).



REMARQUE : une fois la configuration terminée, dès que vous enregistrez une modification dans le formulaire Help Desk Case, cette dernière est soumise à un service Sentinel.

5. Cliquez sur *Save* (Enregistrer).

Installation de Sentinel

Vous devez disposer d'un compte Remedy pour pouvoir installer Sentinel avec Remedy. Les informations suivantes vous seront demandées à partir de ce compte.

REMARQUE : vous devez disposer d'une autorisation Remedy Integration (Intégration Remedy).

- Nom d'utilisateur
- Mot de passe
- Nom du demandeur
- ID du demandeur
- Login du demandeur
- Nom du groupe (facultatif)
- Nom individuel (facultatif)
- Nom du serveur
- Nom du service

Pour permettre les flux de données Remedy vers Sentinel, vous serez invité à entrer les informations suivantes :

- Serveur Web Sentinel (<nom de la machine:port>)
- Nom utilisateur Sentinel (par ex. esecadm)
- ID d'utilisateur Sentinel
- Sentinel UUID
- ID de verrou Sentinel (généralement défini sur 1 ou 2)

Pour installer Sentinel

1. Sélectionnez Remedy Integration (Intégration Remedy) lors de l'installation.
2. Gardez à disposition les informations indiquées ci-dessus, elles vous serviront au cours de l'installation.

Configuration des flux de données Remedy vers Sentinel

Si vous envisagez l'intégration de produits tiers (Intégration Remedy), il est recommandé d'effectuer les opérations d'installation et de configuration en respectant l'ordre suivant :

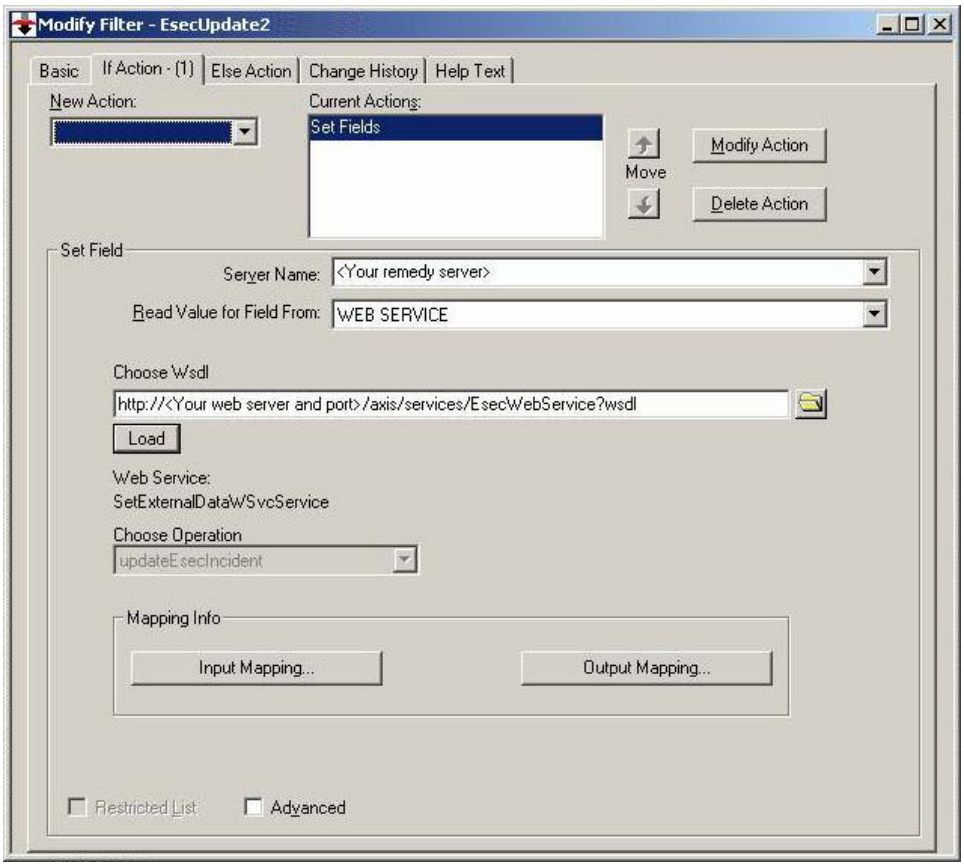
- Installez l'application Remedy Help Desk et Remedy 6.0 avec le plug-in des services Web.
- Configurez les nouveaux services Web et de filtres dans l'application Remedy Help Desk.
- Installez Sentinel.

Pour permettre les flux de données de Remedy vers Sentinel, vous devez suivre la procédure suivante :

- Pour que le service Web Sentinel soit accessible, l'application Axis Web doit être en cours d'exécution sur votre serveur Web avant le démarrage du serveur Sentinel.
- Copiez tous les fichiers jar des emplacements suivants sur votre serveur Sentinel dans le répertoire <application Axis Web>\webclient\lib.
  - %ESEC_HOME%\lib
  - %ESEC_HOME%\sentinel\console
  - %ESEC_HOME%\communicator (v4.2 uniquement)
- Copiez les fichiers configuration.xml et. keystore du serveur Sentinel à l'emplacement de votre choix sur le serveur Web. Vous trouverez ces deux fichiers sous %ESEC_HOME%.
  - Modifiez le fichier configuration.xml sur le serveur Web de sorte qu'il pointe vers le fichier. keystore.
  - Ajoutez l'option JVM suivante à votre serveur Web,

```
Dcom.esecurity.configurationfile=<chemin vers
   configuration.xml>\configuration.xml
```

- Créez un filtre pour le formulaire Help Desk Case qui sera exécuté lors d'un événement de modification. Ce filtre permet d'appeler le serveur Web Sentinel.



2 Opérations liées à Remedy Help Desk

L'intégration de Remedy permet de créer des applications de workflow. Les fonctions générées par cette intégration sont les suivantes :

- Possibilité de créer un cas dans Remedy Help Desk basé sur un incident survenu dans Sentinel
- Possibilité de mettre à jour un cas associé dans Remedy Help Desk lors de la mise à jour d'un incident Sentinel
- Possibilité de mettre à jour un incident Sentinel lors de la mise à jour d'un cas associé dans Remedy Help Desk

Opérations liées à Remedy Help Desk

Pour envoyer un incident à Remedy Help Desk (v5.0.1 et ultérieures)

1. Cliquez sur l'onglet *Incidents*.
2. Dans le volet de navigation, développez le dossier *Vues d'incidents* et mettez en surbrillance *Gestionnaire de vues d'incidents*.

