Novell® Sentinel™

5.1.3

7 juillet 2006

www.novell.com

Volume III : Guide d'utilisation du composant Wizard de Sentinel

Novell®

Avis juridique

Novell Inc. décline toute responsabilité quant au contenu ou à l'utilisation de cette documentation et, en particulier, exclut toute garantie, expresse ou implicite de qualité loyale et marchande ou d'adéquation à un usage particulier. En outre, Novell Inc. se réserve le droit de revoir la présente publication et d'apporter des modifications à son contenu à tout moment, sans être tenu d'en avertir les personnes ou entités concernées.

Novell Inc. décline toute responsabilité en ce qui concerne les logiciels, et, en particulier, exclut toute garantie, expresse ou implicite de qualité loyale et marchande ou d'adéquation à un usage particulier. De plus, Novell Inc. se réserve le droit d'apporter des modifications à tout ou partie des logiciels Novell, à tout moment, et sans être tenu d'en avertir les personnes ou entités concernées.

Tout produit ou documentation technique fourni dans le cadre de cet accord peut faire l'objet de contrôles à l'exportation aux frontières des États-Unis et est soumis au droit commercial des autres pays. Vous vous engagez à vous conformer aux réglementations propres aux contrôles à l'exportation et à obtenir toutes les autorisations ou classifications nécessaires pour exporter, réexporter ou importer des produits livrables. Vous acceptez de vous conformer aux règles d'exportation américaines et vous vous engagez donc à ne pas exporter ou réexporter les produits ou documentations techniques Novell à des entités figurant sur les listes d'exclusion d'exportation américaines ou vers des pays sous embargo américain ou soupçonnés de terrorisme. Vous ne pouvez en aucun cas utiliser les produits livrables Novell dans le cadre d'armes et de missiles nucléaires, bactériologiques et chimiques (NBC). Pour plus d'informations sur l'exportation de logiciels Novell, reportez-vous au site www.novell.com/info/exports/. Novell ne peut être tenu pour responsable si vous n'obtenez pas les autorisations d'exportation nécessaires.

Novell Inc. détient les droits de propriété intellectuelle relatifs aux technologies intégrées dans le produit décrit dans le présent document.Ces droits de propriété intellectuelle peuvent notamment comprendre sans limitation un ou plusieurs des brevets répertoriés à l'adresse http://www.novell.com/company/legal/patents/, ainsi qu'un ou plusieurs brevets ou applications en attente d'être brevetées aux États-Unis et dans d'autres pays.

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

Préface

La documentation technique de Sentinel explique le fonctionnement général de l'application et constitue un guide de référence. Elle est destinée aux professionnels de la sécurité des informations. Elle est la source de référence relative à Enterprise Security Management System de Sentinel. Une documentation supplémentaire est disponible sur le portail Web Sentinel.

La documentation technique de Sentinel se compose de cinq volumes. Ces volumes sont les suivants :

- Volume I : Guide d'installation de Sentinel™ 5
- Volume II : Guide de l'utilisateur de Sentinel™ 5
- Volume III : Guide d'utilisation du composant Wizard de Sentinel™ 5
- Volume IV : Guide des références utilisateur de Sentinel™ 5
- Volume V : Guide de l'intégration de produits tiers de Sentinel™5

Volume I : Guide d'installation de Sentinel

Ce guide explique comment installer les composants suivants :

- Sentinel Server
- Console Sentinel
- Moteur de corrélation Sentinel
- Sentinel Crystal Reports
- Générateur de collecteurs Wizard
- Gestionnaire des collecteurs Wizard
- Advisor

Volume II : Guide de l'utilisateur de Sentinel

Ce guide aborde les sujets suivants :

- Fonctionnement de la console Sentinel
- Fonctionnalités de Sentinel
- Architecture de Sentinel
- Serveur de communication Sentinel
- Arrêt et démarrage de Sentinel
- Évaluation des vulnérabilités
- Surveillance des événements
- Filtrage des événements
- Corrélation des événements
- Gestionnaire de données Sentinel
- Configuration des événements en rapport avec l'entreprise
- Service d'assignation
- Rapports d'historique
- Gestion d'hôte Wizard
- Incidents
- Cas
- Gestion des utilisateurs
- Processus de travail

Volume III : Guide d'utilisation du composant Wizard de Sentinel

Ce guide aborde les sujets suivants :

- Fonctionnement du générateur de collecteurs Wizard
- Gestionnaire des collecteurs Wizard
- Collecteurs
- Gestion d'hôte Wizard
- Génération et gestion des collecteurs

Volume IV : Guide des références utilisateur de Sentinel

Ce guide aborde les sujets suivants :

- Langage de script de Wizard
- Commandes d'analyse de Wizard
- Fonctions administratives de Wizard
- Balises META de Wizard et de Sentinel
- Moteur de corrélation Sentinel
- Autorisations utilisateur
- Options de ligne de commande de corrélation
- Schéma de la base de données Sentinel

Volume V : Guide d'intégration de produits tiers de Sentinel

- Remedy
- HP OpenView Operations
- HP Service Desk

1 Présentation de Wizard

REMARQUE : les termes Agent et Collecteur sont interchangeables. Le terme Collecteur sera utilisé dans la suite de cette documentation.

Le guide d'utilisation du composant Wizard constitue une présentation du fonctionnement de Novell Wizard. Ce guide explique le fonctionnement de chaque composant ainsi que les interactions entre tous les composants.

Son contenu implique que vous soyez déjà familiarisé avec la sécurité réseau, l'administration de bases de données et les systèmes d'exploitation Windows et UNIX.

Sommaire

Ce guide contient les chapitres suivants :

- Chapitre 1 : Présentation de Wizard
- Chapitre 2 : Gestion d'hôtes Wizard
- Chapitre 3 : Génération et gestion des collecteurs
- Annexe A : Connecteur Syslog
- Annexe B : Serveur de socket
- Annexe C : Informations de copyright

Conventions utilisées

Conventions relatives aux remarques et aux points devant attirer votre attention

REMARQUE : les remarques apportent des informations supplémentaires utiles.

ATTENTION : ces paragraphes vous mettent en garde contre les opérations susceptibles d'endommager ou d'entraîner la perte de données sur votre système.

Commandes

Les commandes s'affichent dans la police courier. Exemple :

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

Wizard

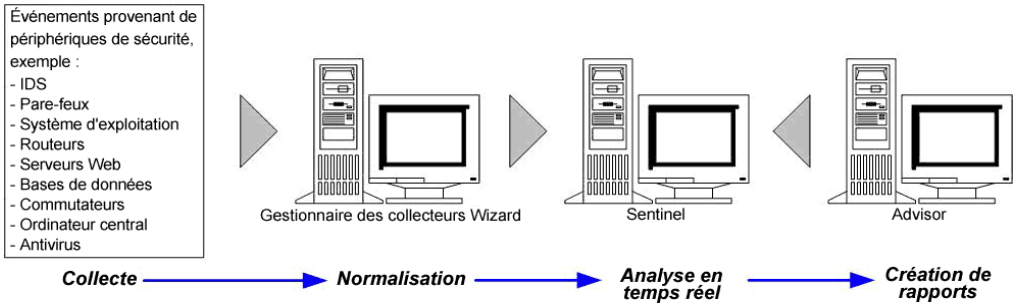
Le composant Wizard vous permet de créer, configurer et contrôler les collecteurs. Ces collecteurs servent à recueillir et à normaliser les événements provenant de périphériques et de programmes de sécurité. Ces événements normalisés sont ensuite envoyés à Sentinel pour être analysés en temps réel, traités par des corrélations et utilisés dans la réponse aux incidents.

REMARQUE : dans une configuration à plusieurs Générateurs de collecteurs, il est recommandé, mais pas obligatoire, de désigner l'un des Générateurs comme Générateur de collecteurs principal. L'ordinateur correspondant peut alors servir d'emplacement de stockage, de développement et de modification de configuration des collecteurs ainsi que d'emplacement de configuration des ports.

Wizard comprend les éléments suivants :

- Le Générateur de collecteurs est l'interface utilisateur du composant Wizard. Il permet de créer, de configurer, de déployer et de contrôler les collecteurs. Il exécute les collecteurs localement mais sert également à télécharger et contrôler les collecteurs sur des systèmes distants.
- Le Gestionnaire des collecteurs est l'interface dorsale du composant Wizard. Il gère les collecteurs, surveille les messages de statut du système et filtre de manière globale les événements.

Un collecteur est un récepteur qui récupère et normalise des événements bruts provenant de périphériques et de systèmes de sécurité, et qui génère des événements normalisés. Ces événements peuvent ensuite faire l'objet de corrélations et de rapports et être utilisés pour répondre à des incidents. Le logiciel Sentinel est livré avec des collecteurs de niveau logiciel 1. Pour télécharger d'autres collecteurs, rendez-vous sur le portail client de Sentinel à l'adresse http://www.esecurityinc.com.



Collecteurs

Les collecteurs sont utilisés pour le filtrage et la standardisation de données d'événement sensibles afin de les convertir dans un format normalisé pour que le processus Sentinel puisse les traiter. Il existe trois niveaux de collecteur :

- Collecteurs pris en charge de niveau 1 (T1), dont les caractéristiques sont les suivantes :
  - documentés ;
  - dotés de métadonnées ;
  - disponibles pour tous les clients ;
  - agrémentés d'une assistance technique.
- Collecteurs documentés de niveau 2 (T2), dont les caractéristiques sont les suivantes :
  - destinés à la bibliothèque des collecteurs ;
  - documentés ;
  - dotés de métadonnées ;
  - conçus sur les modèles du composant Sentinel standard ;
  - agrémentés d'une assistance technique restreinte.
- Collecteurs d'exemple de niveau 3 (T3), dont les caractéristiques sont les suivantes :
  - dotés d'échantillons de concept ;
  - développés de façon personnalisée pour chaque client ;
  - pas nécessairement dotés de métadonnées et/ou documentés ;
  - agrémentés d'une assistance technique restreinte.

Les collecteurs vous donnent accès à des données d'événement provenant de sources multiples :

- Systèmes de détection d'intrusion (hôte)
- Systèmes de détection d'intrusion (réseau)
- Pare-feux
- Systèmes d'exploitation
- Surveillance des stratégies
- Authentification
- Routeurs et commutateurs
- VPN (Virtual Private Network)
- Antivirus
- Serveurs Web
- Bases de données
- Ordinateur central
- Évaluation des vulnérabilités
- Services d'annuaire
- Gestion du réseau
- Systèmes propriétaires

Les composants des collecteurs sont les suivants :

- Fichiers de modèle
- Fichiers de paramètre
- Fichiers de recherche
- Fichiers d'assignation
- Fichier de description des paramètres et fichiers de manifeste

Le fichier de modèle et le fichier de paramètre associé sont fusionnés dans différents fichiers de script lorsque le script du collecteur est généré.

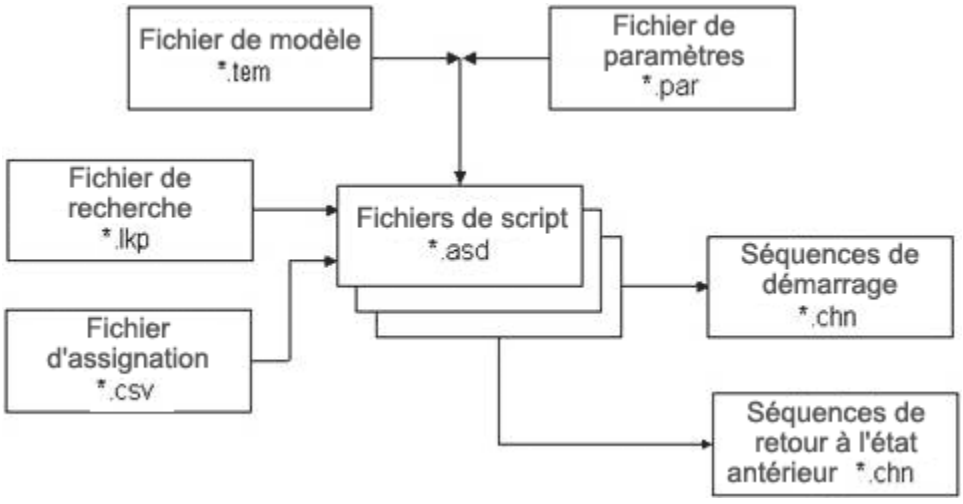
Chaque fichier de script se voit attribuer le nom correspondant à l'en-tête de la colonne comprenant l'ensemble des valeurs dans le fichier de paramètre. Ces fichiers de script sont regroupés de façon ordonnée par séquences de démarrage et séquences de retour à l'état antérieur.

Des séquences de démarrage et de retour à l'état antérieur sont assignées à un port qui exécute les séries de scripts qu'il contient lorsqu'il est démarré ou arrêté. Un script doit être inclus dans une séquence de démarrage ou de retour à l'état antérieur pour pouvoir être utilisé par un port. Les ports permettent à un collecteur de localiser les hôtes Wizard sur un réseau, car ils fournissent l'adresse IP ou un nom de fichier relatif à ces hôtes. Ils apportent également à Sentinel les informations relatives à l'emplacement des capteurs et au collecteur utilisé pour gérer les données de ces capteurs. Les options suivantes peuvent être configurées pour les ports :

- Type de connexion
  - Serial : données lues sur un port série RS-232C.
  - Socket : connexion par socket TCP.
  - File New (fichier actualisé) : lit uniquement les données d'événement de sécurité qui ont été ajoutées au fichier après le démarrage du script (lit à partir de la fin du fichier).
  - File All (tout le fichier) : lit toutes les données d'événement de sécurité d'un fichier.
  - Persistent Process (processus permanent) : lance un processus permanent lorsque le port a démarré ; permet la communication entre le collecteur assigné à ce port et une application externe via des états de réception et de transmission ; s'exécute sans arrêt tant que le port est actif.
  - Transient Process (processus temporaire) : permet la communication entre le collecteur assigné à ce port et une application externe via des états de réception et de transmission. Un processus temporaire peut être démarré à plusieurs reprises.
  - SNMP : reçoit des trappes SNMP v1, v2 et v3.
  - Aucun
- Nom du collecteur : vous pouvez renommer, copier et ajouter des collecteurs.

Lorsqu'un modèle utilise la commande d'analyse LOOKUP() , le fichier de recherche approprié est analysé pour y repérer le bloc de commandes d'analyse à exécuter voulu.

Lorsqu'un modèle utilise la commande d'analyse TRANSLATE, cette dernière charge un fichier d'assignation permettant une recherche rapide sur des entrées de clé.



Fichiers de modèle

Vous pouvez créer des modèles, y insérer des états, modifier et supprimer ces modèles. Ces derniers déterminent la façon dont les enregistrements sont traités. La plupart des décisions concernant les modèles ont à voir avec le type des enregistrements utilisés et leur format. Les fichiers de modèle correspondant à ce type de fichier portent l'extension .tem. Ils se trouvent dans le répertoire %WORKBENCH_HOME%\elements\<Nom du collecteur>.

Les fichiers de modèle sont élaborés en fonction d'états. Un état est un point décisionnel précis dans le flux ou sur le chemin logique d'un modèle. Chaque point, ou état, contient des informations sur le processus à exécuter. Ces états font référence à des paramètres. Lorsque le modèle est fusionné avec un fichier de paramètres, des valeurs spécifiques remplacent les paramètres. Lorsque les paramètres sont remplacés par ces valeurs, un ou plusieurs fichiers de script sont créés.

Lors de son insertion dans un modèle, un état se voit assigner un numéro qu'il conserve, quel que soit son emplacement dans le modèle par la suite. Il existe trois ensembles d'états :

- Les états Transmit (Transmettre), Receive (Recevoir), Decide (Décider) et Parse (Analyser), numérotés selon l'ordre dans lequel ils sont insérés dans le modèle :
  - État Transmit (Transmettre) (Tx) : transmet une chaîne à un port défini.
  - État Receive (Recevoir) (Rx) : définit si le composant Wizard peut recevoir les informations provenant d'une application de sécurité dans la mémoire tampon. Les informations sont extraites de la définition du port.
  - État Decide (Décider) : utilise une chaîne de données ou une variable pour déterminer l'état auquel passer ensuite.
  - État Parse (Analyser) : utilise les commandes d'analyse pour créer des modèles capables de traiter les informations collectées dans le tampon de réception.
- Les états Next (Suivant) et Go To (Retourner à) , identifiés par le numéro de l'état vers lequel ils pointent :
  - État Next (Suivant) : indique l'état auquel passer dans le script suivant.
  - État Go To (Retourner à) : permet de revenir à un état précédent du script en cours.
- L'état Arrêter, toujours désigné par le numéro 0. Indique le moment où l'exécution d'un processus doit prendre fin sur un port.

État Transmit (Transmettre)

L'état Transmit (Transmettre) envoie une chaîne de données ou une variable, selon le type de données sélectionné, vers la connexion configurée pour le collecteur concerné. Si la connexion est rompue au moment où le processus arrive à l'état de transmission et qu'une valeur est entrée dans la zone Rx/Tx Value (Valeur Rx/Tx) du panneau des informations de port du modèle, l'événement suivant se produit et des tentatives de reconnexion ont lieu jusqu'à ce qu'une connexion soit de nouveau établie.

Un espace intercaractères indique le nombre de millisecondes (ms) écoulées entre les envois de chaque octet de données.

État Receive (Réception)

L'état Receive (Réception) indique la méthode que le composant Wizard utilise pour déterminer le moment où les données ont été reçues du collecteur. Pour l'état Receive (Réception), il vous faut indiquer :

- le type de réception ;
- le nombre d'octets minimal ;
- une chaîne de décision séparatrice.

Si la connexion est rompue au moment où le processus arrive à l'état de transmission et qu'une valeur est entrée dans la zone Rx/Tx Value (Valeur Rx/Tx) du panneau des informations de port du modèle, l'événement suivant se produit et des tentatives de reconnexion ont lieu jusqu'à ce qu'une connexion soit de nouveau établie.

Après passage par l'état de réception du tampon de réception Rx Buffer, deux variables sont automatiquement complétées à l'aide des résultats obtenus :

- s_RXBufferString contient le texte reçu par Rx Buffer.
- i_RXBufferLength indique la longueur de la chaîne s_RXBufferString.

Les mêmes résultats sont obtenus par l'exécution du code de script suivant juste après un état de réception :

- COPY(s_RXBufferString:)
- LENGTH(i_RXBufferLength,s_RXBufferString)

Le fait que ces variables soient complétées automatiquement permet une analyse rapide par l'état de décision pour savoir si l'état de réception a expiré ou pas (i_RXBufferLength = 0). Cela permet également l'utilisation de Rx Buffer directement, par l'intermédiaire de la variable s_RXBufferString.

Types de réception : dans Template Editor (Éditeur de modèles), il existe quatre types de réception. Ces types sont les suivants :

- Timeout : permet à un script de continuer à s'exécuter même si les données n'ont pas été reçues dans l'intervalle de temps spécifié. Si vous sélectionnez une valeur de timeout, le composant Wizard peut continuer à recevoir des données jusqu'à ce que l'intervalle de temps spécifié soit écoulé, comme défini par la variable RX_TIMEOUT_DELAY.
- Attente : ce type est surtout utilisé lorsque des messages d'événement indésirables sont reçus. Le composant Wizard attend, le temps du timeout, que les données soient reçues.

  REMARQUE : pour les types de réception Timeout et Attente, l'exécution du script s'interrompt jusqu'à ce que le nombre d'octets minimal soit reçu ou jusqu'à ce que le délai de timeout indiqué pour l'option correspondante soit atteint.

- Delim Timeout (Timeout de séparation) : utilise une chaîne de caractères prédéfinie pour indiquer au composant Wizard que les données ont été reçues. Les données de la zone Delimiter Decide String (Chaîne de décision séparatrice) sont comparées aux données du tampon de réception, octet par octet.

- Delim Wait (Attente de séparation) : ce type est utilisé lorsque des messages indésirables sont reçus. Une chaîne de caractères définie par l'utilisateur indique au composant Wizard que les données ont été reçues. Wizard se sert des données de la zone Delimiter Decide String (Chaîne de décision séparatrice) pour vérifier les données reçues, octet par octet. Le paramètre RX_TIMEOUT_DELAY n'intervient pas lors de l'utilisation de cette option.

REMARQUE : pour les types de réception Delim Timeout (Timeout de séparation) et Delim Wait (Attente de séparation), l'exécution du script s'interrompt jusqu'à ce que la chaîne de décision séparatrice soit définie sur true et que le nombre d'octets minimal soit reçu ou jusqu'à ce que le délai de timeout indiqué à l'option Delim Timeout soit atteint.

Minimum Bytes (Nombre d'octets minimal) : le nombre minimal d'octets est le nombre d'octets reçus qui doit être atteint pour que le composant Wizard utilise le délai de timeout défini par défaut. Si ce nombre n'est pas atteint, le composant continue à s'exécuter. Tant que le nombre minimal d'octets reçus n'est pas atteint, le traitement interne au script s'interrompt.

Delimiter Decide String (Chaîne de décision séparatrice) : cette chaîne s'applique lorsque le type de réception est défini sur Delim Timeout (Timeout de séparation) ou Delim Wait (Attente de séparation). Le traitement du collecteur ne passe pas à l'état suivant tant que la chaîne de décision séparatrice ne correspond pas aux données lues et que le nombre minimal d'octets n'a pas été reçu.