   REMARQUE : si un des incidents est déjà défini pour un système externe différent, vous ne pouvez pas le modifier.

3. Développez l'une des vues d'incidents et double-cliquez sur l'incident recherché. L'incident s'affiche.
4. Cliquez sur le bouton *Remedy*.

   Un onglet Données externes et un bouton Remedy viennent s'ajouter à la page de l'incident.

Pour mettre à jour un incident envoyé à Remedy Help Desk (v5.0.1. et ultérieures)

1. Cliquez sur l'onglet *Incidents*.
2. Développez le volet de navigation sur la gauche et double-cliquez sur un incident destiné à Remedy Help Desk.
3. Cliquez sur le bouton *Remedy* dans la page de l'incident. Les annotations sont ajoutées sous l'onglet Données externes.

Reconfiguration manuelle des paramètres de l'interface Remedy

Lors de la première installation de l'interface Remedy Help Desk, les paramètres Remedy sont stockés dans le fichier das_query.xml. Utilisez les informations de cette section pour modifier ces paramètres une fois l'installation terminée.

Paramètres Remedy

Les paramètres Remedy sont stockés dans le fichier das_query.xml sous le composant RemedyARServerService.

Modification du mot de passe Remedy

Les mots de passe Remedy sont stockés dans le fichier das_query.xml sous un format chiffré. Pour les redéfinir, vous devez utiliser l'utilitaire décrit ci-dessous.

Pour redéfinir le mot de passe de l'interface Remedy

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

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

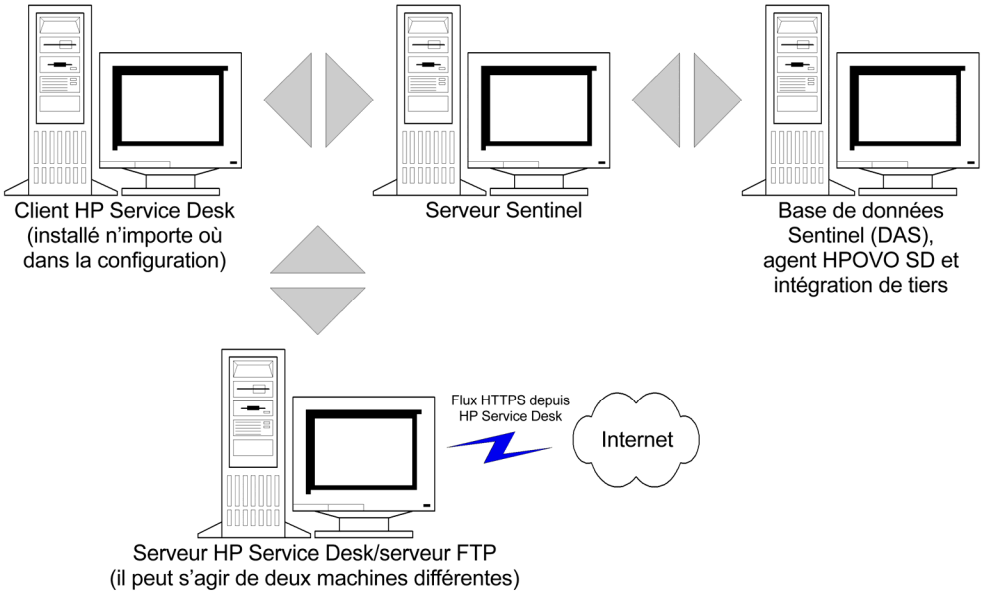
   - -r correspond au mot de passe Remedy.

3 Installation de HP OpenView Service Desk pour Windows

L'intégration bi-directionnelle de Sentinel avec HP OpenView Service Desk, qui fait l'objet d'une licence distincte, apporte de nouvelles fonctionnalités à la console Sentinel. Grâce aux capacités de gestion des actifs de HP OpenView Service Desk, Sentinel peut fournir des informations de référence dans le cadre du traitement des attaques et menaces à la sécurité. Ces nouvelles fonctionnalités permettent les opérations suivantes :

- l'envoi d'incidents à HP Service Desk (SD) ;
- l'association en pièce jointe d'événements à un incident HP SD ;
- l'association en pièce jointe des informations de vulnérabilité à un incident HP SD ;
- la requête et l'indication des informations relatives aux éléments de configuration (Actif) à la fois dans la console Sentinel et SD ;
- Intégration bi-directionnelle : envoi des mises à jour de SD vers Novell et de Novell vers SD ;
- la mise à jour de l'état des incidents SD dans la console Sentinel de Novell ;
- la mise à jour de l'état des incidents Sentinel dans HP SD.

La configuration décrite ci-dessous représente une installation standard. Votre configuration peut être différente.



Configuration système requise

Pour connaître les configurations logicielle et matérielle requises pour le client, le serveur et l'agent HP OpenView Service Desk, reportez-vous au Guide d'installation de HP OpenView Service Desk.

Sentinel prend en charge les versions suivantes de HP OpenView Service Desk :

- Serveur HP OpenView Service Desk, version 4.5 avec Service Pack 8 (4.5.0588.0802 SP 8)
- Client HP OpenView Service Desk, version 4.5 avec Service Pack 8
- Agent HP OpenView Service Desk, version 4.5 avec Service Pack 8
- Sentinel 4.2.1.8 ou 4.2.1.15 pour Windows
- Tout serveur FTP tiers

Le serveur HP OpenView Service Desk et le client HP OpenView Service Desk doivent être installés sur l'ordinateur désigné comme serveur Service Desk. Pour plus d'informations sur l'installation de Service Desk, reportez-vous au Guide d'installation de HP OpenView Service Desk.

Pour que l'interface bi-directionnelle soit opérationnelle, un agent HP OpenView doit être installé sur l'ordinateur doté du fichier das_cmd.bat. Cette interface permet à HP Service Desk d'informer Sentinel de toute modification apportée à l'état d'un incident Sentinel par un utilisateur Service Desk. Ces incidents doivent provenir de la console Sentinel.

Pour que Service Desk puisse gérer les pièces jointes, vous devez installer un serveur FTP (généralement sur le serveur Service Desk) et configurer Service Desk de sorte qu'ils puissent communiquer. Vous pouvez utiliser n'importe quel serveur FTP tiers. Pour plus d'informations sur l'installation du serveur FTP, reportez-vous au Guide d'installation de votre serveur FTP.

Installation

Si vous envisagez d'installer également HP OpenView Operations, il est recommandé de procéder à son installation préalablement à celle de HP OpenView Service Desk.

REMARQUE : lors de la première installation de l'interface tierce HP OpenView Service Desk, les paramètres Service Desk et OpenView sont stockés dans le fichier das_query.xml. Pour modifier l'un de ces paramètres (tels que le nom d'utilisateur ou le mot de passe), reportez-vous à la section *Reconfiguration manuelle des paramètres de l'interface HP OpenView Service Desk.*

Il est recommandé de respecter l'ordre d'installation suivant :

- Serveur FTP

  REMARQUE : pour plus d'informations sur l'installation du serveur FTP, reportez-vous au Guide d'installation de votre serveur FTP.

- Serveur HP OpenView Service Desk avec Service Pack 8, peut être installé sur le même ordinateur que le serveur FTP
- Client HP OpenView Service Desk avec Service Pack 8
- Agent HP OpenView Service Desk avec Service Pack 8 (pour activer l'interface bi-directionnelle), doit être sur l'ordinateur sur lequel le service DAS est installé

  REMARQUE : pour plus d'informations sur l'installation du logiciel HP OpenView Service Desk, reportez-vous à son Guide d'installation.

- Installation de l'intégration de tiers Sentinel
  - HP OpenView Service Desk

  REMARQUE : pour obtenir des informations sur l'installation, reportez-vous aux notes de version de Sentinel v4.2.1.8 et au Guide d'installation de Sentinel v4.2 pour Windows et Solaris.

Configuration de HP OpenView Service Desk

La configuration de HP OpenView Service Desk s'effectue par le biais du client Service Desk. Avant de modifier la configuration de HP Service Desk afin qu'il puisse communiquer avec le serveur FTP, rassemblez les informations suivantes :

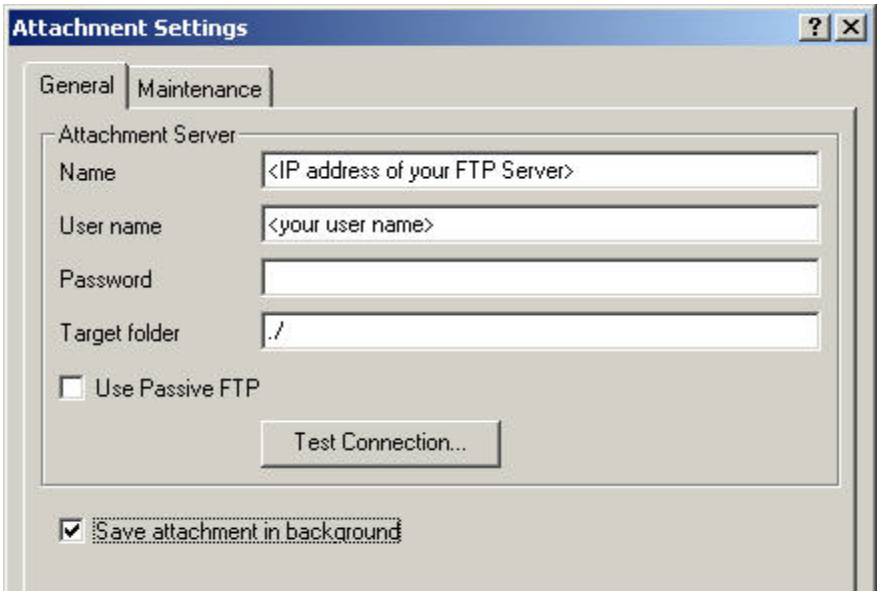
- Nom : adresse IP du serveur FTP.
- Nom d'utilisateur/Mot de passe : tout utilisateur défini sur le serveur FTP.
- Dossier cible : il est recommandé de saisir « ./ ». De cette manière, le répertoire FTP est placé au niveau du répertoire FTP actuel.
- Désactivez la case Use Passive FTP (Utiliser le mode FTP passif).
- Activez la case Save attachment in background (Enregistrer la pièce jointe en arrière-plan).

REMARQUE : pour obtenir des informations détaillées sur la configuration, reportez-vous à la section relative aux tâches post-installation du Guide d'installation de HP OpenView Service Desk.

Pour définir les paramètres de pièce jointe

1. Démarrez le client HP Service Desk.
2. Cliquez sur *Tools* (Outils) > *System* (Système).
3. Cliquez sur *System Panel* (Panneau système) dans le volet de navigation situé à gauche.
4. Double-cliquez sur *Attachment Settings* (Paramètres de pièce jointe). Entrez :
   - Name (Nom) : adresse IP du serveur FTP.
   - Username/Password (Nom d'utilisateur/Mot de passe) : tout utilisateur défini sur le serveur FTP.
   - Target Folder (Dossier cible) : il est recommandé de saisir « ./ ». De cette manière, le répertoire FTP est placé au niveau du répertoire FTP actuel.
   - Désactivez la case *Use Passive FTP* (Utiliser le mode FTP passif).
   - Activez la case *Save attachment in background* (Enregistrer la pièce jointe en arrière-plan).

REMARQUE : pour obtenir des informations détaillées sur la configuration, reportez-vous à la section relative aux tâches post-installation du Guide d'installation de HP OpenView Service Desk.



5. Cliquez sur *Test Connection* (Connexion test).
6. Cliquez sur *Apply* (Appliquer), puis sur *OK*.

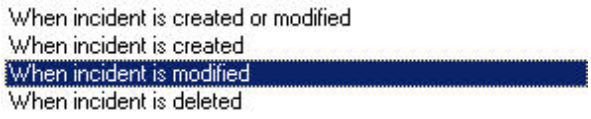
Activation de l'interface Service Desk - Sentinel (bi-directionnelle)

Cette option permet à HP OVO OpenView Service Desk d'informer Sentinel de toute modification apportée à l'état d'un incident (de Sentinel) par un utilisateur Service Desk. Grâce à cette fonction, vous avez la possibilité de suivre l'état actuel de chacun des incidents soumis à HP OVO OpenView Service Desk.