Cette chaîne est une expression régulière conforme à la norme POSIX 1003.2.

Scénarios des types de réception : il existe quatre scénarios possibles selon les types de réception. Ces scénarios sont les suivants :

- Scénario de timeout : une fois l'état de réception atteint, le traitement s'arrête jusqu'à ce que le nombre minimal d'octets soit lu ou qu'un nombre de secondes indiqué par la variable RX_TIMEOUT_DELAY se soit écoulé. Après que le composant Wizard a reçu un nombre d'octets supérieur à ce nombre minimal ou que le délai de timeout a expiré, le processus du port du collecteur continue jusqu'à l'état suivant dans le script.
- Scénario d'attente : l'état correspondant au type de réception Attente attend que le collecteur Wizard ait reçu le nombre d'octets minimal spécifié dans la zone Minimum Bytes (Nombre d'octets minimal). Une fois que le composant Wizard a reçu un nombre d'octets supérieur à ce nombre minimal, le processus du port du collecteur continue jusqu'à l'état suivant dans le script. Si le nombre d'octets minimal reçu n'est pas atteint, le processus du port du collecteur ne s'arrête pas.
- Scénario de timeout de séparation : si la chaîne de décision séparatrice est atteinte après que le nombre minimal d'octets défini dans la zone Minimum Bytes (Nombre d'octets minimal) a été reçu, les données reçues jusqu'au moment où la chaîne séparatrice a été atteinte sont stockées dans le tampon de réception Rx Buffer. Si cette chaîne n'est pas atteinte, aucune donnée n'est transmise au tampon de réception et le processus du port du collecteur prend fin une fois le délai de timeout par défaut expiré.
- Scénario d'attente de séparation : si la chaîne de décision séparatrice est atteinte après que le nombre minimal d'octets défini dans la zone Minimum Bytes (Nombre d'octets minimal) a été reçu, le processus du port du collecteur continue de s'exécuter et les données sont traitées normalement. Tant que cette chaîne n'est pas atteinte, aucune donnée n'est transmise au tampon de réception et le processus du port du collecteur ne prend pas fin. Si cette chaîne n'est jamais atteinte, le processus du port du collecteur ne prend jamais fin. De même, si la chaîne de décision séparatrice est atteinte mais que le nombre minimal d'octets requis n'est pas reçu, le processus du port du collecteur ne prend jamais fin.

État Decide (Décider)

L'état Decide (Décider) vérifie le contenu du tampon ou de la variable de réception et détermine ensuite l'action à effectuer. Si les informations du tampon de réception contiennent le type Decide (Décider) sélectionné, le Gestionnaire des collecteurs traite la commande comme étant vérifiée (true) et la route suivie est la route « Oui ». Si le tampon de réception ne contient pas le type Decide (Décider) sélectionné, le Gestionnaire des collecteurs traite la commande comme étant irrecevable (false) et la route suivie est la route « Non ».

Le tampon de réception (taille du tampon Rx Buffer) est un paramètre modifiable situé à l'emplacement suivant :

```
$WORKBENCH_HOME/config/wizard.properties/
   system.max_receive_buffer_size
```

Ce paramètre vous permet de configurer le tampon de réception du Gestionnaire des collecteurs (Rx buffer). La valeur par défaut est 50 000 événements. La valeur minimale est 5 000 événements. Lorsque le tampon de réception atteint sa taille maximale, les nouveaux événements entrants sont abandonnés au fur et à mesure de leur réception en raison de la limitation qui a été définie.

Il existe quatre types de décision. Ces types sont les suivants :

- String (Chaîne) : compare une chaîne de décision définie par l'utilisateur au contenu reçu par le tampon. Le contenu de la chaîne de décision est comparé au contenu du tampon de réception ou à une variable pour déterminer la route que les données reçues doivent suivre. Cette chaîne est une expression régulière conforme à la norme POSIX 1003.2. Une variable peut contenir des chaînes, des entiers ou des valeurs flottantes.
- True (Vrai) : force une évaluation vraie. Le Gestionnaire des collecteurs achemine les données vers une route « Oui ».
- False (Faux) : force une évaluation fausse. Le Gestionnaire des collecteurs achemine les données vers une route « Non ».
- Data (Données) : compare une chaîne de décision définie par l'utilisateur à une autre chaîne ou à la valeur d'une variable.

État Parse (Analyser)

L'état Parse (Analyser) est utilisé pour développer les scripts afin qu'ils puissent ensuite être exécutés sur les ports. Les commandes d'analyse peuvent inclure des paramètres qui sont ensuite fusionnés avec le modèle voulu lorsque les scripts sont créés. Un éditeur plein écran et un éditeur de texte sont à la disposition de l'utilisateur pour définir les commandes d'analyse.

L'état Parse (Analyser) sert également à insérer des commandes d'analyse dans un modèle. Les commandes d'analyse peuvent comprendre des paramètres qui sont ensuite remplacés par des valeurs spécifiques lorsque le modèle est fusionné avec un fichier de paramètre au cours du processus de génération du script. La fusion d'un modèle et d'un fichier de paramètre permet de générer plusieurs scripts à exécuter sur les ports.

Fichiers de paramètre

Les paramètres sont l'équivalent des variables. Les fichiers de paramètre (fichiers .par) sont des tableaux servant à définir des noms de variable pour les fichiers de script d'exécution associés. Ils sont utilisés lorsqu'ils sont cités dans le code d'analyse. Ils sont stockés sous forme de chaînes. Toute valeur numérique doit être convertie sous forme de chaîne pour pouvoir être utilisée. Lorsque de nouvelles valeurs de paramètre sont entrées, elles s'appliquent une fois que le script a été généré. Ces valeurs sont ensuite intégrées au fichier de modèle au moment de la création du script.

Les noms des fichiers de script d'exécution s'affichent sur la première ligne du tableau et les noms des paramètres, ou étiquettes, s'affichent dans la première colonne. La seconde ligne du tableau sert à définir les icônes qui apparaissent dans l'arborescence du collecteur. Les lignes suivantes permettent de définir les variables ou les valeurs à utiliser pour les paramètres selon le script concerné.

Les valeurs d'un fichier de paramètres peuvent être :

- des balises META, des informations et des commentaires : plus de 200 balises META sont disponibles, dont la moitié sont configurables par l'utilisateur et les autres sont réservées ;
- des règles : les noms définis pour les fichiers de règle s'affichent sur la ligne d'en-tête du tableau tandis que les paramètres s'affichent dans la première colonne du tableau ;
- des topogrammes binaires : la deuxième ligne du tableau définit le topogramme binaire utilisé pour ce fichier, topogramme qui apparaît ensuite dans la liste des collecteurs.

Fichiers de recherche

Les fichiers de recherche (fichiers .lkp) sont des tables facultatives auxquelles les valeurs reçues sont comparées afin de déterminer les actions à entreprendre pour répondre à des événements de sécurité, le cas échéant. Les fichiers de recherche contiennent des clauses de correspondance qui servent à comparer des chaînes une par une. En fonction des clauses de correspondance d'un fichier de recherche spécifique et des données transmises par les périphériques de sécurité, la commande LOOKUP détermine si la chaîne recherchée est trouvée ou pas.

Éventuellement, des commandes d'analyse peuvent être associées à la chaîne recherchée. Ces commandes d'analyse sont exécutées si une correspondance est trouvée.

Fichiers d'assignation

Les fichiers d'assignation sont des fichiers facultatifs (fichiers .csv) qui permettent une recherche rapide sur des entrées de clé. Les fichiers .csv sont des chemins relatifs du répertoire de script d'un collecteur. La modification de ces fichiers n'est actuellement pas possible dans le Générateur de collecteurs mais elle peut être effectuée à l'aide de Microsoft Excel.

Exemple de fichier d'assignation :

```
~Mois~    ~Nombre~
Jan               1
Fév               2
Mar               3
Avr               4
Mai               5
Jun               6
Jul               7
Aoû               8
Sep               9
Oct              10
Nov              11
Déc              12
```

Les entrées peuvent être un nombre indéfini de variables de script (variables de chaîne, entières ou flottantes) servant à indiquer les variables où les données vont être stockées. Dans l'exemple ci-dessus, le mois est traduit par un nombre (c'est-à-dire qu'un nombre lui est assigné). Ici, le nombre 1 est assigné au mois de janvier (Jan).

Fichiers de manifeste

Les fichiers de manifeste sont ceux qui permettent de différencier les versions de collecteur 5.* des versions de collecteur précédentes. Les fichiers de manifeste prennent en charge le déploiement des collecteurs, à partir de la console Sentinel, ainsi que la gestion des versions de collecteur. L'analyse des collecteurs est définie par le fichier agent.lkp. Il existe différents cas de recherche :

- Setup : configuration groupée des variables et des paramètres.
- Check_Setup : vérification groupée des variables et des paramètres.
- Initialize_Vars : début de chaque boucle, où les variables sont initialisées une fois par analyse.
- Parse : emplacement où l'analyse est effectuée.

Ces recherches permettent d'intégrer de nouvelles analyses de collecteur dans les modèles existants. De plus, elles rendent possible l'installation avec support pack intégré des nouvelles versions de l'analyse des collecteurs afin de mettre à jour le code. Voici une liste des fichiers de manifeste et de leur contenu pour la version v5.0 :

- agent.nfo
  - product : Snort ;
  - product.vendor : GNU ;
  - product.version : 2.0 ;
  - product.security.type : IDS ;
  - product.sensor.type : N ;
  - product.name : IDSx_GNUx_SNRT ;
  - file.version : 1.

Autres références Sentinel

Les manuels suivants sont disponibles sur les CD-ROM d'installation de Sentinel.

- Guide d'installation de Sentinel™
- Guide de l'utilisateur de Sentinel™
- Guide d'utilisation du composant Wizard de Sentinel™
- Guide des références utilisateur de Sentinel™
- Guide d'intégration de produits tiers de Sentinel™
- Notes de version

Pour contacter Novell

- Site Web : http://www.novell.com
- Assistance technique Novell : http://www.novell.com/support/index.html
- Assistance technique Novell (international) : http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Auto-assistance : http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Pour une assistance 24 heures sur 24, 7 jours sur 7, appelez le 800-858-4000

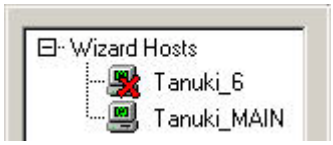
2 Gestion d'hôtes Wizard

REMARQUE : les termes Agent et Collecteur sont interchangeables. Le terme Collecteur sera utilisé dans la suite de cette documentation.

Les hôtes Wizard sont les machines sur lesquelles le Gestionnaire des collecteurs est installé. Ces hôtes interagissent avec les machines du Générateur de collecteurs et avec Sentinel par l'intermédiaire du réseau. Selon les données que les collecteurs reçoivent et analysent, les hôtes envoient des alertes à Sentinel.

Le composant Wizard détecte automatiquement ces hôtes sur le réseau et les ajoute à la liste de l'onglet Wizard Host (Hôte Wizard). Vous ne pouvez pas ajouter d'hôtes manuellement. Vous pouvez renommer les hôtes existants et supprimer ceux qui ne sont plus sur le réseau ou qui ne communiquent plus.

Le Générateur de collecteurs récupère les messages d'état de santé sur les hôtes. Si l'un de ces hôtes ne répond pas par un message d'état de santé, une croix rouge s'affiche en face de l'hôte concerné dans l'arborescence des hôtes Wizard. Vous pouvez supprimer un hôte marqué d'une croix rouge mais ce dernier s'affiche à nouveau dans l'arborescence des hôtes Wizard dès que le Générateur de collecteurs détecte une communication en provenance de cet hôte. De même, si vous supprimez un hôte en cours de communication, le message d'état de santé émis entraîne le réaffichage de l'hôte dans l'arborescence.



Lorsqu'un hôte est détecté, un numéro d'identification lui est assigné.

Les derniers collecteurs disponibles se trouvent sur le CD du Service Pack. Pour plus d'informations, reportez-vous aux notes de publication accompagnant le Service Pack.

REMARQUE : pour plus d'informations concernant la configuration des collecteurs de démo, reportez-vous à la section intitulée « Tester l'installation » du Guide d'installation de Sentinel.

Récupération de données du collecteur par un hôte Wizard

Pour permettre à un hôte Wizard (un ordinateur sur lequel le Gestionnaire des collecteurs est installé) de recevoir des données provenant d'un collecteur, vous devez télécharger ce collecteur de l'ordinateur où se trouve le Générateur de collecteurs vers l'hôte Wizard par l'intermédiaire d'un port configuré dans le Générateur de collecteurs. Après qu'un collecteur a été téléchargé sur un hôte, ce dernier est prêt à recevoir les données du collecteur.

Chaque hôte Wizard peut être connecté à plusieurs ports et peut surveiller les données provenant de plusieurs collecteurs. Un hôte Wizard peut disposer de ports de collecteurs qui sont connectés à différents types de source de données. Chaque collecteur d'un port d'hôte Wizard doit être téléchargé pour pouvoir être exécuté. En outre, les ports fournissent au Gestionnaire des collecteurs des informations relatives à l'emplacement des sources de données.

Autorisations de l'hôte Wizard

Les autorisations de l'hôte Wizard peuvent être administrées dans l'onglet Admin du Centre de contrôle Sentinel. Les autorisations utilisateur d'un hôte Wizard sont les suivantes :

Nom de l'autorisation	Description
View Collectors (Affichage des collecteurs)	▪ Affichage de l'onglet Collecteurs dans le Centre de contrôle Sentinel. ▪ Affichage de l'onglet Hôtes de l'assistant dans le Générateur des collecteurs.
Control Collectors (Contrôle des collecteurs)	▪ Mêmes autorisations d'accès que l'affichage des collecteurs. ▪ Autorisation de commande et de contrôle des collecteurs dans le Centre de contrôle Sentinel. ▪ Autorisation de commande et de contrôle des collecteurs dans le Générateur de collecteurs Wizard.
Collector Administration (Administration des collecteurs)	▪ Mêmes autorisations d'accès que le contrôle des collecteurs. ▪ Dans le Générateur de collecteurs, autorisation de modification et de déploiement. ▪ Dans le Générateur de collecteurs, autorisation de création, de modification, de compilation et de débogage. ▪ Dans le Générateur de collecteurs, autorisation de téléchargement des collecteurs. ▪ Dans le Générateur de collecteurs, autorisation d'exportation des hôtes d'assistant. ▪ Dans le Générateur de collecteurs, autorisation d'ajout, de modification et de suppression des ports. ▪ Dans le Générateur de collecteurs, autorisation de configuration des options de port.

L'autorisation de commande et de contrôle concerne les opérations suivantes :

- démarrage/arrêt des ports un par un ;
- démarrage/arrêt de tous les ports ;
- redémarrage des hôtes ;
- assignation d'un nouveau nom aux hôtes.

Gestion d'hôte Wizard

Les sujets suivants sont abordés dans ce chapitre :

Démarrage et arrêt du Gestionnaire des collecteurs

REMARQUE : la première fois que le Générateur de collecteurs Wizard est exécuté, le message suivant s'affiche : « Directory ‘Collectors’ does not exist. » It will be automatically created for you. Some information may have been lost. » (Le répertoire « Collecteurs » n'existe pas. Il sera créé automatiquement. Des informations ont peut-être été perdues). Cliquez sur OK pour que le répertoire soit créé et que le Générateur de collecteurs Wizard démarre. Si ce message continue de s'afficher chaque fois que le Générateur de collecteurs est exécuté, il est possible que le répertoire Collecteur ait été supprimé par inadvertance et qu'il faille vérifier si des informations ont été perdues.

Démarrage et arrêt du Gestionnaire des collecteurs sous Windows

Pour démarrer ou arrêter le Gestionnaire des collecteurs sous Windows

1. Cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration*.
2. Dans le *Panneau de configuration,* double-cliquez sur *Outils d'administration* et cliquez sur *Services.*
3. Dans la boîte de dialogue Services, cliquez avec le bouton droit sur *Gestionnaire des collecteurs* et sélectionnez *Démarrer* ou *Arrêter*.

Pour démarrer les services du Gestionnaire des collecteurs sous Windows (ligne de commande)

1. Accédez au répertoire %WORKBENCH_HOME%.
2. Pour démarrer le Gestionnaire des collecteurs :
   - ./agent-manager start
   - ./agent-manager restart : démarre le script du Gestionnaire des collecteurs en arrière-plan et redémarre automatiquement le processus lorsqu'il s'arrête. Si le processus agentmanager est en cours d'exécution, il s'arrête et redémarre.
   - ./agent-manager.sh console : démarre le processus du Gestionnaire des collecteurs au premier plan.

REMARQUE : en mode console, assurez-vous de n'exécuter qu'une seule instance du Gestionnaire des collecteurs sur votre machine.

Pour arrêter les services du Gestionnaire des collecteurs sous Windows (ligne de commande)

1. Accédez au répertoire %WORKBENCH_HOME%.
2. Pour arrêter le Gestionnaire des collecteurs :

```
./agent-manager stop
```

Démarrage du Gestionnaire des collecteurs sous UNIX (mode standard et mode console)

Pour démarrer le Gestionnaire des collecteurs sous UNIX

1. En tant qu'utilisateur esecadm, accédez au répertoire :

```
$WORKBENCH_HOME
```

2. Entrez la commande suivante :

```
./agent-manager.sh start
```

   - ./agent-manager.sh restart : démarre le script du Gestionnaire des collecteurs en arrière-plan et redémarre automatiquement le processus lorsqu'il s'arrête. Si le processus du Gestionnaire des collecteurs est en cours d'exécution, il s'arrête et redémarre.
   - ./agent-manager.sh console : démarre le processus du Gestionnaire des collecteurs au premier plan.

Arrêt du Gestionnaire des collecteurs sous UNIX

Pour arrêter le Gestionnaire des collecteurs sous UNIX

1. En tant qu'utilisateur esecadm, accédez au répertoire :

```
$WORKBENCH_HOME
```

2. Entrez la commande suivante :

```
./agent-manager.sh stop
```

Administration du Gestionnaire des collecteurs

Un fichier exécutable sous Windows et un script sous UNIX vous permettent :

- d'installer le service du Gestionnaire des collecteurs (Windows uniquement) ;
- de supprimer le service du Gestionnaire des collecteurs (Windows uniquement) ;
- de configurer le service du Gestionnaire des collecteurs ;
- d'imprimer des informations de débogage détaillées ;
- d'afficher la version ;
- d'afficher l'aide.

Installation des services du Gestionnaire des collecteurs (Windows uniquement)

Pour installer les services du Gestionnaire des collecteurs (Windows uniquement)l

1. À l'invite de commande, accédez au répertoire %workbench_home%.
2. Entrez la commande suivante :

   ```
   agent-manager.bat -install
   ```

3. Pour démarrer le service, vous disposez de deux possibilités :
   - À l'invite de commande, entrez ce qui suit :

     ```
     net start « agent manager »
     ```

   - Cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration*. Double-cliquez sur *Services* et sélectionnez *Gestionnaire des collecteurs.* Démarrez le *Gestionnaire des collecteurs.*

REMARQUE : si la fenêtre des services est déjà ouverte, cliquez sur *Action,* sélectionnez *Rafraîchir* et démarrez le *Gestionnaire des collecteurs*.

Suppression des services du Gestionnaire des collecteurs (Windows uniquement)

Pour supprimer les services du Gestionnaire des collecteurs (Windows uniquement)l

1. Pour arrêter le Gestionnaire des collecteurs, vous disposez de deux possibilités :
   - À l'invite de commande, entrez ce qui suit :

     ```
     net stop « agent manager »
     ```

   - Cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration*. Double-cliquez sur *Services* et sélectionnez *Gestionnaire des collecteurs.* Arrêtez le *Gestionnaire des collecteurs* et fermez la fenêtre des services.
2. À l'invite de commande, accédez au répertoire %workbench_home%.
3. Entrez la commande suivante :

   ```
   agent-manager.bat -remove
   ```

Changement du mot de passe du Gestionnaire des collecteurs sous Windows

REMARQUE : pour des raisons de conformité aux exigences de sécurité imposées par la certification CC (Common Criteria), il est fortement recommandé de configurer un mot de passe fort doté des caractéristiques suivantes :

1. Choisissez un mot de passe comportant au moins 8 caractères qui inclut au moins un caractère en MAJUSCULE, un caractère en minuscule, un symbole spécial (!@#$%^&*()_+) et un caractère numérique (0 à 9).

2. Votre mot de passe ne peut contenir ni votre adresse de messagerie ni une partie de votre nom.

3. Votre mot de passe ne doit pas être un mot courant (par exemple, un mot du dictionnaire ou un mot d'argot courant).

4. Votre mot de passe ne doit pas contenir de mots d'une langue, quelle qu'elle soit, car de nombreux programmes de reconnaissance de mots de passe sont capables de rechercher parmi des millions de combinaisons de mots possibles en quelques secondes.

5. Choisissez un mot de passe qui soit facile à mémoriser tout en étant élaboré. Par exemple, Mf1l$a5!A (mon fils a 5 ans) OU J!hb1tE75 (j'habite à Paris).