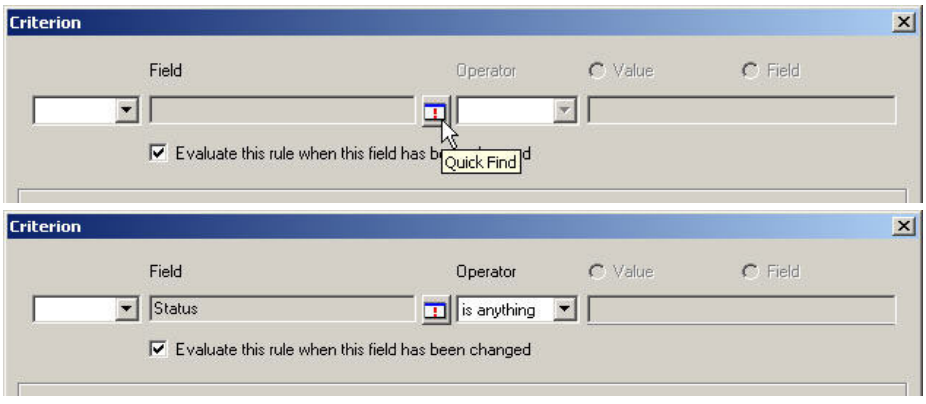
Pour que cette fonction soit activée, vous devez installer un agent HP OVO OpenView Service sur l'ordinateur doté du fichier das_cmd.bat. De cette manière, HP Service Desk peut exécuter l'utilitaire das_cmd de Sentinel.

Pour activer l'interface bi-directionnelle

1. Démarrez le client Service Desk.
2. Affichez la console de l'administrateur en sélectionnant *Tools* (Outils) > *System* (Système).
3. Cliquez sur Business Logic (Logique métier) dans le volet de navigation situé à gauche.
4. Double-cliquez sur *Database Rules* (Règles de base de données).
5. Double-cliquez sur *Incident*. La liste des règles de base de données s'affiche.
6. Cliquez avec le bouton droit dans la section Database Rules (Règles de base de données) et sélectionnez *New Database Rule* (Nouvelle règle de base de données).
7. Mettez en surbrillance *When incident is modified* (Lors de la modification d'un incident) et cliquez sur *Next* (Suivant).

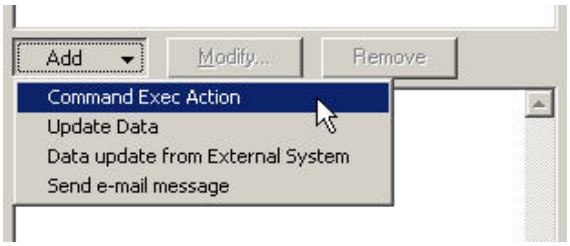


8. Cliquez sur le bouton *Condition...*.
9. Cliquez sur le bouton *Add Criterion*...(Ajouter un critère).
10. Cliquez sur le bouton *Quick Find* (Recherche rapide), sélectionnez *Status* (État), puis sélectionnez *is anything* (quelconque) dans le champ Operator (Opérateur).



Cliquez à deux reprises sur *OK*.

11. Cliquez sur *Add* (Ajouter). Sélectionnez *Command Exec Action* (Action d'exécution de la commande).



12. Ajoutez une nouvelle action Command Exec Action de sorte que le script « das_cmd.bat » soit exécuté sur le serveur Sentinel à chaque évaluation de la règle.

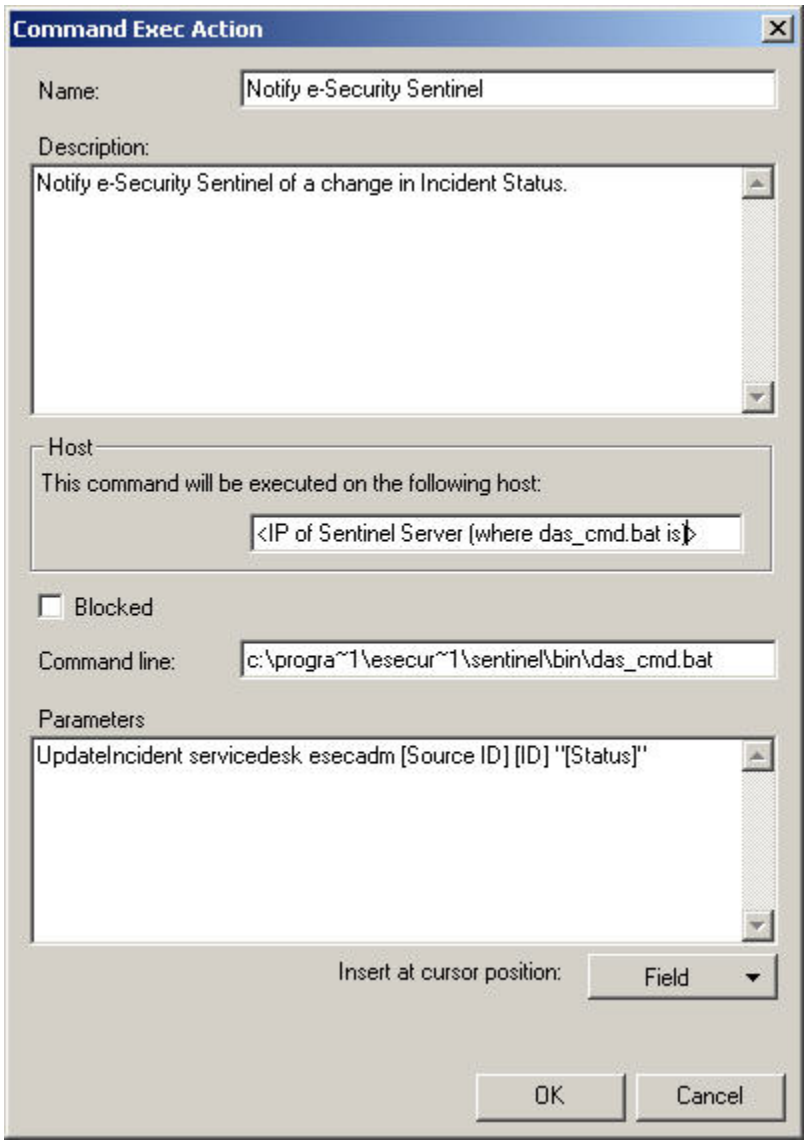
    Lorsque vous configurez l'action, assurez-vous de bien spécifier le nom (ou l'adresse IP) de votre serveur Sentinel (l'ordinateur sur lequel réside le script das_cmd.bat) dans la section Host (Hôte). Veillez également à indiquer le chemin d'accès complet du fichier das_cmd.bat situé sur le serveur Sentinel dans le champ Command line (Ligne de commande), tel que :

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

REMARQUE : utilisez la convention de dénomination DOS 8.3 pour spécifier les noms de répertoire avec espaces. Par exemple, utilisez « progra~1 » au lieu de « Program Files ».

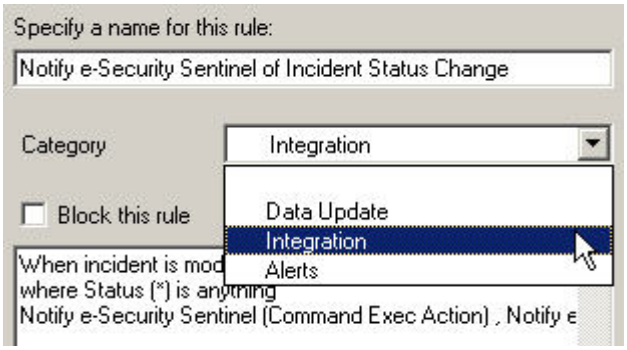
Enfin, n'oubliez pas d'indiquer l'option Parameters (Paramètres) comme suit :

```
UpdateIncident servicedesk esecadm [Source ID] [ID]
   « [Status] »
```



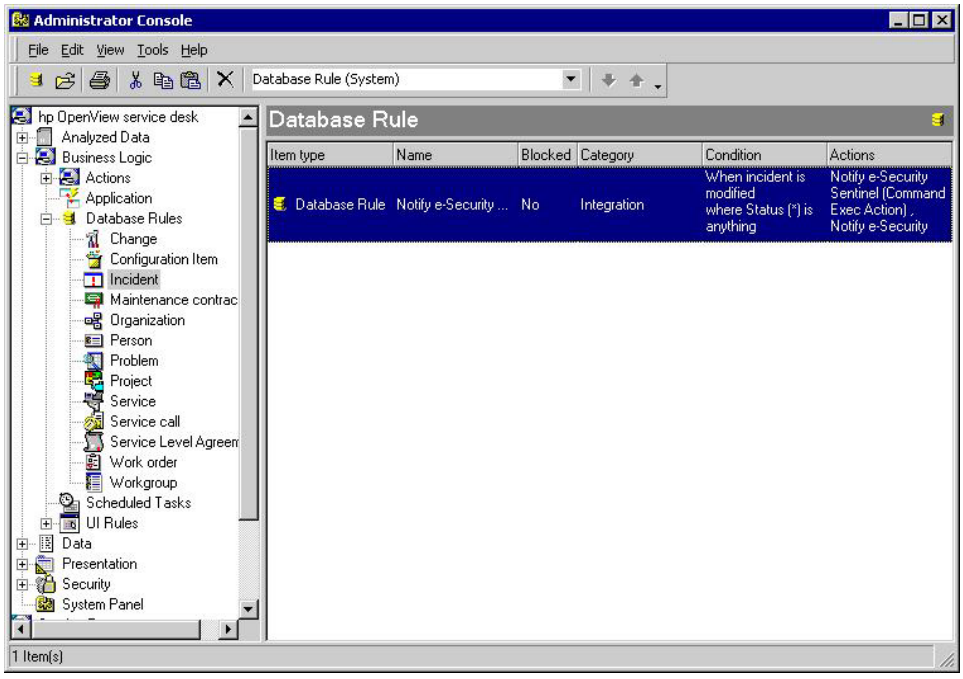
Attribuez le nom de votre choix à la nouvelle règle de base de données, accompagné d'une description. Cliquez sur *OK*, puis sur *Next* (Suivant).

13. Dans le champ Category (Catégorie), sélectionnez Integration (Intégration) et attribuez un nom à cette règle. N'activez pas la case *Block this rule* (Bloquer cette règle).



Cliquez sur *Finish* (Terminer).

14. À l'issue de cette configuration, une nouvelle règle s'affiche dans la liste des règles de base de données.



4 Intégration de HP OpenView Service Desk

L'intégration de HP OpenView Service Desk avec Sentinel vous permet d'envoyer des événements à HP OpenView Service Desk depuis n'importe quelle page d'affichage d'incidents et d'événements de Sentinel.

HP OpenView Service Desk

L'intégration de Sentinel avec HP OpenView Service Desk vous permet de bénéficier de nouvelles fonctionnalités de gestion des actifs. Ces fonctionnalités sont les suivantes :

- Envoi d'incidents à HP Service Desk (SD)
  - association en pièce jointe d'événements à un incident HP SD ;
  - association en pièce jointe des informations de vulnérabilité à un incident HP SD ;
  - association en pièce jointe des informations Advisor à un incident HP SD ;
  - requête et indication des informations relatives aux éléments de configuration (Actif) dans le centre de contrôle Sentinel.
- Mise à jour de l'état des incidents SD dans le centre de contrôle Sentinel
- Mise à jour de l'état des incidents Sentinel dans HP SD

Les informations sur les incidents Sentinel que vous pouvez envoyer à HP OpenView Service Desk sont les suivantes :

- ID de l'incident Sentinel
- État
- Titre
- Annotations/Historique
- Événements (pièce jointe)
- Informations sur la vulnérabilité (pièce jointe)
- Informations Advisor (pièce jointe)

Certaines opérations, comme la conversion et l'assignation des états, se font automatiquement lors de l'envoi d'informations à HP OpenView Service Desk ou de la réception d'informations depuis cette application.

La conversion et l'assignation des états Sentinel vers les états Service Desk se présentent comme suit :

État Sentinel	État Service Desk
Open (Ouvert)	Registered (Enregistré)
Acknowledged (Reconnu)	Waiting (En attente)
Assigned (Assigné)	Informed (Notifié)
Investigating (Enquête en cours)	In Progress (En cours)
False Positive (Faux positif)	Closed (Fermé)
Verified (Vérifié)	Completed (Terminé)
Approved (Approuvé)	In Progress (En cours)
Closed (Fermé)	Closed (Fermé)

La conversion et l'assignation des états Service Desk vers les états Sentinel se présentent comme suit :

État Service Desk	État Sentinel
Registered (Enregistré)	Open (Ouvert)
In Progress (En cours)	Investigating (Enquête en cours)
Waiting (En attente)	Acknowledged (Reconnu)
Completed (Terminé)	Verified (Vérifié)
Informed (Notifié)	Assigned (Assigné)
Closed (Fermé)	Closed (Fermé)