Pour changer le mot de passe du Gestionnaire des collecteurs sous Windows

1. À l'invite de commande, accédez au répertoire %workbench_home%.
2. Entrez la commande suivante :

ATTENTION : vous ne serez à aucun moment invité à confirmer votre nouveau mot de passe ou à entrer votre ancien mot de passe.

```
agent-manager.bat –password <nouveau mot de passe>
```

3. Pour que le mot de passe soit effectivement appliqué, procédez de l'une des façons suivantes :
   - À l'invite de commande, entrez ce qui suit :

     ```
     net stop « agent manager »
     ```

     ```
     net start « agent manager »
     ```

   - Dans le Générateur de collecteurs, cliquez avec le bouton droit sur l'ordinateur hôte et sélectionnez le redémarrage de l'hôte.
   - Cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration*. Double-cliquez sur *Services* et sélectionnez *Gestionnaire des collecteurs.* Arrêtez et redémarrez les services *du Gestionnaire des collecteurs*.

Changement du mot de passe du Gestionnaire des collecteurs sous UNIX

REMARQUE : pour des raisons de conformité aux exigences de sécurité imposées par la certification CC (Common Criteria), il est fortement recommandé de configurer un mot de passe fort doté des caractéristiques suivantes :

1. Choisissez un mot de passe comportant au moins 8 caractères qui inclut au moins un caractère en MAJUSCULE, un caractère en minuscule, un symbole spécial (!@#$%^&*()_+) et un caractère numérique (0 à 9).
2. Votre mot de passe ne peut contenir ni votre adresse de messagerie ni une partie de votre nom.
3. Votre mot de passe ne doit pas être un mot courant (par exemple, un mot du dictionnaire ou un mot d'argot courant).
4. Votre mot de passe ne doit pas contenir de mots d'une langue, quelle qu'elle soit, car de nombreux programmes de reconnaissance de mots de passe sont capables de rechercher parmi des millions de combinaisons de mots possibles en quelques secondes.
5. Choisissez un mot de passe qui soit facile à mémoriser tout en étant élaboré. Par exemple, Mf1l$a5!A (mon fils a 5 ans) OU J!hb1tE75 (j'habite à Paris).

Pour changer le mot de passe du Gestionnaire des collecteurs sous UNIX

1. En tant qu'utilisateur esecadm, accédez au répertoire $WORKBENCH_HOME.
2. Entrez la commande suivante :

   ATTENTION : vous ne serez à aucun moment invité à confirmer votre nouveau mot de passe ou à entrer votre ancien mot de passe.

   ```
   ./agent-manager.sh -password <nouveau mot de passe>
   ```

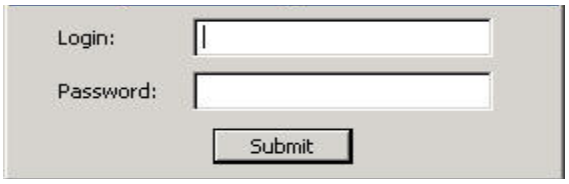
3. Pour que le mot de passe soit effectivement appliqué, accédez au répertoire /usr/local/bin et entrez la commande suivante :

   ```
   ./agent-manager.sh -restart
   ```

Démarrage du Générateur de collecteurs

Pour démarrer le Générateur de collecteurs

1. Cliquez sur *Démarrer* > *Programmes* > *Sentinel* > *Générateur de collecteurs* ou double-cliquez sur l'icône *Générateur de collecteurs* sur le bureau.
2. Selon votre installation, connectez-vous en tant qu'utilisateur esecadm ou sous votre nom d'authentification Windows.



Assignation d'un nouveau nom à un hôte Wizard

Pour renommer un hôte Wizard

1. Dans le Générateur de collecteurs (Wizard), cliquez sur l'onglet Wizard Hosts (Hôtes Wizard) pour ouvrir le panneau de l'arborescence des hôtes Wizard.
2. Dans cette arborescence, cliquez avec le bouton droit sur l'hôte à renommer et sélectionnez *Rename Host (Renommer l'hôte)*. Vous pouvez uniquement renommer un hôte actif.
3. Entrez le nouveau nom de l'hôte et appuyez sur Entrée.

REMARQUE : renommer un hôte n'entraîne pas de changement au niveau du numéro d'ID qui lui est assigné au moment de son installation. Ces informations sont conservées à l'emplacement suivant : %WORKBENCH_HOME%\wizard\agents\names.dat.

Suppression d'un hôte Wizard

Pour pouvoir supprimer un hôte, ce dernier doit d'abord être supprimé du réseau. Les hôtes qui communiquent sur le réseau ne peuvent pas être supprimés. Lorsqu'un hôte est présent sur le réseau mais ne communique plus, une croix rouge s'affiche sur l'icône correspondant dans l'arborescence des hôtes Wizard.

Pour supprimer un hôte Wizard

1. Cliquez sur l'onglet *Wizard Hosts (Hôtes Wizard)* pour ouvrir le panneau de l'arborescence des hôtes Wizard.
2. Dans l'arborescence des hôtes Wizard, cliquez avec le bouton droit sur l'hôte voulu.
3. Cliquez sur Delete Host (Supprimer l'hôte).

Redémarrage d'un hôte Wizard

Pour redémarrer un hôte Wizard

1. Cliquez sur l'onglet *Wizard Hosts (Hôtes Wizard)* pour ouvrir le panneau de l'arborescence des hôtes Wizard et sélectionner un hôte.
2. Cliquez avec le bouton droit sur un hôte et cliquez sur *Start Ports (Démarrer les ports)*. Vous pouvez uniquement redémarrer un hôte Wizard actif.

Exportation d'un hôte Wizard

Pour exporter un hôte Wizard

1. Cliquez sur l'onglet *Wizard Hosts (Hôtes Wizard)* pour ouvrir le panneau de l'arborescence des hôtes Wizard. Sélectionnez un hôte.
2. Cliquez sur *Fichier* et sélectionnez *Export Host (Exporter l'hôte)*. Le sous-répertoire suivant est créé :

   ```
   %WORKBENCH_HOME%\upload_<nom de l'hôte>
   ```

   Ce sous-répertoire peut être déplacé vers une machine distante à l'aide de Secure Shell (SSH) ou d'un disque. Une fois le sous-répertoire placé sur la machine distante, exécutez la commande uploadhost. Cette opération entraîne la copie des fichiers nécessaires dans les répertoires appropriés.

REMARQUE : si les paramètres SNMP ont été changés, le Générateur de collecteurs n'est plus en mesure de communiquer avec la machine distante entre le moment où vous cliquez sur le bouton Exporter et celui où le téléchargement des fichiers du collecteur exporté prend fin.

Affichage des propriétés de l'hôte Wizard

Pour afficher les propriétés de l'hôte Wizard

1. Cliquez sur l'onglet *Wizard Hosts (Hôtes Wizard)* pour ouvrir le panneau de l'arborescence des hôtes Wizard.
2. Dans cette arborescence, cliquez avec le bouton droit sur l'hôte voulu et sélectionnez *Propriétés*. La fenêtre des propriétés de l'hôte Wizard contient les informations suivantes :
   - Nom
   - ID
   - Nom d'hôte
   - Adresse IP
   - Version
   - Temps de fonctionnement
3. Cliquez sur *OK* pour fermer la fenêtre des propriétés.

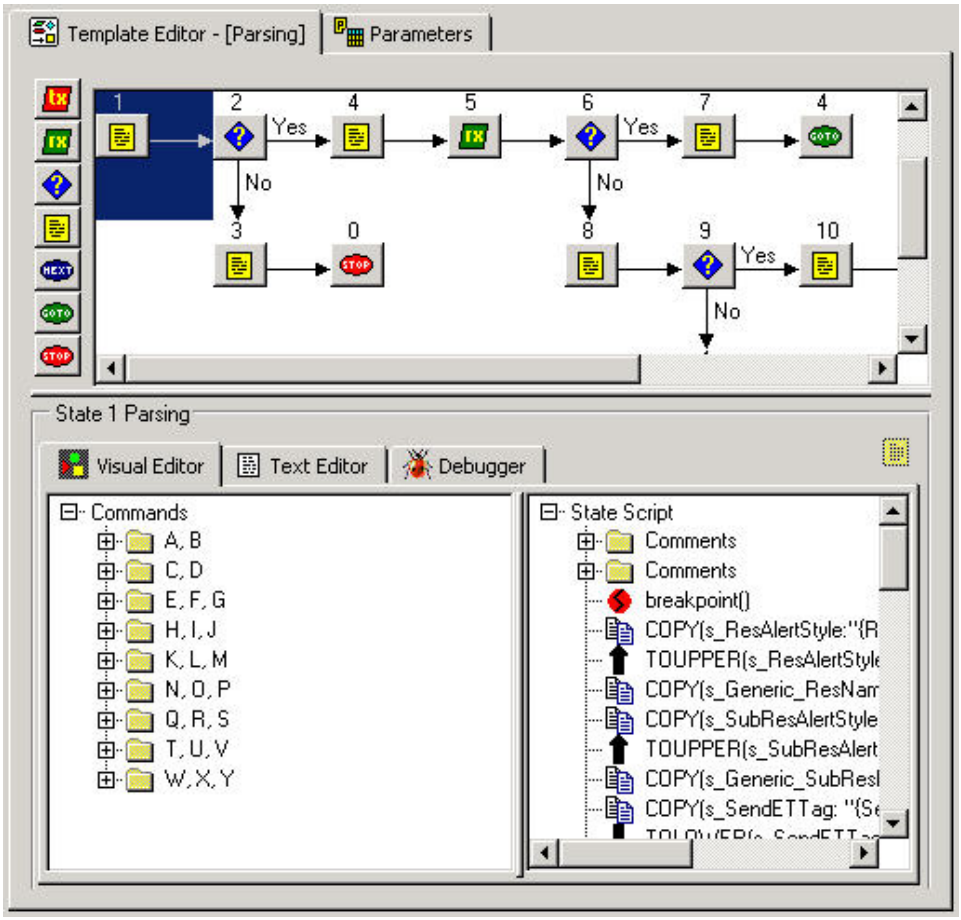
REMARQUE : si l'hôte n'est pas en cours d'exécution, une fenêtre indiquant qu'il ne répond pas s'affiche lorsque vous sélectionnez Propriétés.

Modification d'un fichier de modèle

Pour modifier un fichier de modèle

1. Cliquez sur l'onglet Collecteurs pour ouvrir le panneau de l'arborescence des collecteurs.
2. Dans l'arborescence des collecteurs, cliquez sur un modèle, puis sur l'onglet Template Editor (Éditeur de modèles).

3. Dans Template Editor (Éditeur de modèles), cliquez sur l'état voulu et effectuez vos modifications. Vous pouvez modifier un état à l'aide de l'éditeur plein écran ou de l'éditeur de texte. Pour plus d'informations sur les commandes d'analyse, reportez-vous au Guide des références utilisateur de Sentinel.



Suppression d'un fichier de modèle

Pour supprimer un fichier de modèle

1. Cliquez sur l'onglet *Collecteurs* pour ouvrir le panneau de l'arborescence des collecteurs.
2. Dans l'arborescence des collecteurs, cliquez avec le bouton droit sur un modèle et sélectionnez *Supprimer le modèle*.

Assignation d'un nouveau nom à un fichier de recherche

Pour renommer un fichier de recherche

1. Cliquez sur l'onglet *Collecteurs* pour ouvrir le panneau de l'arborescence des collecteurs.
2. Cliquez avec le bouton droit sur un fichier de recherche et sélectionnez *Rename Lookup File (Renommer le fichier de recherche)*.

3. Tapez le nouveau nom et appuyez sur *Entrée*.

Suppression d'un fichier de recherche

Pour supprimer un fichier de recherche

1. Cliquez sur l'onglet *Collecteurs* pour ouvrir le panneau de l'arborescence des collecteurs.
2. Cliquez avec le bouton droit sur un fichier de recherche et sélectionnez *Delete Lookup File (Supprimer le fichier de recherche)*.

Suppression d'un script

Pour supprimer un script

1. Vous pouvez supprimer un script de deux façons différentes :
   - Dans l'arborescence des collecteurs, cliquez avec le bouton droit sur un script et sélectionnez *Supprimer*.
   - Cliquez avec le bouton droit sur le script voulu dans les colonnes Startup Scripts (Scripts de démarrage) ou Backout Scripts (Scripts de retour à l'état antérieur) et sélectionnez Delete Script (Supprimer le script).

Suppression d'une séquence de démarrage

Pour supprimer une séquence de démarrage

1. Dans le panneau Startup Scripts (Scripts de démarrage), sélectionnez une séquence de démarrage dans le menu déroulant afin que son nom apparaisse dans la zone Startup Scripts (Scripts de démarrage).
2. Cliquez avec le bouton droit sur un script dans l'arborescence des collecteurs et sélectionnez Delete Current Startup Sequence (Supprimer la séquence de démarrage actuelle). La séquence de démarrage est supprimée de la liste des scripts de démarrage.

REMARQUE : si vous supprimez la séquence de démarrage par défaut, tous les scripts qui lui sont assignés sont supprimés de la colonne Startup Scripts (Scripts de démarrage). En revanche, la séquence par défaut continue de s'afficher dans le menu Startup Sequences (Séquences de démarrage).

Ports Wizard

Cette section traite de l'arrêt, du démarrage, de la modification de configuration, de la suppression et du débogage d'un port Wizard.

Démarrage et arrêt d'un port Wizard (interface utilisateur graphique)

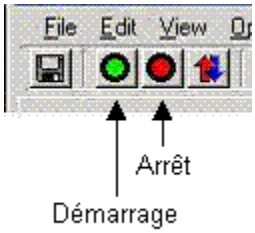
Selon que le collecteur démarre ou s'arrête, le bouton affiché dans la colonne Démarrer/Arrêter change. Si vous travaillez avec un collecteur distant, ce changement de bouton ne se fait pas tant que l'état du collecteur n'a pas été détecté.

Le démarrage ou l'arrêt d'un port entraîne l'exécution du script du démarrage et de retour à l'état antérieur sélectionnés.

Lorsque vous démarrez tous les ports, un port ne démarre que si la case Run Port at Startup (Exécuter le port au démarrage) est cochée dans la boîte de dialogue Other Port Options (Autres options de port) du menu Options.

Pour démarrer et arrêter tous les ports Wizard

1. Dans la fenêtre Wizard :
   - Pour arrêter tous les ports, cliquez sur le bouton Arrêter dans la barre d'outils.
   - Pour démarrer tous les ports, cliquez sur le bouton Démarrer dans la barre d'outils.



Pour démarrer et arrêter les ports Wizard un par un

1. Dans la fenêtre Wizard :
   - Pour arrêter un port, cliquez sur le bouton Arrêt dans la colonne Démarrer/Arrêter correspondant au port.
   - Pour démarrer un port, cliquez sur le bouton Démarrer dans la colonne Démarrer/Arrêter correspondant au port.

Modification de la configuration d'un port Wizard

Si vous modifiez la configuration d'un port en cours d'exécution, le port s'arrête. Pour éviter de perdre des données, arrêtez manuellement le port avant d'en modifier la configuration.

Pour modifier la configuration d'un port Wizard

1. Arrêtez le port de l'hôte voulu.
2. Suivez les instructions relatives à la création d'un port Wizard énoncées au chapitre 3. La nouvelle configuration écrase la configuration existante lorsque vous enregistrez ou que vous téléchargez le port.

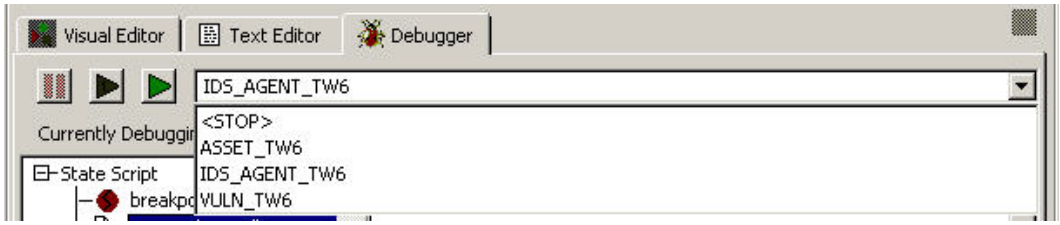
Suppression d'un port Wizard

Pour supprimer un port Wizard

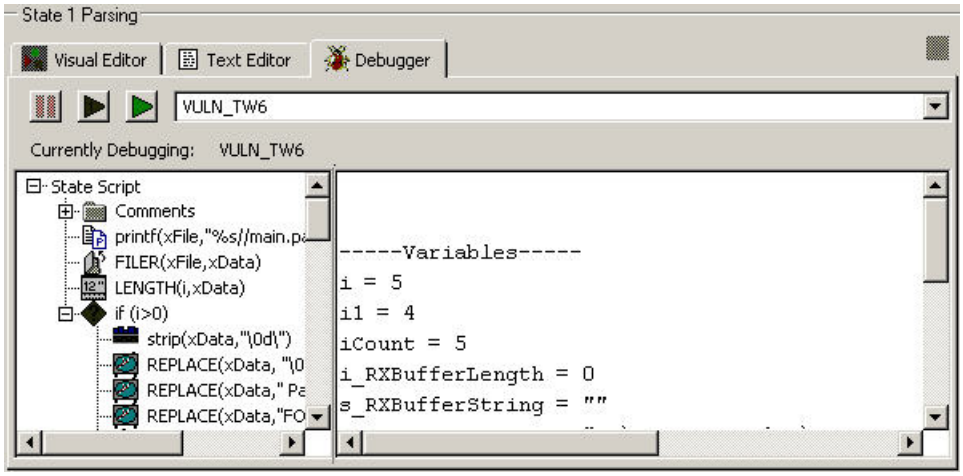
1. Arrêtez le port.
2. Dans le panneau Port Information (Informations de port) du Générateur de collecteurs, cliquez avec le bouton droit sur un port et sélectionnez Delete Port (Supprimer le port). Tous les ports affichés sous ce port supprimé s'arrêtent automatiquement.
3. Vous pouvez effectuer cette suppression localement ou à distance :
   - Hôte local : cliquez sur *Fichier, Enregistrer* et sélectionnez Port Information (Informations de port).
   - Hôte distant : cliquez sur *Fichier* et sur *Upload/Download (Télécharger).*

Débogage d'un port Wizard

L'outil Debugger (Débogueur) vous permet de résoudre les erreurs de code du collecteur s'exécutant sur un port. La partie gauche du panneau Debugger (Débogueur) contient les scripts d'état. La partie droite du panneau contient les variables des scripts et du tampon de réception (Rx Buffer), dont les noms peuvent comprendre jusqu'à 32 caractères.



Pour que le débogueur soit actif, le premier de vos états doit être un état d'analyse et des commandes Breakpoint() (point d'interruption) doivent être présentes.



Lors du débogage, attendez que le tampon de réception Rx Buffer soit mis à jour pour activer une autre fonction.

REMARQUE : si le Gestionnaire des collecteurs n'est plus connecté (), vous ne pouvez pas déboguer un port de l'hôte correspondant.

Pour débogueur un port Wizard

1. Dans Template Editor (Éditeur de modèles), sélectionnez l'onglet Debugger (Débogueur) du panneau de modification pour accéder à la fonctionnalité de débogage. Un panneau vide s'affiche avec une liste déroulante dans laquelle vous pouvez sélectionner le port Wizard que vous voulez déboguer.

   Si vous cliquez sur l'onglet Wizard Hosts (Hôtes Wizard), l'indication Debug (Déboguer) est affichée en face du port en cours de débogage pour indiquer son état.

VULN_TW6	File All	C:\workarea\vuln_inf	DemoVulnerabilityUploa	Stop	Debug
ASSET_TW6	File All	c:\workarea\asset_ou	T1_GNUx_NMAP_035!	Start	Off

2. Dans la liste déroulante, sélectionnez un port et démarrez le processus de débogage. Vous pouvez déboguer le port de deux manières différentes :

   - Appuyez sur F6 pour exécuter les commandes l'une après l'autre ou cliquez sur Execute One Command (Exécuter une commande).

     Pour reprendre l'exécution du script, cliquez à nouveau sur le bouton ou réappuyez sur F6.
   - Appuyez sur F7 pour exécuter les commandes l'une après l'autre ou cliquez sur Resume Command Execution (Reprendre l'exécution de la commande).

     Appuyez sur F5 pour interrompre l'exécution ou cliquez sur le bouton Pause Command Execution (Interrompre l'exécution de la commande).

     L'exécution de la commande est donc interrompue jusqu'à ce que vous appuyiez sur F7 ou que vous cliquiez sur Resume Command Execution (Reprendre l'exécution de la commande).

   Le débogueur marque une pause à tous les points d'interruption mais continue de s'exécuter. L'état du port est défini sur Actif.

   En mode débogage, aucun événement n'est envoyé lors des interruptions d'exécution.

   Lorsque l'analyseur est fermé, ces boutons sont grisés et la liste déroulante est définie sur « No Port is being Debugged » (Aucun port en cours de débogage).

   Le débogueur ne met pas fin à une interruption d'exécution. Par conséquent, si vous déboguez un analyseur ayant atteint une commande d'interruption (PAUSE), l'action correspondant à un clic sur le bouton Arrêter ou le bouton Step (Pas à pas) ne s'applique pas tant que l'interruption n'a pas pris fin.