Envoi d'incidents à HP OpenView Service Desk

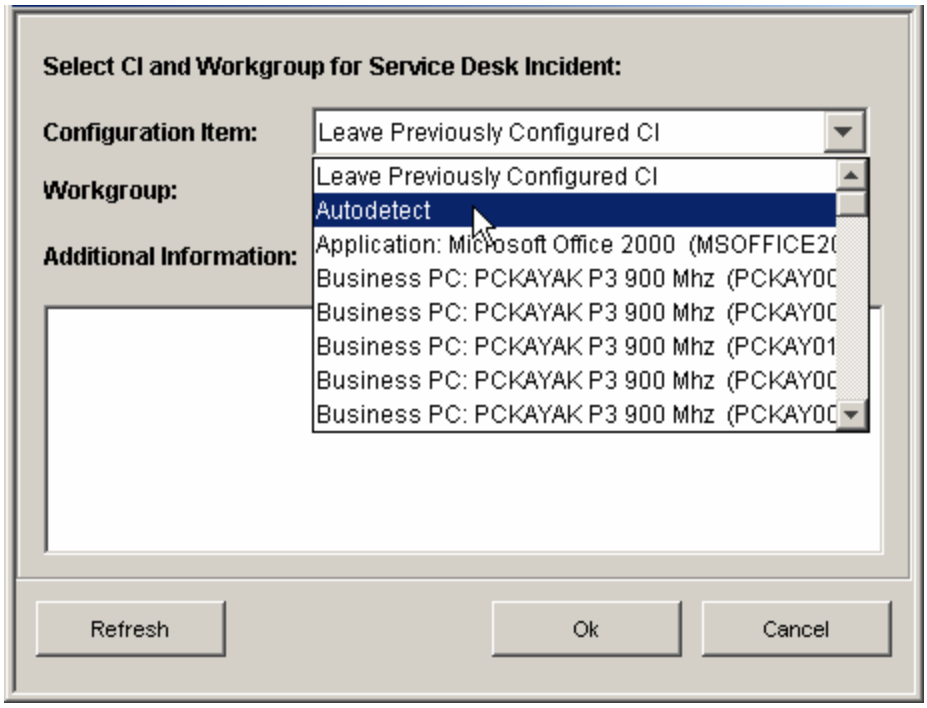
Pour envoyer un incident à HP OpenView Service Desk

1. Cliquez sur l'onglet *Incidents*.
2. Dans le volet de navigation, développez le dossier *Vues d'incidents* et mettez en surbrillance *Gestionnaire de vues d'incidents*.

   REMARQUE : si un des incidents est déjà défini pour un système externe différent, vous ne pouvez pas le modifier.

3. Développez l'une des vues d'incidents et double-cliquez sur l'incident recherché. L'incident s'affiche.
4. Cliquez sur le bouton *HP SD*.

5. La fenêtre *Envoyer l'incident au centre de service HP* s'affiche. La boîte de dialogue *Envoyer l'élément au Service Desk* contient une liste de sélection intitulée Élément de configuration. Cette liste répertorie les éléments de configuration accessibles par HP Service Desk.

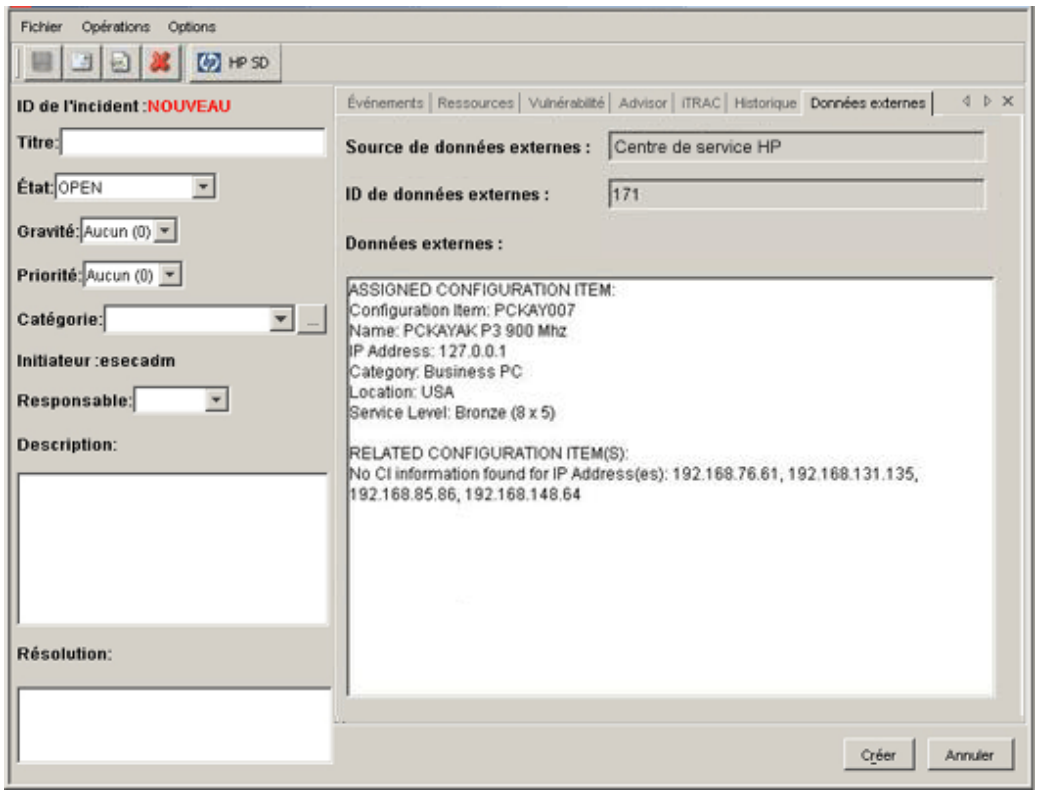


L'option *Détection automatique* figure dans cette liste. Si vous la sélectionnez, Sentinel tente de déterminer l'élément de configuration connexe de Service Desk à l'aide des adresses IP de destination des événements associés à l'incident Sentinel.

6. (Facultatif) La boîte de dialogue *Envoyer l'élément au Service Desk* fournit également la liste déroulante Groupe de travail dans laquelle vous pouvez sélectionner les groupes de travail accessibles par Service Desk.

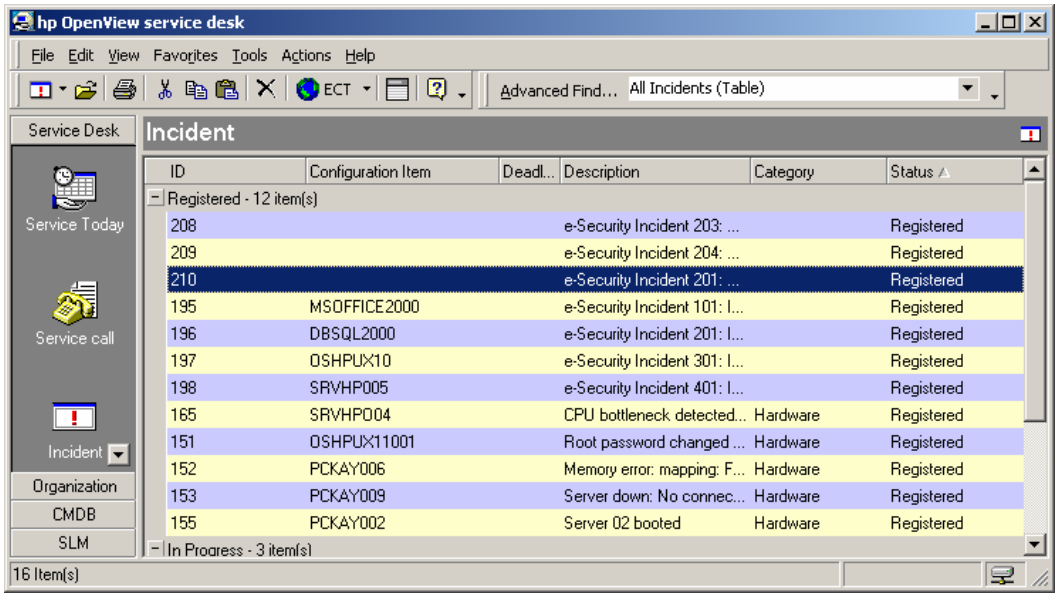
7. Cliquez sur *OK*. L'incident est transmis à *HP OpenView Service Desk*.

REMARQUE : un onglet Données externes est ajouté à la page contenant l'incident Sentinel. Il indique l'ID de l'incident Service Desk et l'élément de configuration Service Desk auquel le nouvel incident a été attribué.



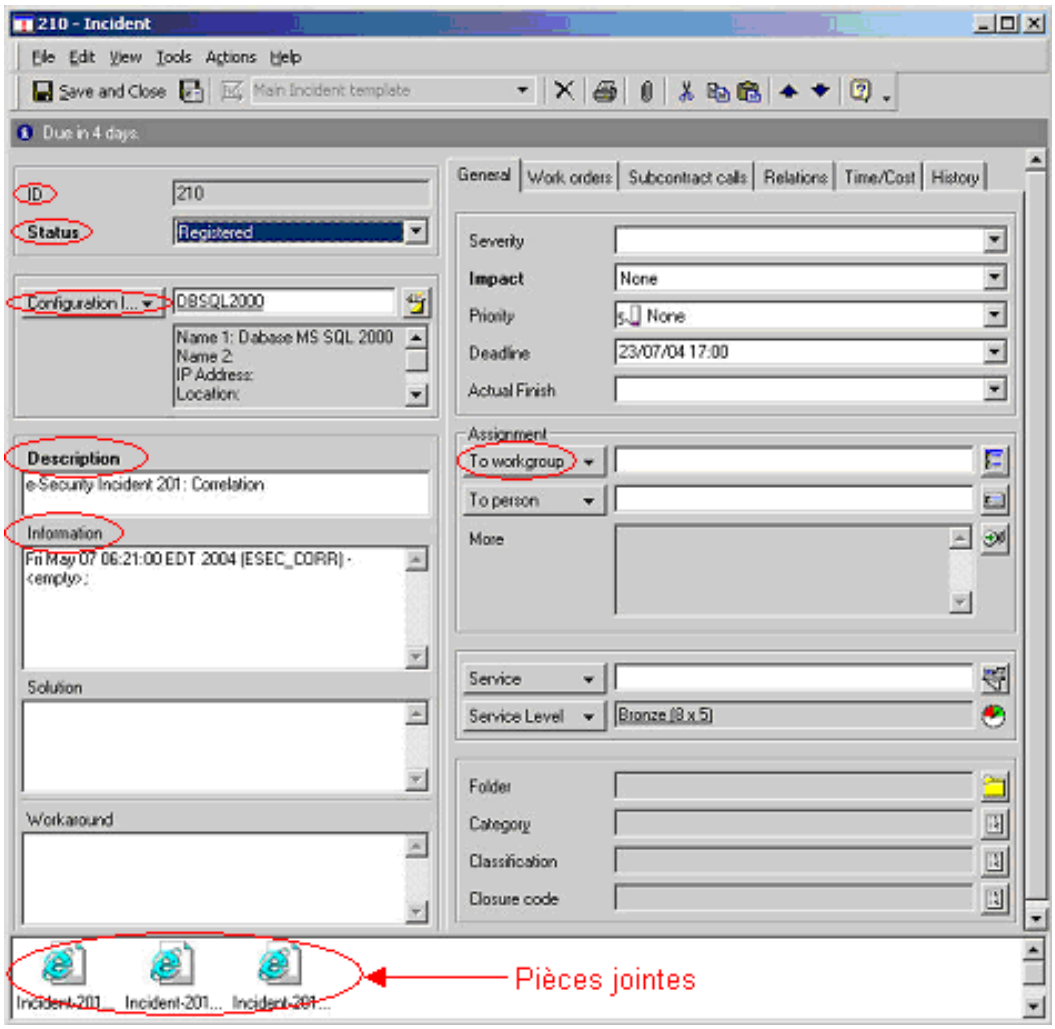
Client HP OpenView Service Desk

Lorsqu'un incident est envoyé à HP OpenView Service Desk, il apparaît dans le client HP OpenView Service Desk, où il est répertorié par son ID de données étendues (Extended Data ID) et non par son ID d'incident.



Double-cliquez sur un incident pour afficher les informations détaillées le concernant.