Téléchargement de collecteurs et d'hôtes

La fenêtre Upload/Download (Téléchager) dispose de trois onglets :

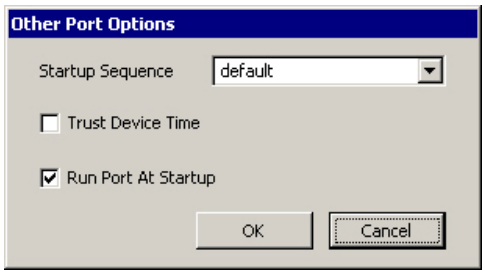
- Hosts (Hôtes) : téléchargement de chaque configuration de port et de chaque ensemble de collecteurs vers les hôtes indiqués. Les hôtes de destination conservent leur configuration de port et leur ensemble de collecteurs.
- Collecteurs : téléchargement des collecteurs un par un.
- Populate Network (Propager à tout le réseau) : téléchargement de la configuration de port et des collecteurs d'un seul hôte vers tous les hôtes sélectionnés. Ces derniers sont alors dotés de la même configuration de port et du même ensemble de collecteurs que l'hôte source.

Lors du téléchargement, la configuration de port d'un collecteur distant s'applique à l'hôte local sélectionné pour recevoir le téléchargement et tout collecteur de l'hôte distant qui porte le même nom qu'un collecteur de l'hôte local est écrasé.

Téléchargement d'un collecteur vers un seul hôte

Pour télécharger un collecteur vers un seul hôte

1. Si votre collecteur est déjà correctement configuré et que vous avez généré votre script, vous pouvez ignorer les étapes 2 à 11.
2. Cliquez sur l'onglet Wizard Hosts (Hôtes Wizard) et sélectionnez un hôte.
3. Dans la colonne Port Name (Nom du port), double-cliquez sur *Nouveau...* et entrez un nom de votre choix.
4. Dans la colonne *Collecteur*, sélectionnez un collecteur.
5. Configurez le collecteur en respectant les indications de la documentation du collecteur (`%WORKBENCH_HOME%\Elements\<nom du collecteur>\docs\<nom du fichier>.pdf`).
6. Cliquez sur l'onglet *Collecteurs*, développez le nœud Collecteur et sélectionnez le fichier de modèle.
7. À droite, cliquez sur l'onglet *Paramètres*.
8. Définissez les valeurs des paramètres en fonction des indications de la documentation du collecteur.
9. (Facultatif) Si vous souhaitez que ce collecteur ne s'exécute pas au démarrage ou qu'il se fie à l'heure indiquée par le périphérique, cliquez sur l'onglet *Wizard Host* (Hôte Wizard), cliquez avec le bouton droit sur le port Wizard voulu, sélectionnez *Other Port Options (Autres options de port)* et décochez la case *Run Port At Startup (Exécuter le port au démarrage)* ou cochez la case *Trust Device Time (Se fier à l'heure du périphérique)*. Cliquez sur *OK*.



10. Cliquez sur *Enregistrer*.
11. Cliquez sur l'onglet *Collecteurs*, cliquez avec le bouton droit sur le fichier de modèle souhaité et sélectionnez *Build Script (Générer un script)*.
12. Procédez de l'une des façons suivantes :
    - Cliquez sur *Fichier* et sélectionnez *Upload/Download (Télécharger).*
    - Cliquez avec le bouton droit sur le collecteur puis sélectionnez *Upload Collector (Télécharger le collecteur)*.
    - Cliquez sur le bouton *Upload/Download (Télécharger) :* 

    La fenêtre Upload/Download (Télécharger) s'ouvre.
13. Dans la fenêtre *Upload/Download (Télécharger)*, cliquez sur l'onglet *Collecteurs*.
14. Dans la liste déroulante, sélectionnez le collecteur que vous souhaitez télécharger.
15. Cliquez sur *Upload (Télécharger)*. La première fois que vous effectuez cette opération, le mot de passe du Gestionnaire des collecteurs vous sera demandé, même s'il s'agit d'un hôte Wizard local. La fenêtre indiquant la progression du téléchargement s'ouvre et affiche l'avancement du transfert en cours.

REMARQUE: vous pouvez vous servir de cette fenêtre de progression du téléchargement pour redémarrer les hôtes une fois le téléchargement terminé.

Téléchargement d'un collecteur vers plusieurs hôtes

Pour télécharger un collecteur vers plusieurs hôtes

ATTENTION : si vous téléchargez un hôte dont un collecteur porte le même nom qu'un collecteur de l'hôte local, le collecteur de l'hôte distant est écrasé sans que vous en soyez averti.

1. Si votre collecteur est déjà correctement configuré et que vous avez généré votre script, vous pouvez ignorer les étapes 2 à 11.
2. Cliquez sur l'onglet *Wizard Hosts* (Hôtes Wizard) et sélectionnez un hôte.
3. Dans la colonne Port Name (Nom du port), double-cliquez sur *Nouveau...* et entrez un nom de votre choix.
4. Dans la colonne *Collecteur*, sélectionnez un collecteur.
5. Configurez le collecteur en respectant les indications de la documentation du collecteur (`%WORKBENCH_HOME%\Elements\<nom du collecteur>\docs\<nom du fichier>.pdf`).
6. Cliquez sur l'onglet *Collecteurs*, développez le nœud Collecteur et sélectionnez le fichier de modèle.
7. À droite, cliquez sur l'onglet *Paramètres*.
8. Définissez les valeurs des paramètres en fonction des indications de la documentation du collecteur.
9. (Facultatif) Si vous souhaitez que ce collecteur ne s'exécute pas au démarrage ou qu'il se fie à l'heure indiquée par le périphérique, cliquez sur l'onglet *Wizard Host* (Hôte Wizard), cliquez avec le bouton droit sur le port Wizard voulu, sélectionnez Other Port Options (Autres options de port) et décochez la case Run Port At Startup (Exécuter le port au démarrage*)* ou cochez la case Trust Device Time (Se fier à l'heure du périphérique). Cliquez sur OK.

10. Cliquez sur *Enregistrer*.
11. Cliquez sur l'onglet *Collecteurs* pour ouvrir le panneau de l'arborescence des collecteurs.
12. Cliquez sur un collecteur.
13. Procédez de l'une des façons suivantes :
    - Cliquez sur *Fichier* et sélectionnez Upload/Download (Télécharger).
    - Cliquez avec le bouton droit sur le collecteur puis sélectionnez Upload Collector (Télécharger le collecteur).
    - Cliquez sur le bouton Upload/Download (Télécharger) *:* 

    La fenêtre Upload/Download (Télécharger) s'ouvre.
14. Dans la fenêtre Upload/Download (Télécharger), cliquez sur l'onglet Hosts (Hôtes) et cochez ou décochez la case Upload Collectors When Uploading (Télécharger les collecteurs lors du téléchargement vers l'hôte).

    Lorsque cette case est cochée, les collecteurs sélectionnés dans l'onglet Collecteurs sont téléchargés. Par défaut, cette case est cochée. Cette option ne s'applique pas lors d'une récupération de collecteurs à partir d'un hôte distant.
15. Dans la liste, sélectionnez les hôtes Wizard vers lesquels vous souhaitez télécharger les collecteurs.

    Tous les hôtes Wizard du réseau sont automatiquement inclus dans la liste. Des boutons spécifiques indiquent si la machine de l'hôte est en ligne ou pas.

    Cliquez sur Sélectionner tout pour sélectionner l'intégralité des hôtes Wizard de la liste. Cliquez sur Select None (Désélectionner tout) pour n'en sélectionner aucun.
16. Cliquez sur Upload (Télécharger) pour télécharger les collecteurs sélectionnés vers le ou les hôtes sélectionnés. La première fois que vous effectuez cette opération, le mot de passe du Gestionnaire des collecteurs vous sera demandé, même s'il s'agit d'un hôte Wizard local.

Téléchargement d'un hôte

Pour télécharger un hôte

ATTENTION : si vous téléchargez un hôte dont un collecteur porte le même nom qu'un collecteur de l'hôte local, le collecteur de l'hôte local est écrasé sans que vous en soyez averti.

1. Cliquez sur l'onglet Wizard Hosts (Hôtes Wizard) pour ouvrir le panneau de l'arborescence des hôtes.
2. Dans cette arborescence, cliquez sur l'hôte que vous souhaitez récupérer.
3. Procédez de l'une des façons suivantes :
    - Cliquez sur Fichier et sélectionnez Upload/Download (Télécharger).
    - Cliquez avec le bouton droit sur le collecteur puis sélectionnez Upload Collector (Télécharger le collecteur).
    - Cliquez sur le bouton Upload/Download (Télécharger) : 

    La fenêtre Upload/Download (Télécharger) s'ouvre. Le collecteur sélectionné est coché par défaut.

4. Cliquez sur Download (Télécharger). La première fois que vous effectuez cette opération, le mot de passe du Gestionnaire des collecteurs vous sera demandé, même s'il s'agit d'un hôte Wizard local. L'hôte est téléchargé et ajouté à l'arborescence des hôtes Wizard. La fenêtre indiquant la progression du téléchargement s'ouvre et affiche l'avancement du transfert en cours.

REMARQUE: vous pouvez vous servir de cette fenêtre de progression du téléchargement pour redémarrer les hôtes une fois le téléchargement terminé.

REMARQUE : vous ne pouvez télécharger qu'un seul hôte à la fois. Si vous sélectionnez plusieurs hôtes, les téléchargements ne démarrent pas.

Téléchargement des collecteurs à partir d'un seul hôte

Pour télécharger des collecteurs à partir d'un seul hôte

1. Procédez de l'une des façons suivantes :
   - Cliquez sur Fichier et sélectionnez Upload/Download (Télécharger).
   - Cliquez sur le bouton Upload/Download (Télécharger) : 

   La fenêtre Upload/Download (Télécharger) s'ouvre.
2. Dans la liste, sélectionnez l'hôte Wizard à partir duquel vous souhaitez télécharger les collecteurs.

   Tous les hôtes Wizard du réseau sont automatiquement inclus dans la liste. Des boutons spécifiques indiquent si la machine de l'hôte est en ligne ou pas.

   Cliquez sur Sélectionner tout pour sélectionner l'intégralité des hôtes Wizard de la liste. Cliquez sur Select None (Désélectionner tout) pour n'en sélectionner aucun.
3. Cliquez sur Download (Télécharger) pour télécharger les collecteurs à partir des hôtes sélectionnés.

Téléchargement de ports vers plusieurs hôtes

Pour télécharger des ports vers plusieurs hôtes

1. Procédez de l'une des façons suivantes :
   - Cliquez sur Fichier et sélectionnez Upload/Download (Télécharger).
   - Cliquez sur le bouton Upload/Download (Télécharger) : 
2. La fenêtre Upload/Download (Télécharger) s'ouvre.
3. Dans la fenêtre Upload/Download (Télécharger), cliquez sur l'onglet Populate Network (Propager à tout le réseau).
4. Dans la liste intitulée « Select which host's port configuration and Collectors you would like to upload » (Sélectionnez l'hôte dont vous souhaitez télécharger la configuration de port et les collecteurs), sélectionnez l'hôte dont vous voulez télécharger les paramètres de configuration de port et les collecteurs.
5. Dans la liste intitulée « Select hosts you would like to upload this configuration to » (Sélectionnez les hôtes vers lesquels vous souhaitez télécharger cette configuration), sélectionnez l'hôte vers lequel vous voulez télécharger les paramètres sélectionnés.

Tous les hôtes Wizard du réseau sont automatiquement inclus dans la liste. Des boutons spécifiques indiquent si la machine de l'hôte est en ligne ou pas.

Cliquez sur Sélectionner tout pour sélectionner l'intégralité des hôtes Wizard de la liste. Cliquez sur Select None (Désélectionner tout) pour n'en sélectionner aucun.

Téléchargement de plusieurs collecteurs vers un réseau

Pour télécharger plusieurs collecteurs vers un réseau

1. Dans la fenêtre Wizard principale, sélectionnez un collecteur dans l'arborescence des collecteurs.
2. Procédez de l'une des façons suivantes :
   - Cliquez sur Fichier et sélectionnez Upload/Download (Télécharger).
   - Cliquez avec le bouton droit sur le collecteur puis sélectionnez Upload Collector (Télécharger le collecteur).
   - Cliquez sur le bouton Upload/Download (Télécharger) : 
3. Sélectionnez l'onglet Populate Network (Propager à tout le réseau).
4. Dans le menu déroulant de la première zone de sélection, sélectionnez l'hôte dont vous souhaitez télécharger la configuration de port et les collecteurs.
5. Dans le menu déroulant de la deuxième zone de sélection, sélectionnez les hôtes vers lesquels vous souhaitez télécharger la configuration.

   REMARQUE: au moins un élément doit être sélectionné dans l'une des zones de sélection si vous voulez pouvoir télécharger la configuration de l'élément concerné.

   Vous pouvez sélectionner un collecteur différent selon le menu déroulant. Chaque collecteur sélectionné dans la liste principale récupère la configuration de port et les collecteurs de l'hôte sélectionné dans la zone intitulée

   « Sélectionnez l'hôte dont vous souhaitez télécharger la configuration de port et les collecteurs », sauf si Select None (Tout désélectionné) est défini.
6. Lorsque vous avez terminé de paramétrer la configuration du réseau, cliquez sur le bouton Upload (Télécharger) pour démarrer le processus de transfert.

Mise à niveau des collecteurs

Pour mettre à niveau les collecteurs

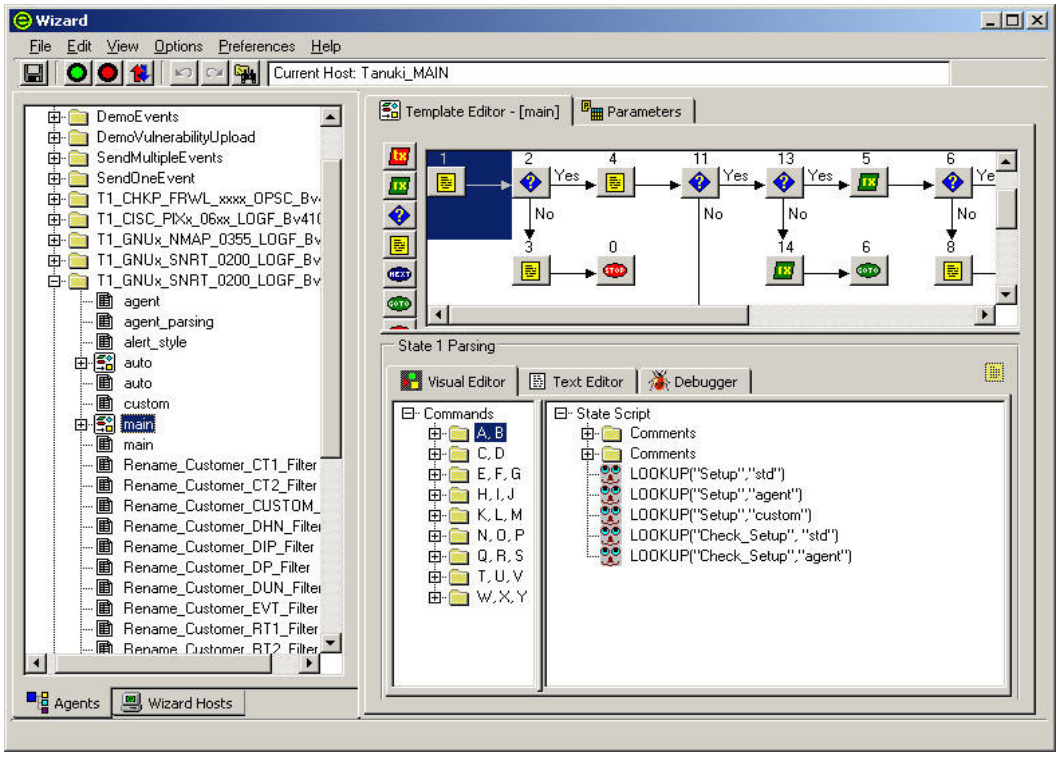
1. Prenez connaissance de la documentation qui accompagne le nouveau collecteur et qui en décrit les modifications.
2. Installez la nouvelle version du collecteur dans le répertoire %workbench_home%/Elements sur l'ordinateur principal choisi pour le collecteur.
3. Ouvrez le fichier de paramètre du collecteur à remplacer. Coupez et collez les paramètres appropriés dans le nouveau collecteur.
4. Le cas échéant, supprimez ou ajoutez des variables de paramètre selon les instructions de la documentation du nouveau collecteur. Si vous ajoutez des variables de paramètre, vous devez indiquer vous-même les valeurs de ces variables.
5. Enregistrez le fichier de paramètre dans le nouveau collecteur.
6. Générez le nouveau collecteur.
7. Modifiez les informations de configuration de port de façon à pouvoir utiliser correctement le nouveau collecteur.
8. Enregistrez ces informations.
9. Téléchargez le nouveau collecteur et la configuration de port correspondante.
10. Redémarrez le port.

3 Génération et gestion des collecteurs

REMARQUE : les termes Agent et Collecteur sont interchangeables. Le terme Collecteur sera utilisé dans la suite de cette documentation.

REMARQUE : pour les utilisateurs de Microsoft SQL 2000, la taille d'un événement ne peut pas dépasser 8 Ko.

Un collecteur est chargé d'analyser des données provenant d'un dispositif qui génère des événements de sécurité et d'envoyer des événements vers Sentinel. La création, l'activation et la gestion des collecteurs se font à l'aide du Générateur de collecteurs Wizard. Cliquez sur l'onglet *Collecteurs* pour afficher l'arborescence correspondante et faire apparaître tous les collecteurs et les composants de collecteur installés sur votre système Sentinel.



Le gestionnaire des collecteurs vous permet de :

- générer des collecteurs :
  - création et configuration de fichiers de modèle ;
  - création de fichiers de paramètre ;
  - création de fichiers de recherche ;

    - génération de scripts ;
    - création d'un port Wizard.

Notions de base nécessaires à la génération d'un collecteur

Les principales étapes de génération d'un collecteur sont les suivantes :

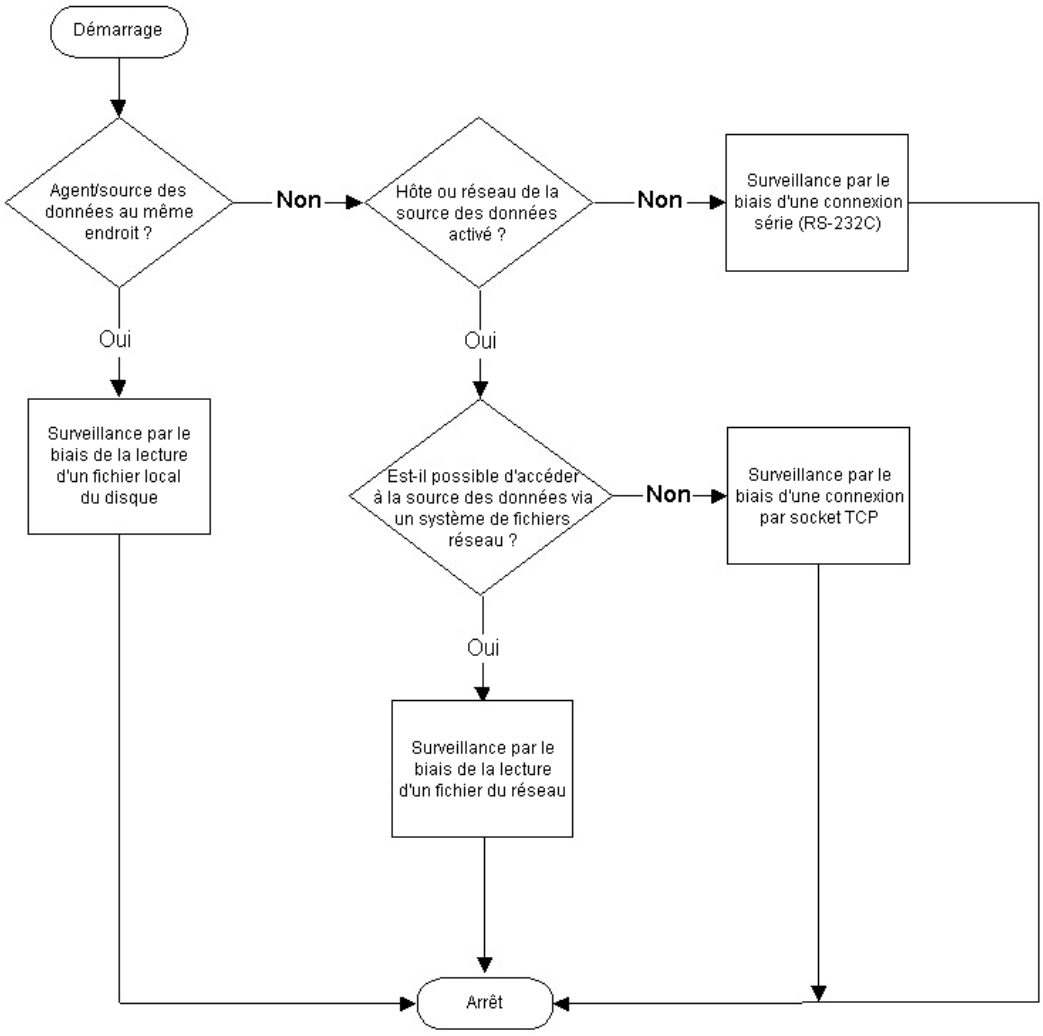
- créer et configurer des fichiers de modèle, en précisant les points décisionnels en fonction de la façon dont les états sont appliqués ;
- créer et configurer un fichier de paramètre ;
- créer et configurer un fichier de recherche (facultatif) ;
- générer un script ;
- assigner une séquence de démarrage ;
- créer un port et lui assigner un collecteur avant de le démarrer.