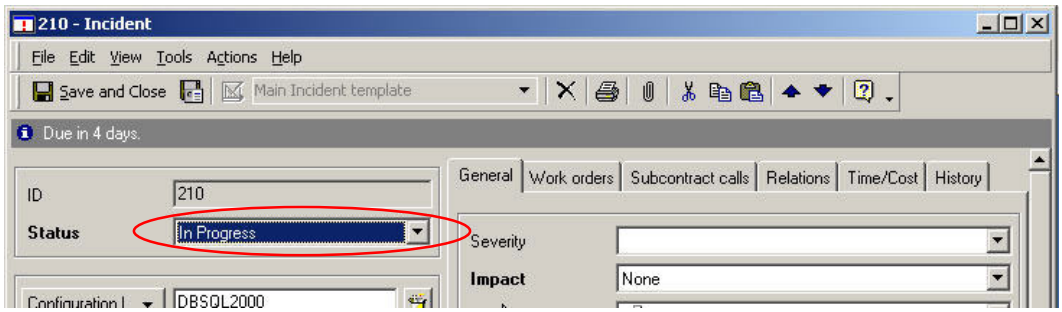
- ID source étendu
- Statut
- Élément de configuration
- Description
- Informations
- Groupe de travail
- Informations sur l'événement (pièce jointe)
- Informations sur la vulnérabilité (pièce jointe)
- Informations Advisor (pièce jointe)



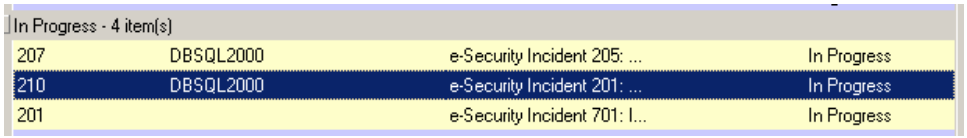
HP OpenView Service Desk – Interface bi-directionnelle

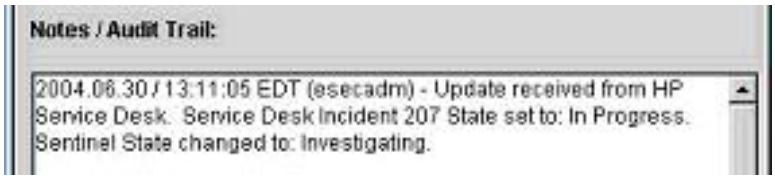
Lorsque cette option est activée (voir le Guide d'installation de Sentinel), Service Desk informe Sentinel de toute modification de l'état d'un incident (de Sentinel) par un utilisateur Service Desk. Grâce à cette fonction, les utilisateurs Sentinel peuvent suivre l'état actuel de chacun des incidents soumis à Service Desk.

Si vous affichez des informations sur un incident, que vous les modifiiez et les enregistriez, le statut En cours apparaîtra.



Cette mise à jour est visible tant dans le client HP OpenView Service Desk que dans la fenêtre des incidents de la console Sentinel.





Reconfiguration manuelle des paramètres de l'interface HP OpenView Service Desk

Lors de la première installation de l'interface tierce HP OpenView Service Desk, les paramètres Service Desk sont stockés dans le fichier das_query.xml. Utilisez les informations de cette section pour modifier ces paramètres une fois l'installation terminée.

Paramètres de HP OpenView Service Desk

Les paramètres de HP OpenView Service Desk sont stockés dans le fichier das_query.xml sous le composant HpServiceDeskService, comme suit :

- server : défini sur l'adresse IP/nom d'hôte du serveur Service Desk.
- username : défini sur le nom d'utilisateur du serveur Service Desk.
- password : défini sur le mot de passe du serveur Service Desk chiffré par le biais de l'utilitaire décrit à la section Modification des mots de passe HP OpenView.
- attachment_path : défini automatiquement sur le répertoire tiers « attach ».
- ftp_server : défini sur l'adresse IP/nom d'hôte du serveur FTP (utilisé par Service Desk pour les pièces jointes).
- ftp_username : défini sur le nom d'utilisateur du serveur FTP (utilisé par Service Desk pour les pièces jointes).
- ftp_password : défini sur le mot de passe chiffré de l'utilisateur du serveur FTP (utilisé par Service Desk pour les pièces jointes) par le biais de l'utilitaire décrit à la section Modification des mots de passe HP OpenView.
- ftp_user_home : défini sur le chemin complet du répertoire de l'utilisateur FTP.
- attachment.events : défini sur « yes » pour indiquer que les événements seront envoyés en pièce jointe.
- attachment.events.filename : le nom des fichiers de pièce jointe des événements.
- attachment.vuln : défini sur « yes » pour indiquer que les informations sur la vulnérabilité seront envoyées en pièce jointe.
- attachment.vuln.filename : le nom des fichiers de pièce jointe sur la vulnérabilité.
- attachment.adv.attack : défini sur « yes » pour indiquer que les informations sur les attaques Advisor seront envoyées en pièce jointe.
- attachment.adv.attack.filename : le nom des fichiers de pièce jointe sur les attaques Advisor.

Modification des mots de passe HP OpenView

Les mots de passe de HP OpenView sont stockés dans le fichier das_query.xml sous un format chiffré. Pour les redéfinir, vous devez utiliser l'utilitaire décrit ci-dessous.

Pour redéfinir les paramètres de l'interface HP OpenView Service Desk

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

```
extconfig -n das_query.xml [-s sd_password] [-f
   sd_ftp_password]
```

   - -s est le mot de passe du serveur HP OpenView Service Desk.
   - -f est le mot de passe du serveur FTP (utilisé par Service Desk pour les pièces jointes).

Index

HP - Service Desk 4-1

HP OpenView Service Desk 3-1, 4-1
- configuration pour le serveur FTP 3-3
- définition des paramètres de pièce jointe ... 3-4
- envoi d'un incident (v5.0) 4-2
- installation 3-3

HP SD 4-1

HP Service Desk 3-1, 4-1
- configuration pour le serveur FTP 3-3
- définition des paramètres de pièce jointe ... 3-4
- envoi d'un incident (v5.0) 4-2
- installation 3-3

HP-OpenView Operations 4-1

HP-OVO 4-1

installation
- Sentinel 1-11

installation
- HP OpenView Service Desk 3-3

installation de Sentinel 1-11

interface bi-directionnelle
- HP OpenView Service Desk 3-5

Remedy 1-1

Remedy Help Desk
- configuration des incidents (v5.0.1 et ultérieures) 2-1
- création du service Web 1-3
- envoi d'un incident à Remedy Help Desk (v5.0.1 et ultérieures) 2-1
- flux de données 1-7
- flux de données - assignation de sortie 1-9
- flux de données - assignation d'entrée 1-10
- installation de Sentinel 1-11
- modification du formulaire des cas 1-2
- opCreate – entrée 1-5
- opCreate – sortie 1-4
- opSet - entrée 1-6

Remedy Help Desk 2-1