Principales étapes d'implémentation d'un collecteur

Les principales étapes d'implémentation d'un collecteur sont les suivantes :

- définition des données à surveiller ;
- définition de la manière dont les données doivent être surveillées ;
- définition du système d'exploitation sous lequel est exécuté le produit :
    - lorsque l'hôte et le produit se trouvent au même endroit, la logique veut que les données soient obtenues par lecture du fichier journal du produit ;
    - lorsque l'hôte et le produit ne sont pas installés sur la même machine, les données sont obtenues par l'intermédiaire d'un système de fichiers réseau (partage de fichiers NFS, Samba ou SMB), une connexion par socket TCP/IP ou une connexion série ;

- génération des collecteurs et démarrage des ports ;
- en cas d'utilisation d'hôtes distants, téléchargement des fichiers de collecteur vers ces hôtes distants et démarrage du port pour exécuter les scripts de démarrage (les informations récupérées sont ensuite transmises au système Sentinel).



Génération d'un collecteur

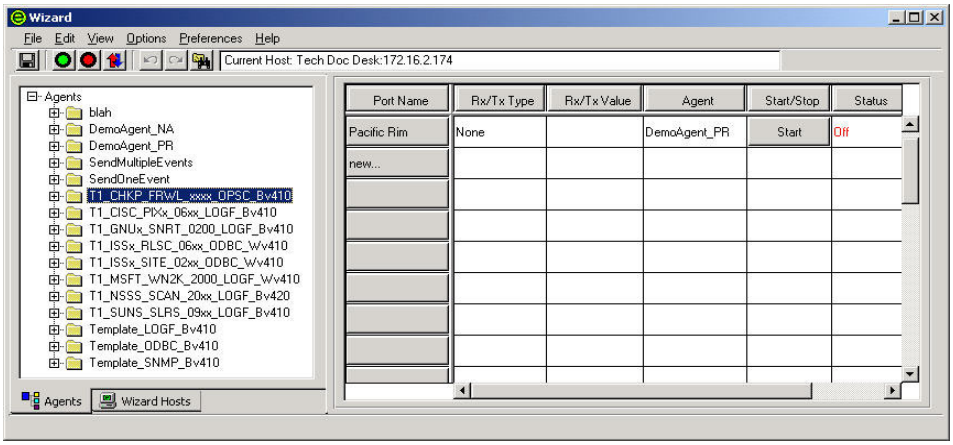
Comme mentionné plus avant, la génération d'un collecteur exige la création des éléments suivants :

- fichiers de modèle ;
- fichiers de paramètre ;
- fichiers de recherche (facultatif) ;
- scripts ;
- assignation d'un nom de port Wizard à un collecteur.

Création et configuration de fichiers de modèle

Pour créer et configurer des fichiers de modèle

1. Lancez le Générateur de collecteurs.
2. Cliquez sur l'onglet *Collecteurs* pour ouvrir le panneau de l'arborescence des collecteurs.
3. Dans l'arborescence des collecteurs, cliquez avec le bouton droit sur *Collecteurs*, puis sélectionnez *New Collector (Nouveau collecteur)*.
4. Entrez le nom du nouveau collecteur dans la zone prévue à cet effet et appuyez sur Entrée.
5. Cliquez avec le bouton droit sur le nouveau collecteur, puis sélectionnez *New Template (Nouveau modèle)*.



6. Dans la zone New Template (Nouveau modèle) de l'arborescence des collecteurs, tapez un nom et appuyez sur Entrée.
7. Sélectionnez le nouveau modèle et cliquez sur l'onglet *Template Editor (Éditeur de modèles)*.
8. Dans le panneau *Template Editor (Éditeur de modèles)*, déplacez les états en les faisant glisser vers la zone d'édition à l'aide des boutons d'état situés à gauche du panneau. Pour plus d'informations sur l'ajout d'états à un modèle, voir la rubrique Ajout d'un état à un fichier de modèle.
9. Cliquez sur *Enregistrer*.

Ajout d'un état à un fichier de modèle

Tous les collecteurs démarrent leur traitement à l'état 1, quel que soit l'emplacement de cet état 1 dans le modèle. En admettant que l'état 1 soit un état de traitement, un nouvel état peut être inséré à la suite de cet état 1.

Le Générateur de collecteurs assigne au premier état le numéro 1. Il est recommandé de faire en sorte que ce premier état contienne uniquement une commande d'analyse BREAKPOINT(). En insérant uniquement un point d'interruption (commande BREAKPOINT) après l'état 1, le débogage est facilité. En cas de débogage, l'analyseur s'arrête automatiquement sur l'état suivant.

Lors de la création d'un modèle, il faut commencer par un état d'analyse contenant uniquement un point d'interruption. Ensuite, il est possible d'ajouter l'état de fonctionnement (état de réception, d'analyse, etc.) en tant qu'état 2. Lorsqu'il est nécessaire d'ajouter un état au début du modèle, il ne doit être inséré qu'après le point d'interruption.

Il est conseillé de ne supprimer l'état d'analyse comprenant le point d'interruption que lorsque l'ajout d'un état au début du modèle est vraiment nécessaire. Le cas échéant, il est possible d'entrer des commentaires concernant la fonctionnalité du modèle dans cette commande BREAKPOINT.

Pour ajouter un état à un modèle

1. Cliquez sur l'onglet *Collecteurs* pour ouvrir le panneau de l'arborescence des collecteurs.
2. Dans l'arborescence des collecteurs, sélectionnez un modèle pour pouvoir afficher Template Editor (Éditeur de modèles) dans le panneau de droite.
3. Cliquez sur *Options >Add State (Ajouter un état)*, puis sélectionnez l'un des états *Transmit (Transmettre), Receive (Recevoir), Decide (Décider), Parse (Analyser), Next (Suivant), Go To (Retourner à)* et *Arrêter* ou cliquez sur les boutons correspondants.
   -  Transmit (Transmettre)
   -  Receive (Recevoir)
   -  Decide (Décider)
   -  Parse (Analyser)
   -  Next (Suivant)
   -  Go To (Retourner à)
   -  Arrêter
4. À l'aide des panneaux d'édition situés dans la partie inférieure du panneau Template Editor (Éditeur de modèles), insérez un nouveau code pour chaque état que vous ajoutez.

Une autre méthode consiste à déplacer un bouton d'état d'analyse en le faisant glisser de la partie gauche du Template Editor (Éditeur de modèles) vers la zone d'édition.

REMARQUE : n'utilisez de guillemets doubles dans la chaîne de décision ni pour l'état de réception (entre autres, pour des raisons de correspondance avec le séparateur dans un fichier journal), ni pour celui de décision, sous peine de voir le message d'erreur suivant s'afficher :

```
***ERROR: Reading Template File..." (ERREUR lors de la lecture du fichier de modèle)
```

Lorsque des guillemets doubles sont insérés dans une chaîne de décision ou de séparation, une anomalie est générée :

```
StateDecideString: "test"123"
```

Pour éviter ce problème, utilisez \22\ au lieu de (").

REMARQUE : si vous sélectionnez un autre élément de l'onglet Collecteurs (même si cet élément fait partie du même collecteur) et que vous revenez au modèle qui pose problème, le Générateur de collecteurs génère le message d'erreur ci-dessus et n'affiche aucun élément ni aucun état du modèle. L'erreur est générée parce qu'un guillemet double (") est utilisé pour séparer des valeurs de champ dans un fichier .tem. Par exemple :

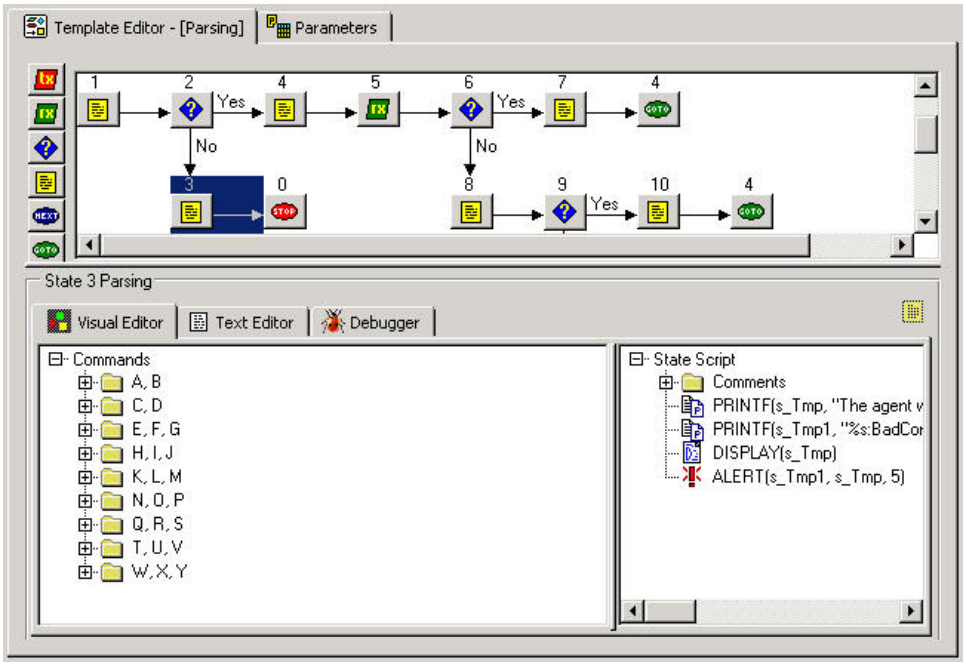
```
StateDecideString: "test"
StateDelimiterString: "123"
```

Entrée d'une commande d'analyse à l'aide de l'éditeur plein écran

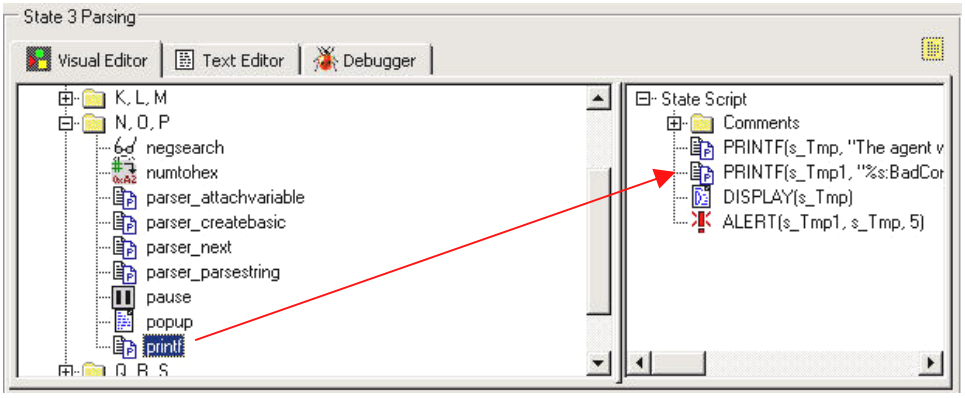
Il existe deux façons d'entrer une commande d'analyse : en utilisant l'éditeur plein écran ou l'éditeur de texte. Limitez le nombre de vos commandes à 4 096.

Pour entrer une commande d'analyse à l'aide de l'éditeur plein écran

1. Dans l'éditeur Template Editor (Éditeur de modèles), sélectionnez un état d'analyse. L'onglet correspondant à l'éditeur plein écran s'ouvre par défaut lorsque vous cliquez sur un modèle.



2. Dans cet éditeur, faites glisser les commandes d'analyse à droite du panneau.



3. Entrez les valeurs des arguments dans la fenêtre de l'éditeur de commande contextuelle.
   - Sélectionnez un type : les types possibles pour chaque commande d'analyse sont décrits dans le Guide des références utilisateur de Sentinel.

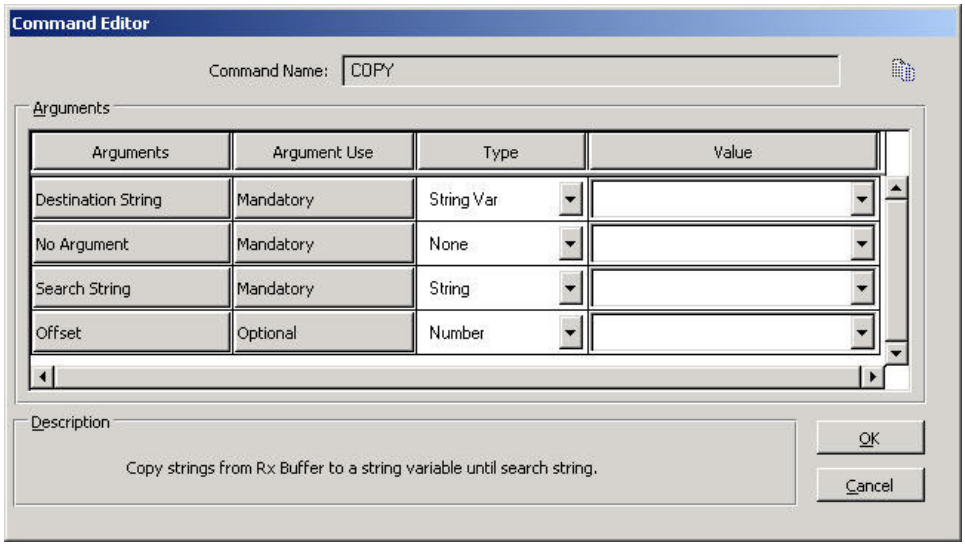
- Spécifiez une valeur : les valeurs sont définies pour une application spécifique. Des exemples de valeurs possibles pour chaque commande d'analyse sont indiqués dans le Guide des références utilisateur de Sentinel.

Pour entrer une commande d'analyse à l'aide de l'éditeur de texte

1. Dans l'éditeur Template Editor (Éditeur de modèles), cliquez sur l'onglet correspondant à l'éditeur de texte.
2. Entrez manuellement vos commandes d'analyse.

   Servez-vous de la touche Tab du clavier pour aligner votre texte lorsque vous utilisez une police fixe. Copiez, coupez et collez vos options de la même manière que dans un éditeur de texte classique.

Modification d'une commande d'analyse



- Arguments : comprend tous les arguments disponibles pour la commande d'analyse sélectionnée dans l'éditeur plein écran.
- Argument Use (Utilisation de l'argument) : définit si l'argument est obligatoire ou facultatif.
- Type : détermine le type de la variable (chaîne, variable de chaîne, nombre, variable de nombre, valeur flottante, variable flottante ou variable prédéfinie).
- Valeur : valeur définie pour la variable déterminée dans la colonne Type.

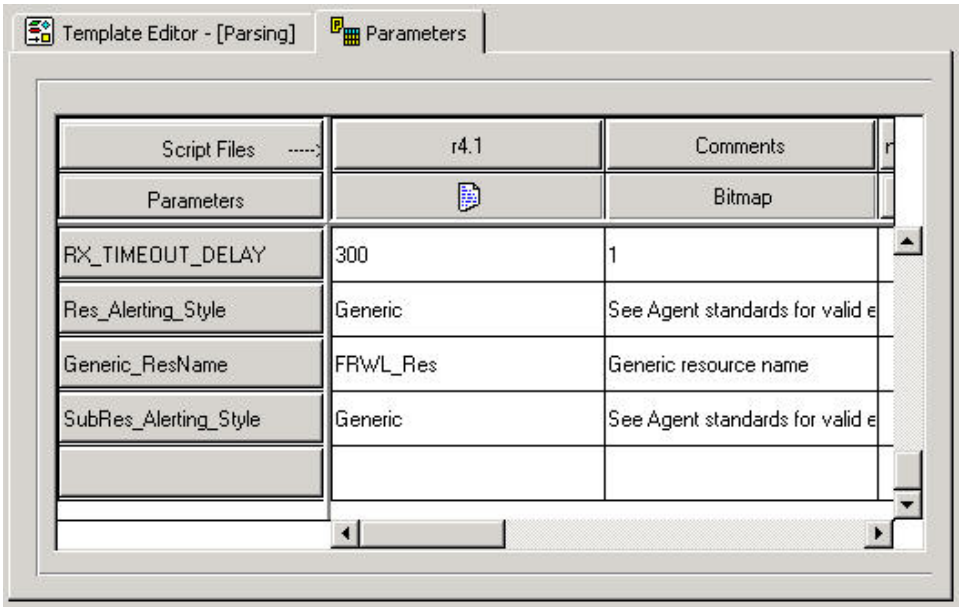
Pour modifier une commande d'analyse

1. Dans l'éditeur plein écran, procédez de l'une des façons suivantes :
   - Cliquez avec le bouton droit sur la commande d'analyse et sélectionnez *Add to State Parsing List (Ajouter à la liste d'analyse des états)*.
   - Double-cliquez sur une commande d'analyse. L'éditeur Command Editor (Éditeur de commandes) s'ouvre.
2. Renseignez les types et les valeurs souhaitées dans les zones de liste déroulante correspondantes pour terminer la modification. Pour plus d'informations sur les descriptions de commande d'analyse, reportez-vous au *Guide des références utilisateur de Sentinel*.

Création et configuration de fichiers de paramètre

Pour créer et configurer des fichiers de paramètre

1. Cliquez sur l'onglet *Collecteurs*.
2. Sélectionnez un modèle et cliquez sur l'onglet *Paramètres* dans le panneau de droite.



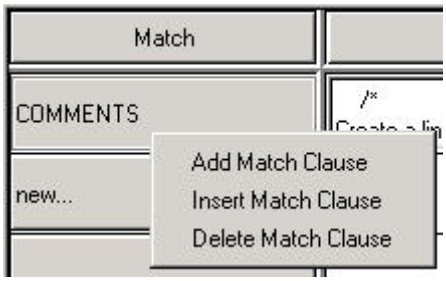
3. Double-cliquez sur le bouton *Nouveau...* dans la première colonne du tableau des paramètres.
4. Entrez le nom du nouveau paramètre (il s'agit du nom du script, r4.1 par exemple) et appuyez sur Entrée.
5. (Facultatif) Cliquez avec le bouton droit sur le bouton *Bitmap* (deuxième colonne/deuxième ligne) et cliquez sur *Assign Bitmap (Assigner un bouton Bitmap)*. Dans la boîte de dialogue Bitmap Assignment (Assignation de bouton Bitmap), sélectionnez un bouton *Bitmap*.
6. Double-cliquez sur chacune des zones d'édition des nouveaux paramètres et entrez les valeurs appropriées.
7. Une fois toutes les valeurs définies, le fichier de paramètre et le fichier de modèle doivent être compilés pour créer un script. Reportez-vous à la section Génération d'un script.

Création et configuration de fichiers de recherche

Cette procédure est facultative.

Pour créer et configurer des fichiers de recherche

1. Cliquez sur l'onglet *Collecteurs* pour ouvrir le panneau de l'arborescence des collecteurs.
2. Cliquez avec le bouton droit sur un collecteur, puis sélectionnez *New Lookup File (Nouveau fichier de recherche)*.
3. Dans la zone New Lookup File (Nouveau fichier de recherche), tapez un nom et appuyez sur Entrée.
4. Dans la colonne Match (Correspondance), double-cliquez sur *Nouveau...*, entrez la chaîne à faire correspondre et appuyez sur Entrée. Vous pouvez ajouter, insérer et supprimer des clauses de correspondance.
   - Ajout : dans la colonne Match (Correspondance), cliquez avec le bouton droit sur une clause de correspondance et sélectionnez *Add Match Clause (Ajouter une clause de correspondance)*.
   - Insertion : dans la colonne Match (Correspondance), cliquez avec le bouton droit sur une clause de correspondance et sélectionnez *Insert Match Clause (Insérer une clause de correspondance)*.
   - Suppression : dans la colonne Match (Correspondance), cliquez avec le bouton droit sur une clause de correspondance et sélectionnez *Delete Match Clause (Supprimer une clause de correspondance)*.



5. (Facultatif) : pour entrer des commandes d'analyse, cliquez avec le bouton droit dans la colonne Parsing (Analyse) pour ouvrir l'éditeur plein écran. Pour plus d'informations sur l'utilisation de l'éditeur plein écran, voir Entrée d'une commande d'analyse à l'aide de l'éditeur plein écran.
6. Sélectionnez les commandes d'analyse voulues et définissez-les dans Command Editor (Éditeur de commandes). Les commandes s'affichent dans la colonne Parsing (Analyse).
7. Une fois toutes les valeurs définies, le fichier de recherche doit être compilé pour créer un script. Reportez-vous à la section Génération d'un script.

Scripts

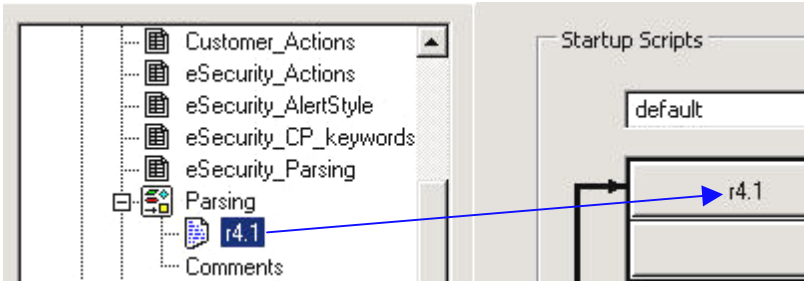
Les scripts sont générés en fonction de modèles. Un seul modèle vous permet de générer plusieurs scripts. Le gestionnaire des collecteurs vous permet de :

- générer un script ;
- déboguer un script ;
- assigner une séquence de démarrage à un script.

Génération d'un script

Pour générer un script

1. Cliquez sur l'onglet *Collecteurs* pour ouvrir le panneau de l'arborescence des collecteurs.
2. Dans le panneau de gauche, sélectionnez le modèle en fonction duquel vous voulez générer vos scripts.
3. Sélectionnez *Fichier* > *Build Scripts (Générer des scripts)*.
4. Dans l'onglet Template Editor (Éditeur de modèles), faites glisser un script du modèle vers la colonne Startup Scripts (Scripts de démarrage) ou Backout Scripts (Scripts de retour à l'état antérieur) du panneau de droite.



Les scripts s'exécutent dans l'ordre dans lequel ils apparaissent dans les colonnes Startup Scripts (Scripts de démarrage) et Backout Scripts (Scripts de retour à l'état antérieur). Pour réorganiser l'ordre des scripts, faites glisser les scripts vers le haut ou vers le bas dans les colonnes.

REMARQUE : le dernier script d'une séquence de retour à l'état antérieur doit se terminer sur l'état de traitement Arrêter.

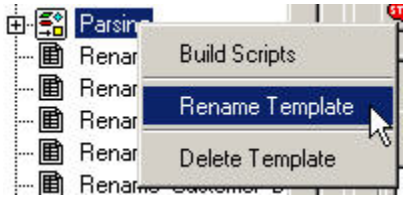
5. (Facultatif) Déboguez vos scripts à l'aide du débogueur.
6. Cliquez sur *Fichier* > *Enregistrer*.
7. Pour que les modifications soient appliquées, démarrez et arrêtez le port à l'aide des boutons Arrêter et Démarrer dans la barre d'outils.

Activation de la fonctionnalité AutoBuild (Génération automatique) pour les collecteurs antérieurs à la version 5.0

La fonctionnalité AutoBuild (Génération automatique) vous permet de configurer et de déployer des collecteurs sans passer par l'étape de génération du script.

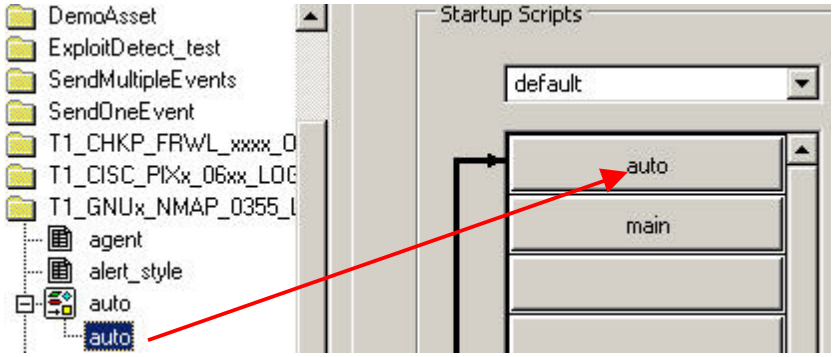
Pour activer la fonctionnalité AutoBuild (Génération automatique) sur les collecteurs antérieurs à la version 5.0

1. Copiez les fichiers suivants dans le collecteur version 5.* existant et placez-les dans le collecteur pour lequel vous souhaitez activer la fonctionnalité AutoBuild (Génération automatique).
   - auto.tem
   - auto.asd
   - auto.lkp
   - auto.par
2. Renommez votre fichier de modèle princ.tem. Vous pouvez effectuer cette opération dans le Générateur de collecteurs.



3. Sélectionnez le fichier de modèle renommé et cliquez sur l'onglet *Paramètres*. Remplacez le nom affiché dans l'en-tête de la colonne portant le nom de votre fichier de script (r4.1, par exemple) par « princ » et appuyez sur la touche Entrée.

4. Cliquez sur le bouton *Enregistrer*.
5. Dans la chaîne Startup (Démarrage), cliquez avec le bouton droit sur auto.asd et faites-le glisser pour le placer avant « princ ».



Débogage d'un script

Lorsque vous commencez le débogage, l'état du port est défini sur « Debug » (Déboguer) dans le panneau d'informations du port. Pour déboguer un script, voir la section Débogage d'un port Wizard au chapitre 2.

Assignation d'une séquence de démarrage à un script

Si vous souhaitez qu'un port soit exécuté au démarrage, vous pouvez définir une séquence de démarrage de sorte qu'elle exécute un ensemble de scripts précis au démarrage. Une séquence de démarrage est un fichier contenant les noms des scripts à exécuter au démarrage.

Pour assigner une séquence de démarrage à un script

1. Cliquez avec le bouton droit sur le nom d'un script dans l'arborescence des collecteurs et sélectionnez New Startup Sequence (Nouvelle séquence de démarrage). La boîte de dialogue correspondante s'affiche.
2. Dans la boîte de dialogue New Startup Sequence (Nouvelle séquence de démarrage), tapez le nom de la séquence puis cliquez sur *OK*. La séquence de démarrage ainsi créée est ajoutée au menu, dans la partie supérieure du panneau Startup Scripts (Scripts de démarrage). Pour les noms de séquence, respectez les instructions suivantes :
   - N'utilisez pas les termes « startup » (démarrage) ou « backout » (retour à l'état antérieur) dans vos noms de séquence.
   - N'utilisez pas deux fois le même nom de séquence dans un collecteur.
3. Faites glisser les fichiers de script de l'arborescence des collecteurs vers la colonne Startup Scripts (Scripts de démarrage). Les scripts sont exécutés dans l'ordre dans lequel ils apparaissent dans la colonne, du haut vers le bas.
4. Pour réorganiser l'ordre des scripts, déplacez les scripts dans la colonne en les faisant glisser vers le haut et vers le bas, ou cliquez avec le bouton droit dans le panneau *Startup Scripts (Scripts de démarrage)* et sélectionnez *Reorder Startup Script (Réorganiser les scripts de démarrage).*

Création d'un port Wizard

Vous pouvez créer plusieurs ports pour un collecteur. Pour certains types de capteur, il se peut que vous deviez créer plusieurs instances d'un même collecteur et assigner chacune d'entre elles à un port différent.

Le type de connexion d'un port détermine la manière dont les données de sécurité sont lues, les informations à lire et le moment où la connexion est établie. Les types de connexion sont les suivants :

- Serial (série)
- Socket
- File New (fichier actualisé)
- File All (tout le fichier)
- Persistent Process (processus permanent)
- Transient Process (processus temporaire)
- SNMP Trap (trappes SNMP)
- None (aucun)

Type de connexion Serial (série)

Le type de connexion Serial est utilisé si les données doivent être lues sur un port série de type RS-232C, par l'intermédiaire d'un câble série ou d'un modem. Vous devez indiquer le port série adéquat (COM1, COM2, etc.) dans la zone Rx/Tx Value (Valeur Rx/Tx). L'hôte exécutant le produit à surveiller doit également disposer d'une connexion série à l'hôte qui héberge le collecteur, soit directement, par le biais d'un câble série, soit par l'intermédiaire de modems à chaque extrémité de la connexion.

Pour ce type de connexion, d'autres modifications et paramétrages sont à prévoir.

Type de connexion Socket

La connexion par socket s'utilise lorsque les données sont lues à partir d'une connexion par socket TCP. Dans la zone Rx/Tx Value (Valeur Rx/Tx), entrez l'adresse IP et le numéro de port TCP de l'hôte distant. L'adresse IP et le numéro de port TCP doivent être séparés par un deux-points. Par exemple, pour indiquer un port SMTP, entrez les informations suivantes dans la zone Rx/Tx Value (Valeur Rx/Tx) :

```
<Adresse IP>:<port>
```

Vous êtes également susceptible de devoir placer un processus serveur de socket TCP sur l'hôte distant et de le configurer de sorte qu'il achemine les données vers le port TCP.

Pour plus d'informations sur la configuration des collecteurs avec ce type de connexion, reportez-vous à la documentation relative aux collecteurs (Snort, Cisco PIX ou Solaris Syslog) à l'emplacement suivant :

```
%workbench_home%\elements\<nom du collecteur>\docs
```

Type de connexion File New (fichier actualisé)

La connexion de type File New (fichier actualisé) permet de lire uniquement les données d'événement de sécurité qui ont été ajoutées à un fichier après le démarrage du script. Ce type de connexion ouvre le fichier et le lit en commençant par la fin. Vous devez indiquer le chemin d'accès au fichier journal dans la zone Rx/Tx Value (Valeur Rx/Tx).

Pour plus d'informations sur la configuration d'un collecteur avec ce type de connexion, reportez-vous à la documentation relative au collecteur (Solaris Syslog) à l'emplacement suivant :

```
%workbench_home%\elements\<nom du collecteur>\docs
```

Type de connexion File All (tout le fichier)

La connexion de type File All (tout le fichier) lit l'intégralité des données d'événement de sécurité d'un fichier.

Si vous sélectionnez File New ou File All, vous pouvez entrer le nom d'un fichier d'entrée et/ou d'un fichier de sortie dans la zone Rx/Tx Value (Valeur Rx/Tx). Le format de cette entrée est le suivant :

```
fichier_d'entrée, fichier_de_sortie
```

ou

```
fichier_d'entrée
```

ou

```
fichier_de_sortie
```

Si vous sélectionnez File New ou File All et que le fichier est réduit, le fichier est lu depuis le début.

Pour plus d'informations sur la configuration des collecteurs avec ce type de connexion, reportez-vous à la documentation relative aux collecteurs (Solaris Syslog et Windows 2000 Event Log) à l'emplacement suivant :

```
%workbench_home%\elements\<nom du collecteur>\docs
```

Type de connexion Persistent Process (processus permanent)

La connexion de type Persistent Process lance un processus permanent au démarrage du port. Ce type de processus permet la communication entre le collecteur assigné à ce port et une application externe via des états de réception et de transmission.

Un processus permanent démarre dès la première lecture et/ou écriture et continue de s'exécuter tant que le port est actif. Il s'arrête en même temps que le port, en tant qu'élément intégré au processus d'arrêt du port. À l'arrêt du port, un événement de niveau 5 est envoyé. À son démarrage, un événement de niveau 1 est envoyé.

Pour plus d'informations, reportez-vous à la section Processus permanents et temporaires. Pour plus d'informations sur la configuration de l'option Rx/Tx Value (Valeur Rx/Tx) pour ce type de connexion, reportez-vous à la section Configuration de l'option Rx/Tx Value (Valeur Rx/Tx) pour une connexion permanente ou temporaire (de type Rx/Tx). Pour plus d'informations sur la configuration des collecteurs avec un type de connexion permanent, reportez-vous à la documentation consacrée aux collecteurs (Check Point Firewall et Check Point VPN) à l'emplacement suivant :

```
%workbench_home%\elements\<nom du collecteur>\docs
```

Type de connexion Transient Process (processus temporaire)

La connexion de type Transient Process est utilisée pour lancer un processus temporaire au démarrage du port. Ce type de processus permet la communication entre le collecteur assigné à ce port et une application externe via des états de réception et de transmission.

Un processus temporaire peut être démarré à plusieurs reprises. Il s'arrête en même temps que le port, en tant qu'élément intégré au processus d'arrêt du port.

REMARQUE : Si vous sélectionnez Persistent Process ou Transient Process, l'option Rx/Tx Value (Valeur Rx/Tx) doit être renseignée à l'aide du chemin et du nom de fichier du processus à exécuter. Vous pouvez utiliser un chemin d'accès et un nom de fichier complets ou relatifs (pointant vers %WORKBENCH_HOME%). Par exemple :

Chemin d'accès complet :

```
C:\Program Files\Cisco\Csids_client – start
```

Chemin d'accès relatif :

```
.\elements\Cisco\Csids_client – start
```

Les processus permanents utilisent d'office le chemin d'accès relatif, sauf si la zone Rx/Tx Value (Valeur Rx/Tx) a été renseignée à l'aide d'un chemin d'accès permanent.

Fin d'un processus temporaire : si le processus temporaire s'arrête avant l'arrêt de l'analyseur, il est redémarré lors du processus de lecture ou d'écriture suivant, sans qu'aucun message ne soit envoyé.

Pour plus d'informations, reportez-vous à la section Processus permanents et temporaires. Pour plus d'informations sur la configuration de l'option Rx/Tx Value (Valeur Rx/Tx) pour ce type de connexion, reportez-vous à la section Configuration de l'option Rx/Tx Value (Valeur Rx/Tx) pour une connexion permanente ou temporaire (de type Rx/Tx).

Type de connexion SNMP Trap (trappes SNMP)

La connexion de type SNMP Trap (trappes SNMP) sert à recevoir des trappes SNMP v1, v2 et v3. Ces trappes sont envoyées par les capteurs vers l'adresse IP du serveur Wizard. En fonction de l'adresse IP et de l'identificateur d'objet (OID) du périphérique expéditeur, le Gestionnaire des collecteurs active l'analyse sur le collecteur approprié. L'état de réception (analyse) transmet les données des trappes SNMP entrantes au collecteur.

Les informations utilisées pour récupérer et analyser les trappes SNMP v1 et v3 sont toutes configurables :

- Les trappes SNMP v1 sont identifiées à l'aide d'une adresse IP, d'un identificateur d'objet (OID) et d'un code de trappe.
- Les trappes SNMP v2 et v3 sont identifiées à l'aide d'une adresse IP, d'un nom de sécurité, d'un ID du moteur, de clés de chiffrement et d'authentification (si activées pour la trappe) ainsi que d'un identificateur d'objet (OID).

Il faut que le format de la trappe, en termes de valeurs de trappe, soit aussi proche que possible du format d'origine. Ce format est généralement défini dans la base MIB (management information base) pour le capteur qui a généré la trappe.

Pour plus d'informations, reportez-vous à la section Configuration de SNMP Trap (trappes SNMP).

Type de connexion None (aucun)

La connexion de type None (aucun) est utilisée sans port de communication. Elle est beaucoup plus efficace, car l'étape consistant à établir une connexion n'existe pas. Ce type de connexion est recommandé lorsqu'un collecteur ne se sert pas de l'état de réception et se contente de traiter des commandes.

Pour plus d'informations sur la configuration des collecteurs avec ce type de connexion, reportez-vous à la documentation relative aux collecteurs (collecteurs ISS RealSecure et ISS SiteProtector) à l'emplacement suivant :

```
%workbench_home%\elements\<nom du collecteur>\docs
```

Création, assignation, démarrage et arrêt d'un port Wizard

Pour créer un port Wizard

1. Pour plus d'informations sur la configuration d'un collecteur, reportez-vous à la documentation du collecteur concerné à l'emplacement suivant : %workbench_home%\elements\<nom du collecteur>\docs.
2. Cliquez sur l'onglet *Collecteurs* et sélectionnez un collecteur.
3. Dans le Générateur de collecteurs, cliquez sur l'onglet Wizard Hosts (Hôtes Wizard) et sélectionnez un hôte.
4. Dans le panneau Port Information (Informations de port), double-cliquez sur *Nouveau*, tapez le nom du port et appuyez sur Entrée.
5. Sélectionnez un type *Rx/Tx*.
6. Précisez les options de configuration en fonction du type de connexion sélectionné :
   - Connexions de type Serial et Socket : dans la zone d'édition Port Name (Nom du port), cliquez avec le bouton droit sur le nom du port et sélectionnez *Edit Rx/Tx Value (Éditer la valeur Rx/Tx).* Spécifiez l'un des ensembles d'options suivants :
     - Pour les connexions de type Serial : sélectionnez le débit en bauds, la taille des mots, la parité et les bits d'arrêt. Cliquez sur OK.
     - Pour les connexions de type Socket : entrez l'adresse IP et le numéro de port de la machine hôte, séparés par un deux-points. Si aucun état de réception n'est utilisé, définissez le type sur None (Aucun) et cliquez sur *OK*.
   - Pour tous les autres types de connexion : double-cliquez sur la cellule *Rx/Tx Value (Valeur Rx/Tx)*, entrez les informations appropriées et appuyez sur Entrée.
   - Pour les connexions de type SNMP Trap, reportez-vous à la section Configuration de SNMP Trap (trappes SNMP).
7. Double-cliquez sur la cellule Collecteur et sélectionnez un collecteur.
8. Cliquez avec le bouton droit sur *Port Name (Nom du port)* et sélectionnez *Other Port Options (Autres options de port).* La boîte de dialogue correspondante s'affiche.

9. Dans la boîte de dialogue *Other Port Options (Autres options de port)*, cochez ou décochez la case *Run Port at Startup (Exécuter le port au démarrage)*, sélectionnez une *séquence de démarrage* et cliquez sur *OK*.
10. Si vous créez un port pour l'hôte local, cliquez sur *Fichier,* sélectionnez *Enregistrer*, puis *Port* Information (Informations de port).

    Si vous créez un port pour un hôte distant, cliquez sur *Fichier* et sélectionnez *Upload/Download (Télécharger)*.

    Le port est ajouté au panneau Port Information (Informations de port). Il n'est pas nécessaire de redémarrer le système pour implémenter le nouveau port. Cliquez sur *Démarrer* pour faire passer l'état du nouveau port d'Inactif à Actif.

Processus permanents et temporaires

Grâce au processus permanent (Persistent Process) ou au processus temporaire (Transient Process), le composant Wizard peut être interfacé avec une autre application à l'aide de scripts qui reçoivent ou transmettent des données et analysent les réponses. Chacun de ces scripts s'exécute sur un port différent et chaque port est lui-même connecté à une application spécifique.

REMARQUE : l'application interfacée avec le composant Wizard doit être spécifiée dans la zone Rx/Tx Value (Valeur Rx/Tx).

Les noms des processus peuvent comprendre les éléments suivants :

- des espaces ;
- des barres obliques et des barres obliques inverses, pour convenir à différents systèmes d'exploitation ;
- des arguments de commande ;
- des chemins d'accès absolu et relatif (la variable d'environnement WORKBENCH_HOME est considérée comme étant le répertoire racine relatif).

Lorsqu'un état de réception/transmission (Rx/Tx) se produit, le processus indiqué dans la zone Rx/Tx Value (Valeur Rx/Tx) est lancé. Lorsque l'analyseur s'arrête, le processus prend fin.

Lorsqu'un processus permanent prend fin, un événement de niveau 5 est envoyé. Lorsqu'un processus permanent démarre, un événement de niveau 1 est envoyé.

La sortie standard (stdout) du processus permanent ou temporaire est connectée à l'état « lecture » de réception de l'analyseur. L'entrée standard (stdin) du processus permanent ou temporaire est connectée à l'état « écriture » de transmission de l'analyseur.

Configuration de l'option Rx/Tx Value (Valeur Rx/Tx) pour une connexion permanente ou temporaire (de type Rx/Tx)

Trois processus de connexion sont disponibles lors de la configuration de connexions permanentes et temporaires. Ces processus sont les suivants :

- DBConnector (connecteur de processus JDBC)
- Client LEA
- RDEP (Remote Data Exchange Protocol)

N'utilisez pas de guillemets dans la zone d'édition Rx/Tx Value (Valeur Rx/Tx) pour les processus permanent et temporaire. Si le processus correspond à un chemin d'accès absolu pointant vers un nom d'exécutable long et comprenant des espaces, entrez-le sans guillemets. Par exemple :

```
%WORKBENCH_HOME%\e-security\elements\checkpoint\lea_clien
   t checkpoint\lea_client.conf -new
```

Dans la zone d'édition Rx/Tx Value (Valeur Rx/Tx), n'utilisez pas d'espaces pour les arguments donnant accès à l'exécutable. Généralement, ces arguments contiennent des espaces si bien que le logiciel comprend qu'il existe deux arguments là où il n'y en a qu'un. Si ces arguments sont passés à l'emplacement d'un fichier de configuration, comme dans le cas du collecteur Check Point, utilisez un chemin d'accès relatif depuis %WORKBENCH_HOME%. Par exemple :

```
checkpoint/\lea_client checkpoint/\lea_client.conf -new
```

DBConnector

Le connecteur DBConnector (connecteur de processus JDBC) exécute un client qui se connecte à un serveur de base de données, lance une requête SQL sur cette base de données et renvoie le résultat vers une sortie standard sous forme de paire nom-valeur. La requête SQL à exécuter est lue dans une entrée standard ou un fichier. Le nom de la paire nom-valeur obtenue est extrait du nom de la colonne de l'ensemble des résultats. C'est pourquoi le nom de la colonne voulue doit être mentionné explicitement au format SQL. La syntaxe exacte varie selon le serveur de base de données utilisé.

L'application DBConnector s'installe à l'aide du Gestionnaire des collecteurs sous $WORKBENCH_HOME/dbconnector.

Pour plus d'informations sur l'utilisation du connecteur DBConnector, reportez-vous au fichier README fourni avec l'application, à la documentation du collecteur Sentinel pour Entercept Host IDS 4.0 (via JDBC) ou visitez le portail client d'e-Security à l'adresse http://www.esecurityinc.com.

Client LEA

Le client LEA (Log Export API) de Sentinel utilise l'API d'exportation de fichiers journaux d'OPSEC pour importer des données de Check Point Firewall-1 et les émettre sous forme de nom paire-valeur. Ce client LEA est généralement utilisé pour fournir des données au collecteur Check Point Firewall-1 de Sentinel. Au sein de ce collecteur, les données sont normalisées, puis, selon l'action impliquée par l'événement (abandon, rejet ou acceptation), une alerte est transmise au serveur Sentinel.

L'application LEA s'installe à l'aide du Gestionnaire des collecteurs sous $WORKBENCH_HOME/checkpoint.

Pour plus d'informations sur l'utilisation du client LEA de Check Point, reportez-vous au fichier README fourni avec l'application, à la documentation du collecteur Sentinel pour Check Point Firewall et VPN (via OPSEC) ou visitez le portail client d'e-Security à l'adresse http://www.esecurityinc.com.

RDEP (Remote Data Exchange Protocol)

Le client RDEP (Remote Data Exchange Protocol) est une application Java qui importe des données depuis des capteurs distants Cisco IDS v4.0 exécutant le protocole RDEP. Ce client se connecte à un capteur distant IDS à l'aide d'une connexion HTTP ou HTTPS. Une fois connecté, il ouvre un abonnement ou en utilise un déjà ouvert. L'abonnement décrit le type de données que le capteur IDS envoie au client. Le type de données que l'abonnement importe peut être modifié dans le fichier de configuration rdep_client. Grâce à cet abonnement, le client lance une requête sur des données d'événement à partir du capteur IDS. Les données sont ensuite renvoyées par le capteur IDS au format XML, converties au format nom paire-valeur par le client RDEP de Sentinel, puis analysées et normalisées par le collecteur. Enfin, le collecteur envoie les événements normalisés à Sentinel.

L'application RDEP s'installe à l'aide du Gestionnaire des collecteurs sous $WORKBENCH_HOME/cisco/rdep_client.

Pour plus d'informations sur l'utilisation de l'application RDEP, reportez-vous au fichier README fourni avec l'application, à la documentation du collecteur Sentinel pour Cisco IDS 4.0 (via RDEP) ou visitez le portail client d'e-Security à l'adresse http://www.esecurityinc.com.

Configuration de SNMP Trap (trappes SNMP)

Sentinel est capable de recevoir des trappes SNMP représentant des événements de sécurité détectés par un capteur installé sur le réseau. Ces événements sont envoyés vers Sentinel par l'intermédiaire d'un réseau utilisant le protocole SNMP. Les trappes SNMP de type v1, v2 et v3 sont prises en charge. Pour permettre à Sentinel de recevoir des trappes SNMP, un collecteur Wizard doit être créé et configuré de façon à utiliser une connexion SNMP Trap de type Rx/Tx.

Définissez les paramètres de configuration de la connexion SNMP Trap appropriés pour que les collecteurs SNMP Wizard puissent transmettre des trappes à Sentinel sous forme d'événements binaires.

Pour cela, servez-vous de la fenêtre de configuration SNMP Trap et indiquez-y le port à utiliser pour les trappes SNMP, les codes des trappes, les informations d'authentification et celles de chiffrement.

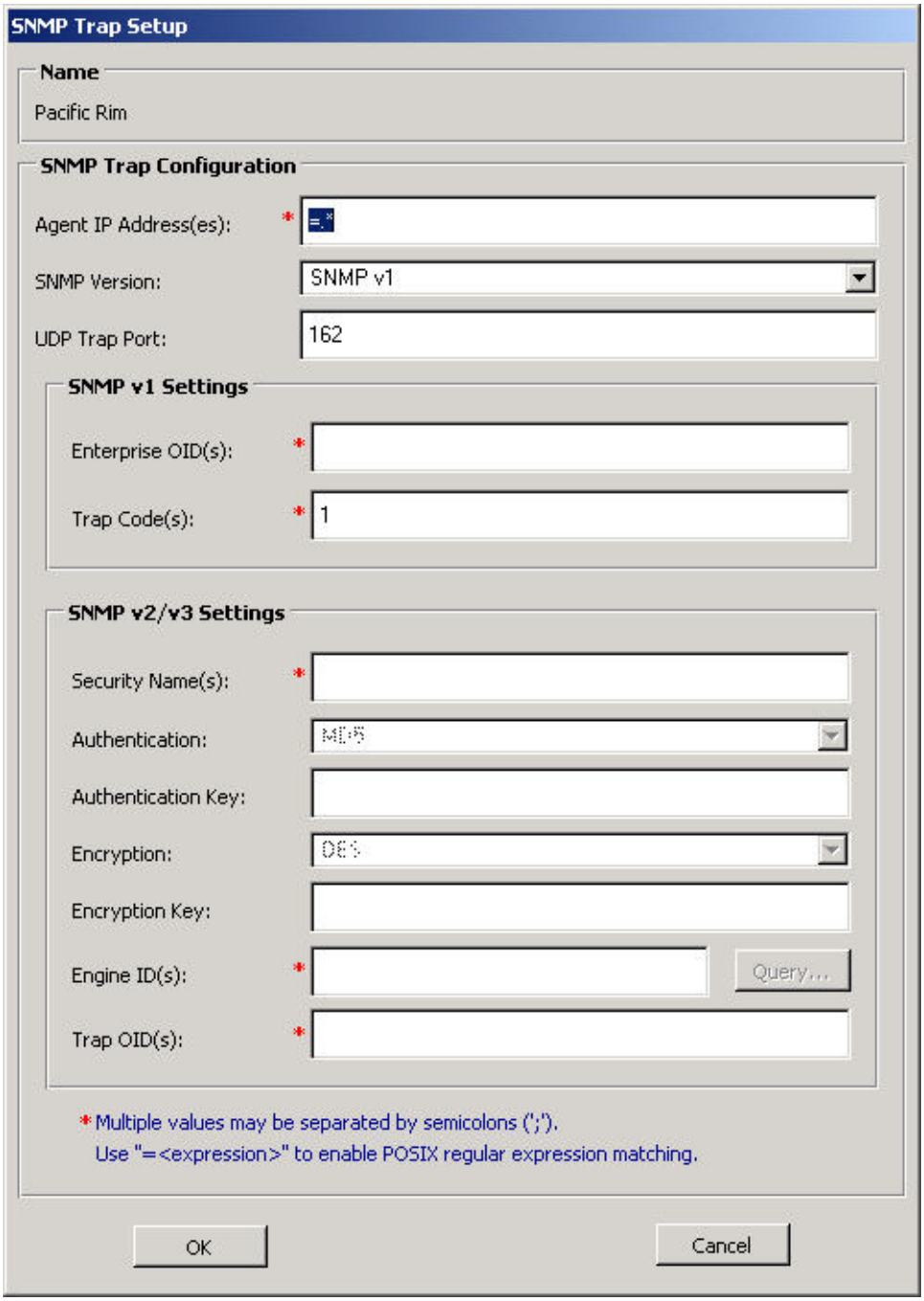
Pour accéder à la fenêtre SNMP Trap

1. Dans le Générateur de collecteurs, assignez un nom de port au collecteur SNMP.
2. Définissez le type Rx/Tx sur SNMP Trap.
3. Cliquez avec le bouton droit sur le nom du port et sélectionnez *Edit Rx/Tx Value (Éditer la valeur Rx/Tx)*.
4. Entrez les informations SNMP.

   REMARQUE : le numéro du port de trappes UDP par défaut est le 162. Assurez-vous qu'il est disponible. Si tel n'est pas le cas, sélectionnez un autre numéro de port.

   REMARQUE : Contrairement aux autres ports du collecteur, le champ Rx/Tx Value (Valeur Rx/Tx) est renseigné d'après les paramètres que vous avez définis dans la fenêtre de configuration de SNMP Trap. Dans le cas d'un collecteur SNMP, il est impossible de modifier manuellement le contenu du champ Rx/Tx Value (Valeur Rx/Tx).
5. Enregistrez et téléchargez le collecteur SNMP.
6. Activez ce collecteur en arrêtant, puis en redémarrant votre Gestionnaire des collecteurs.

   REMARQUE : pour activer ce collecteur, vous devez arrêter et redémarrer votre Gestionnaire des collecteurs comme indiqué à l'étape 6.



La configuration SNMP comprend la définition des éléments suivants :

- Adresse(s) IP du collecteur
- Version du protocole SNMP
- Port de trappes UDP
- Paramètres SNMP v1
  - Enterprise OID(s) (OID d'entreprise)
  - Trap Code(s) (Code(s) de trappe)

- Paramètres SNMP v2/v3
  - Security Name(s) (Nom(s) de sécurité)
  - Authentification
  - Authentication Key (Clé d'authentification)
  - Encryption (Chiffrement)
  - Encryption Key (Clé de chiffrement)
  - Engine ID(s) (ID de moteur) avec bouton Requête
  - Trap OID(s) (OID de trappe)

Dans la boîte de dialogue de configuration de SNMP Trap, que vous ouvrez en cliquant avec le bouton droit sur un port dans le panneau des informations de port du Générateur de collecteurs et en sélectionnant Edit Rx/Tx Value (Éditer la valeur Rx/Tx), vous pouvez configurer le composant Wizard pour :

- recevoir des trappes sur des ports autres que le port UDP 162 (port par défaut) ;
- créer un seul script d'analyse Wizard pour traiter les trappes à partir de plusieurs adresses IP à l'aide d'informations telles que des codes et des identificateurs d'objet (OID) de trappe ;
- autoriser les correspondances d'expressions régulières POSIX (Portable Operating System Interface for UNIX) pour les champs d'adresse IP, d'identificateur d'objet (OID) d'entreprise, de codes de trappe et d'identificateurs d'objet de trappe ;
- définir, après décodage des trappes, les valeurs des variables intégrées au script.

Adresse(s) IP du collecteur

La ou les adresses IP du collecteur sont celles sur lesquelles vous souhaitez recevoir les trappes. Séparez les différentes valeurs par des points-virgules (;). Vous pouvez utiliser le format =<expression> pour la correspondance des expressions régulières compatibles avec l'interface POSIX. L'astérisque (*) constitue un modificateur du caractère ou de l'expression qui le précède tandis que le point (.) peut s'utiliser en tant que caractère générique et peut apparaître à n'importe quel endroit de la chaîne si vous utilisez des expressions régulières.

Les expressions régulières les plus courantes sont les suivantes :

=	Correspond à n'importe quelle séquence de caractères de n'importe quelle longueur.
= 192\.168.*	Correspond à n'importe quelle séquence de caractères contenant 192.168. Pour obtenir une correspondance de type « commence par », utilisez la syntaxe suivante : ^192.168... où ^ correspond au marqueur de début de ligne. Pour obtenir une correspondance de type « se termine par », utilisez la syntaxe suivante : 0.47$... où $ correspond au marqueur de fin de ligne.
= [abc]	Correspond à « a » ou « b » ou « c ».
= [a-zA-Z0-9]	Correspond à n'importe quel caractère de l'alphabet (majuscule ou minuscule) ou à n'importe quel chiffre de 0 à 9.

En résumé, les règles appliquées dans les exemples d'expressions régulières précédents sont les suivantes :

. Correspond à n'importe quel caractère.

* Correspond à 0 ou plusieurs occurrences du modèle d'expression précédent ce signe.

[] Correspond à n'importe quel caractère du modèle défini entre crochets.

REMARQUE : Ces règles peuvent être utilisées de manière combinée.

Version SNMP

Une seule version du protocole SNMP peut être configurée. Les options du panneau des paramètres SNMP v1 et de celui des paramètres SNMP v2/v3 sont activées en fonction de la version sélectionnée.

Port de trappes UDP

Le port UDP de destination par défaut et le port 162.

Paramètres SNMP v1

Ces paramètres ne sont disponibles que si vous sélectionnez SNMP v1 dans la liste des versions de protocole SNMP.

- Enterprise OID(s) (OID d'entreprise) : identificateur(s) d'objet permettant de déterminer le type de collecteur qui a envoyé la trappe. Séparez les différentes valeurs par des points-virgules (;).
- Trap Code(s) (Code(s) de trappe) : codes de trappe pour les capteurs qui envoient les trappes SNMP. Ces codes de trappe indiquent le type des trappes envoyées par le collecteur SNMP. Séparez les différentes valeurs par des points-virgules (;).

Paramètres SNMP v2/v3

- Security Name(s) (Nom(s) de sécurité) : nom d'utilisateur permettant d'accéder au collecteur. Une distinction entre les majuscules et les minuscules est opérée pour les noms de sécurité. Séparez les différentes valeurs par des points-virgules (;).
- Authentification : méthode d'authentification. Les valeurs possibles sont les suivantes :
  - Aucun : aucun processus d'authentification n'est appliqué pour les trappes SNMP v3.
  - MD5 : le nom de sécurité est configuré de façon à utiliser l'algorithme MD5 pour créer une signature d'authentification numérique.
- Authentication Key (Clé d'authentification) : mot de passe utilisé pour authentifier l'utilisateur du collecteur. Option activée uniquement si la méthode d'authentification est MD5. Doit comporter au moins 8 caractères. Une distinction entre les majuscules et les minuscules est opérée. Une clé identique à celle-ci doit être configurée sur le collecteur SNMP d'envoi.
- Encryption (Chiffrement) : méthode de chiffrement. Les valeurs possibles sont les suivantes :
  - Aucun : aucun processus de chiffrement n'est appliqué pour les trappes SNMP v3.
  - DES : réception de trappes chiffrées à l'aide de la méthode DES (Data Encryption Standard).

- Encryption Key (Clé de chiffrement) : clé utilisée pour déchiffrer les trappes envoyées aux collecteurs Wizard. Doit comporter au moins 8 caractères. Une distinction entre les majuscules et les minuscules est opérée. Option activée uniquement si DES est sélectionné dans la liste Encryption (Chiffrement).
- Engine ID(s) (ID de moteur) : identificateur unique destiné à un collecteur SNMP v3. Un bouton de requête des ID de moteur permet de rechercher l'adresse IP sur laquelle vous souhaitez lancer une requête. Une requête fructueuse renvoie les informations et ajoute l'ID du moteur trouvé. Si un ID de moteur est déjà affiché dans la zone correspondante, l'ID de moteur trouvé est ajouté à la suite.
- Trap OID(s) (OID de trappe) : identificateur d'objet de trappe indiquant le type de la trappe reçue.

REMARQUE : Si vous spécifiez plusieurs noms de sécurité et plusieurs ID de moteur, la même méthode d'authentification et de chiffrement est appliquée à tous les noms et tous les ID.

REMARQUE : Si des clés d'authentification et de chiffrement différentes sont requises selon les collecteurs SNMP, vous devez configurer un port par collecteur.

Variables de trappes SNMP

Certaines variables de trappes sont valables pour tous les types de trappe (SNMP v1 et v3), tandis que d'autres ne sont valables que pour une seule version du protocole SNMP. Les tableaux suivants répertorient toutes les variables de trappes SNMP par version ou groupe de versions SNMP :

- Variables de trappes SNMP v1 et v3
- Variables de trappes SNMP v1
- Variables de trappes SNMP v3

Variables de trappes SNMP v1 et v3

Variable	Description
`s_Trap_IP`	Adresse IP du collecteur/capteur qui a envoyé la trappe.
`s_Trap_Time`	Temps de fonctionnement relevé par le collecteur/capteur qui a envoyé la trappe. En général, il s'agit de la valeur correspondant au temps pendant lequel le collecteur était actif. Format : J:HH:MM:SS.ss (jours, heures, minutes, secondes, centièmes de seconde).
`i_Trap_Version`	Valeur correspondant à une version SNMP particulière : 1 = SNMP v1 3 = SNMP v3
`i_Trap_Vars`	Nombre de variables liées dans la trappe.
`s_Trap_OID[]`	Tableau (de la taille spécifiée par la variable « i_Trap_Vars ») des noms des variables MIB liées dans le message de trappe. Chaque élément du tableau de variables s_Trap_OID est un OID tel que « .1.3.6.1.4.1.4286.... ».
`s_Trap_Value[]`	Tableau (de la taille spécifiée par la variable « i_Trap_Vars ») des valeurs des variables MIB liées dans le message de trappe. Les indices de ce tableau et ceux du tableau des variables s_Trap_OID correspondent de telle sorte que s_Trap_OID[0] est le nom de la variable et que s_Trap_Value[0] est sa valeur.

Variables de trappes SNMP v1

Variable	Description
s_Trap_Ent	Identificateur d'objet d'entreprise (OID) du collecteur/capteur qui a envoyé la trappe.
s_Trap_Code_Generic	Code générique de la trappe. Les valeurs possibles sont les suivantes : 1-5 = types de trappe standard définis par l'IETF (Internet Engineering Task Force) 6 = trappe spécifique à l'entreprise (son code est défini par la variable s_Trap_Code_Specific)
s_Trap_Code_Specific	Code de trappe spécifique. À spécifier uniquement si s_Trap_Code_Generic = 6.

Variables de trappes SNMP v3

Variable	Description
s_Trap_Engine_ID	ID de moteur du collecteur SNMP v3 qui a envoyé la trappe.
s_Trap_OID	Identificateur d'objet (OID) indiquant le type de trappe SNMP v3 reçue. Pour des raisons d'identification des trappes, l'OID de trappe SNMP v3 prend la place de l'OID d'entreprise SNMP v1 ainsi que celle du code de trappe générique ou spécifique.
s_Trap_Security_Name	Nom de sécurité sous lequel apparaît le collecteur SNMP v3 qui a envoyé la trappe.

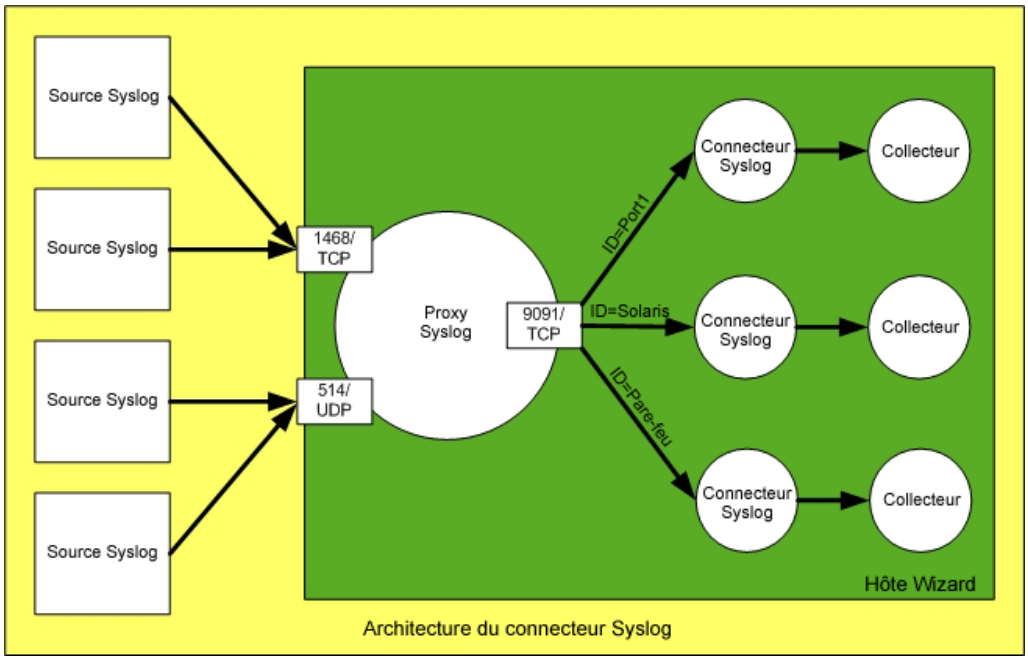
A Connecteur Syslog v1.0.2

REMARQUE : les termes Agent et Collecteur sont interchangeables. Le terme Collecteur sera utilisé dans la suite de cette documentation.

Novell a commercialisé ce connecteur Syslog afin de permettre une intégration sans soucis entre les collecteurs Sentinel et les produits capables de générer des messages Syslog. Ce document vise à expliquer l'architecture, l'installation, l'utilisation et les options du connecteur Syslog.

Architecture

Le connecteur Syslog se compose de deux éléments. L'un de ces éléments est le proxy Syslog et l'autre, le client du connecteur Syslog. Le proxy Syslog écoute les ports UDP et TCP sélectionnés. Le port UDP par défaut est le 514. Le port TCP par défaut est le 1468, port généralement utilisé par Cisco PIX pour l'envoi de messages Syslog à l'aide du protocole TCP.



Architecture du connecteur Syslog

Vous trouverez ci-dessous une description des fonctions de chacun des composants du connecteur Syslog :

- Proxy Syslog
  - Écoute un port TCP et/ou UDP pour détecter les messages Syslog.
  - Analyse les messages entrants pour y rechercher des composants de message Syslog standard (priorité, date, nom de l'hôte et message).
  - Lorsqu'un message envoyé ne comporte pas de priorité, de date ou de nom d'hôte, la norme RFC 3164 intitulée « BSD Syslog Protocol » est suivie et les données manquantes sont insérées.
  - Une fois les champs Facility (Type) et Level (Niveau) déterminés à partir des éléments Priority (Priorité) et Hostname (Nom de l'hôte), le proxy transmet les messages aux sessions du connecteur Syslog concernées par ce message.
  - Lorsque la session cliente du connecteur Syslog prend fin, le proxy Syslog place les messages dans une file d'attente entrante de ce client pendant 10 minutes. Cela doit garantir que le collecteur ne rate aucun message pendant son redémarrage ou une interruption temporaire de son exécution.
  - Le proxy Syslog écoute sur un port TCP (en général, le port 9091) afin de desservir les sessions clientes du connecteur Syslog.
- Client du connecteur Syslog
  - Le connecteur est démarré en tant que processus permanent (Persistent Process), toutes les options d'exécution du connecteur étant entrées dans la zone Rx/Tx Value (Valeur Rx/Tx).
  - L'un des paramètres d'exécution est l'ID. L'ID configuré pour un connecteur Syslog particulier doit être unique entre les ID des connecteurs Syslog connectés au même proxy Syslog.
  - Un filtre de contenu peut être spécifié pendant l'exécution afin de limiter l'étendue des messages soumis au collecteur pour analyse.
  - Le connecteur Syslog établit une connexion au service délivré par le client du connecteur du proxy.
  - Le connecteur Syslog enregistre son ID et ses filtres de contenu auprès du proxy Syslog.
  - Les messages que le proxy Syslog associe à l'ID enregistré sont lus par le connecteur Syslog et dirigés vers la sortie standard correspondante.
  - Pour le moment, la structure et le contenu des messages sont transmis au collecteur tels quels. À l'avenir, le connecteur Syslog sera capable de mettre le message au format approprié de façon à répondre aux exigences d'analyse du collecteur.

Le protocole Syslog a toujours reposé sur le protocole UDP jusqu'à aujourd'hui. En l'absence d'une diversité et d'un nombre suffisants d'applications et de périphériques capables de transmettre des messages par TCP ou par un protocole Syslog standard reconnu fonctionnant avec TCP, la méthode de clôture de message finalement adoptée est celle de Cisco PIX (retour chariot et saut de ligne). La clôture de message est nécessaire lorsque Syslog fonctionne avec le protocole TCP, car il n'existe aucune ligne de démarcation entre les messages, qu'elle soit naturelle ou normalisée. Pour le protocole UDP, Syslog dispose d'une méthode de clôture de message naturelle puisqu'un paquet UDP ne transporte qu'un seul message et que le protocole UDP ne nécessite pas de connexion.

Installation et désinstallation

Le connecteur Syslog a été conçu de manière à fonctionner sur n'importe quelle plate-forme Wizard. Pour répondre à ces exigences de compatibilité, les deux composants Syslog sont écrits en Java. Les configurations logicielles et matérielles requises sont répertoriées ci-après.

Configuration système requise

Logiciel

- Java 1.4.1 ou version ultérieure
- Wizard 4.2 ou version ultérieure
- Windows (2000/XP/2003), Solaris (8/9), RedHat Enterprise Linux (v3 ES/AS)

Matériel

- 14 Mo de RAM supplémentaires (45 Mo de mémoire virtuelle) pour chaque instance du connecteur Syslog et du proxy

Installation

Les fichiers du proxy Syslog ainsi que du client du connecteur sont automatiquement installés en même temps que le service du collecteur. Les fichiers Syslog se trouvent dans le répertoire suivant :

Sous UNIX :

```
$ESEC_HOME/wizard/syslog
```

Sous Windows :

```
%ESEC_HOME%\wizard\syslog
```

Le composant Wizard ne démarre pas le proxy Syslog automatiquement. Si vous souhaitez que le proxy Syslog démarre automatiquement, vous devez l'installer en tant que service. Pour cela, suivez les instructions suivantes :

Pour installer le proxy en tant que service Windows (sous Windows)

REMARQUE : le proxy Syslog peut être installé en tant que service Windows afin de pouvoir être exécuté automatiquement. Pour installer le proxy Syslog en tant que service, exécutez les commandes suivantes lorsque vous y êtes invité :

1. cd /d “%ESEC_HOME%\wizard\syslog”
2. syslog-server.bat install

   Cette opération entraîne la création d'un service Windows intitulé « eSecurity Syslog Server ».

Pour installer le proxy en tant que service (sous UNIX)

REMARQUE : le proxy Syslog peut être installé en tant que service sous UNIX afin de pouvoir être exécuté automatiquement au démarrage de la machine qui l'héberge. Pour installer le proxy Syslog en tant que service, exécutez les commandes suivantes :

1. Connectez-vous en tant qu'utilisateur root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh install

   Ainsi, le proxy Syslog est exécuté automatiquement au démarrage de la machine qui l'héberge. Par défaut, le proxy Syslog s'exécute sous une session d'utilisateur root. Cette condition est nécessaire, car, par défaut, le proxy Syslog établit une liaison au port 514, port qui requiert des droits d'utilisateur root. Pour que le proxy Syslog s'exécute sous une session autre qu'une session d'utilisateur root, modifiez le script /etc/init.d/esyslogserver. Vous devez vous assurer que l'utilisateur concerné dispose des autorisations nécessaires pour établir une liaison avec le port sur lequel il compte exécuter un processus d'écoute. Voici deux exemples de procédure :

   - Utilisez la commande « sudo » pour démarrer le proxy Syslog et accordez à l'utilisateur concerné les autorisations « sudo » nécessaires pour établir une liaison avec le port souhaité.
   - Modifiez la configuration Syslog (syslog.conf) et effectuez les opérations nécessaires pour que le proxy Syslog soit lié à un port qui ne requiert pas de droits d'utilisateur root (ex. : le port 1024). Dans ce cas, il vous faudra probablement rediriger les messages envoyés au port 514 vers le nouveau port que vous avez sélectionné.

Désinstallation

Pour désinstaller le service Windows, exécutez les commandes suivantes lorsque vous y êtes invité :

Pour désinstaller le proxy en tant que service Windows (sous Windows)

1. cd /d "%ESEC_HOME%\wizard\syslog"
2. syslog-server.bat remove

Pour désinstaller le proxy en tant que service (sous UNIX)

Pour désinstaller le proxy Syslog en tant que service, exécutez les commandes suivantes :

1. Connectez-vous en tant qu'utilisateur root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

Utilisation

Serveur proxy Syslog

Le composant Wizard ne démarre pas le serveur proxy Syslog automatiquement. Si vous souhaitez que le proxy Syslog démarre automatiquement, vous devez l'installer en tant que service. Pour cela, suivez les instructions décrites à la section Installation.

La configuration du proxy Syslog est stockée dans le fichier suivant :

Sous UNIX :

```
$ESEC_HOME/wizard/syslog/config/syslog.conf
```

Sous Windows :

```
%ESEC_HOME%\wizard\syslog\config\syslog.conf
```

Par défaut, le proxy Syslog utilise la configuration suivante :

- port d'écoute UDP pour les messages Syslog : 514 ;
- port d'écoute TCP pour les messages Syslog : 1468 ;
- port d'écoute TCP pour les connexions provenant de connecteurs : 9091.

Le proxy Syslog peut être configuré pour écouter sur d'autres ports lors de la réception de messages Syslog ou lors de l'acceptation de connexions clientes.
Commutateurs correspondants :

-udp <port>	Port d'écoute pour les messages UDP provenant de périphériques. Valeur par défaut : 514.
-tcp <port>	Port d'écoute pour les connexions TCP provenant de périphériques. Valeur par défaut : 1468.
-connector <port>	Port d'écoute pour les connexions TCP provenant des connecteurs. Valeur par défaut : 9091.

Pour modifier ces paramètres, accédez à la section suivante du fichier syslog.conf :

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=1468
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
```

Si vous voulez changer les paramètres de port comme suit :

- port d'écoute UDP pour les messages Syslog : 4514 ;
- port d'écoute TCP pour les messages Syslog : 4168 ;
- port d'écoute TCP pour les connexions provenant de connecteurs : 4991,

la section du fichier syslog.conf mentionnée ci-avant doit être modifiée comme suit :

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=4168
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=4514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=4991
```

Par défaut, la configuration du proxy Syslog est définie de manière à accepter les connexions clientes provenant de n'importe quel hôte. Pour renforcer la sécurité de votre système, vous pouvez configurer le proxy Syslog de sorte qu'il accepte uniquement les connexions clientes provenant d'un même hôte. Il s'agit d'une simple mesure de sécurité. En effet, aucun système de respect de la vie privée, de contrôle d'accès ou d'authentification n'existe entre les connecteurs du client et le proxy. Les commutateurs suivants résolvent ce problème :

`-private`	Écoute les connexions provenant de connecteurs sur une boucle.
-shared	Écoute les connexions des connecteurs à l'hôte local (commutateur par défaut).

Le commutateur « –shared » ordonne au proxy d'établir une liaison entre le port d'écoute de la connexion cliente et un socket accessible aux hôtes distants.

Pour modifier ces paramètres, accédez à la section suivante du fichier syslog.conf :

```
wrapper.app.parameter.2=-shared
```

Si vous souhaitez autoriser uniquement des connexions clientes provenant d'un même hôte, vous devez changer le paramètre comme suit :

```
wrapper.app.parameter.2=-private
```

Le proxy Syslog peut être configuré pour enregistrer tous les messages reçus dans un fichier journal. Le format de ces messages est celui que le proxy Syslog utiliserait s'il devait transmettre les messages à un autre serveur Syslog. Par conséquent, la priorité (<PRI>) utilisée par le serveur Syslog de réception pour évaluer les champs Facility (Type) et Level (Niveau) des messages est intégrée à tous les débuts de message. Ce type de connexion est possible grâce au commutateur suivant :

`-log <nom de fichier>`	Nom du fichier journal auquel le message doit être ajouté.

Pour permettre ce type de connexion, ajoutez les deux lignes ci-dessous au fichier syslog.conf, après le dernier paramètre « wrapper.app.parameter » :

```
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=<nom de fichier>
```

Par exemple, pour autoriser ce type de connexion au fichier $ESEC_HOME/wizard/syslog/messages.log, vous devez remplacer les paramètres par les valeurs ci-après :

```
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
wrapper.app.parameter.9=-messageSize
wrapper.app.parameter.10=5000
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=messages.log
```

Si aucun chemin d'accès absolu n'est spécifié pour le fichier, le chemin d'accès pris en compte est le chemin d'accès relatif au répertoire $ESEC_HOME/wizard/syslog.

REMARQUE : le fichier journal pourrait devenir relativement volumineux. Par conséquent, assurez-vous que l'emplacement où ces fichiers doivent être écrits dispose d'un espace suffisant (ex. : un répertoire autre que le répertoire $ESEC_HOME).

Il est recommandé de disposer d'un minimum de 64 Mo et d'un maximum de 256 Mo pour la taille du segment de mémoire JVM pour exécuter le proxy Syslog. Avec cette configuration, vous devez obtenir les performances suivantes :

Limites du serveur proxy :

▪ Nombre maximal d'événements	500 événements par seconde (total de tous les ports du client)
▪ Taille maximale de la file d'attente du connecteur	5 000 messages (valeur par défaut si aucune valeur n'est spécifiée)
▪ Nombre maximal de connecteurs	5

Pour changer les paramètres de mémoire, modifiez la section suivante du fichier syslog.conf :

```
# Initial Java Heap Size (in MB)
wrapper.java.initmemory=64

# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=256
```

Client du connecteur Syslog

Le client du connecteur Syslog se connecte au proxy Syslog pour récupérer les messages auxquels il s'est abonné. Les messages collectés par le client sont ensuite transmis à une sortie standard. La session cliente ouverte sur le serveur ne se termine pas tant que le processus client ou celui du proxy Syslog n'a pas pris fin. Ce type de fonctionnement avec transmission vers une sortie standard permet au moteur du collecteur d'utiliser ce connecteur en mode processus permanent (Persistent Process).

Dans la fenêtre de configuration de port du Générateur de collecteurs, définissez, pour le port, un processus permanent de type Rx/Tx ainsi qu'une valeur Rx/Tx (Rx/Tx Value) similaire à la syntaxe générique décrite ci-après.

Sous UNIX :

```
syslog/SyslogConnectorAgent.sh <arguments>
```

Sous Windows :

```
syslog\SyslogConnectorAgent.bat <arguments>
```

Après avoir défini la zone Rx/Tx Value (Valeur Rx/Tx), sélectionnez le collecteur approprié dans la bibliothèque, puis téléchargez la configuration du port et, si possible, le collecteur, sur l'hôte Wizard distant.

Le client du connecteur Syslog est conçu pour utiliser un certain nombre d'arguments par défaut afin de simplifier son utilisation. La ligne de commande la plus simple pour ce client doit donc être la suivante :

Sous UNIX :

```
syslog/SyslogConnectorAgent.sh –id "MyUniqueID"
```

Sous Windows :

```
syslog\SyslogConnectorAgent.bat –id "MyUniqueID"
```

L'interprétation de cette ligne de commande est la suivante :

- connexion au proxy Syslog en processus d'écoute pour cette connexion sur le port 127.0.0.1:9091 ;
- abonnement à tous les messages envoyés contenant tous les champs Facility (Type) Syslog possibles ;
- abonnement à tous les messages envoyés avec tous les champs Level (Niveau) Syslog possibles ;
- abonnement à tous les messages, quelle que soit l'adresse IP source contenue dans l'en-tête IP ;
- abonnement à tous les messages, quelle que soit la désignation de l'hôte dans le message ;
- assignation de l'ID « MyUniqueID » aux paramètres d'abonnement de cette session.

La session cliente du connecteur Syslog est enregistrée auprès du proxy Syslog avec le filtre d'abonnement décrit plus haut sous l'ID « MyUniqueID ». Cet ID est requis. L'ID a été choisi arbitrairement mais doit être unique parmi tous les ID de sessions clientes du connecteur Syslog connectées au même proxy Syslog. Si le même ID est assigné à deux clients de connecteur Syslog différents, l'une des deux connexions est abandonnée. Des deux sessions ouvertes sous le même ID, seule la dernière à s'être ouverte subsiste.

Le filtre générique du filtre précédent peut entraîner des efforts de traitement inutiles de la part du collecteur si les messages qui répondent aux critères du filtre et qui sont tous des messages reçus, ne sont pas pertinents par rapport aux opérations effectuées par le collecteur concerné. Dans l'exemple mentionné plus haut, il est évident que l'expression de filtre est très générale. L'exemple suivant, sous UNIX, propose une description plus restrictive, et donc plus précise, des messages effectivement pertinents par rapport au collecteur.

```
syslog/SyslogConnectorAgent.sh -facilities "user,kernel" -
   levels "warning,error" -sender
   "192.16.0.12,192.16.0.0/16" -host
   "17.16.8.0/24,10.1.1.13" -id "MyOtherUniqueID"
```

L'interprétation de cette ligne de commande est la suivante :

- connexion au proxy Syslog en processus d'écoute pour cette connexion sur le port 127.0.0.1:9091 ;
- (-facilities) abonnement à tous les messages envoyés dont l'option Facility (Type) est définie sur « user » (utilisateur) ou « kernel » (noyau) ;
- (-levels) abonnement à tous les messages envoyés dont l'option Level (Niveau) est définie sur « warning » (avertissement) ou « error » (erreur) ;
- (-sender) abonnement aux messages identifiés par l'adresse IP source des messages entrants dans le proxy Syslog. Cet argument entraîne la vérification par le proxy Syslog des informations de l'en-tête IP afin d'en évaluer les critères. Le filtre peut ainsi établir une correspondance avec les serveurs de relais Syslog, ces derniers n'étant pas identifiés dans les messages qu'ils transmettent. Bien que cet argument ait été spécialement conçu pour établir des correspondances dans des messages retransmis par le serveur de relais, il peut être utilisé pour filtrer des messages provenant directement d'une source Syslog. Les serveurs de relais ou les sources Syslog pertinentes sont, dans cet exemple, les suivantes : 192.16.0.12 et 192.16.0.0/16. Le second de ces éléments représente une plage d'adresses IP. Tant que l'adresse IP source est comprise entre l'adresse 192.16.0.0 et l'adresse 192.16.255.255, les messages correspondants passent le filtre. Les noms d'hôte ne sont pas valides pour cet argument car aucune résolution de nom d'hôte n'est effectuée sur les adresses IP source ;
- (-host) abonnement à des messages Syslog contenant des désignations d'hôte telles que 17.16.8.0/24 ou 10.1.1.13. Le premier élément est une plage d'adresses IP. Si le message contient une désignation d'hôte sous forme d'adresse IP et que cette dernière est comprise entre l'adresse 17.16.8.0 et l'adresse 17.16.8.255, le message rempli les conditions et passe le filtre. Les noms d'hôte sont pris en charge par l'argument –host. Ils peuvent être indiqués en toutes lettres ou sous forme d'expression régulière. Sachez qu'aucune résolution de nom d'hôte n'est effectuée pour cet argument. Il ne faut pas s'attendre à ce que la configuration d'une adresse IP ou d'un nom d'hôte permette au filtre d'établir une correspondance dans le schéma d'assignation des noms. Par exemple, si vous configurez l'argument tel que –host 172.16.0.90, le filtre n'établit pas de correspondance pour un message contenant le nom d'hôte « epsilon1 » (par exemple), même si les services de résolution de nom ont auparavant effectué une assignation entre 172.19.0.90 et « epsilon1 ». Par conséquent, une correspondance peut uniquement être établie entre une désignation IP d'hôte et des adresses IP ou, entre une désignation nominale d'hôte et des noms d'hôte.

Le filtre de l'exemple ci-dessus peut être décrit par l'expression booléenne suivante :

```
(Facility="user" ou Facility="kernel") et (Level="warning"
   ou Level="error") et (Sender="192.16.0.12" ou
   Sender=192.16.0.0/16") et (Host="17.16.8.0/24" ou
   Host="10.1.1.13")
```

Le nombre de combinaisons possibles pour ces arguments est le produit cartésien de types d'arguments, où chaque type d'argument correspond à un ensemble. D'après le site PRINCIPIA CYBERNETICA WEB (http://pespmc1.vub.ac.be/ASC/CARTES_PRODU.html), le produit cartésien se définit comme suit :

> « Arrangement de tous les N-uplets ordonnés pouvant être formés de telle sorte qu'ils contiennent un élément du premier ensemble, un élément du deuxième ensemble, etc. et un élément du N-ième ensemble. Cet arrangement peut être considéré comme un espace à N dimensions dans lequel chaque N-uplet désigne une case. Le produit cartésien le plus simple de deux ensembles est une table bidimensionnelle ou un tableau à double entrée dont les cases peuvent être utilisées pour entrer des fréquences, identifier des possibilités (voir Relation) ou des impossibilités (voir Contrainte) ou pour représenter sous forme graphique les transitions qui constituent le comportement d'un système. » (Krippendorff)
>
> **REMARQUE** : au moment de la publication de ce document, le site Web mentionné ci-dessus était disponible.

Cela implique qu'en théorie, beaucoup de messages distincts peuvent passer le filtre. Seule la pratique peut réellement déterminer le nombre de ces messages distincts.

Outre les arguments de ligne de commande de filtrage, il existe les arguments de ligne de commande facultatifs suivants :

`-proxy <adresse du serveur>:<n° de port>`	Adresse et numéro de port de connexion pour l'hôte qui héberge le proxy du serveur.
`-log <nom de fichier>`	Permet une connexion au fichier spécifié.

L'argument –proxy permet de configurer le client du connecteur afin qu'il se connecte soit à un port TCP autre que le port TCP par défaut, soit à un hôte autre que l'hôte local. Par défaut, le proxy Syslog attend la connexion d'un client du connecteur sur le port 9091. Lorsque le port 9091 n'est pas approprié pour l'hôte hébergeant le proxy Syslog, il peut être redéfini au démarrage du proxy et, au moyen de l'argument –proxy, les clients peuvent recevoir l'instruction de se connecter à un autre port. En outre, il est possible de définir l'hôte cible du client du connecteur comme hôte autre que l'hôte local. Lorsqu'un proxy Syslog accepte des sessions clientes de connecteurs distants, un client du connecteur Syslog peut être configuré de manière à établir une connexion avec ce proxy Syslog distant. L'adresse IP et le port client du connecteur pour le proxy Syslog doivent alors être configurés à l'aide de l'argument -proxy.

L'argument –log active la fonctionnalité de consignation du client du connecteur. Ce dernier écrit les messages au fur et à mesure qu'il les reçoit du proxy Syslog. Contrairement au fichier journal du proxy, le contenu du message est filtré en fonction des informations d'abonnement enregistrées et aucun message consigné ne contiendra le champ de priorité <PRI>. Le contenu correspondra donc à celui que le collecteur reçoit de ce même client de connecteur Syslog.

REMARQUE : le fichier journal pourrait devenir relativement volumineux. Par conséquent, assurez-vous que l'emplacement où ces fichiers doivent être écrits dispose d'un espace suffisant (ex. : un répertoire autre que le répertoire $ESEC_HOME).

Exemple d'utilisation des arguments –proxy et –log (UNIX) :

```
syslog/SyslogConnectorAgent.sh –proxy localhost:9091 –log
   connector_messages.log –id "MyUniqueID"
```

Configuration de la consignation pour le serveur proxy Syslog

Le serveur proxy Syslog écrit les messages de consignation dans le fichier suivant :

```
$ESEC_HOME/wizard/syslog/syslog_trace*.*.log
```

Les niveaux de consignation peuvent être changés en modifiant le fichier des propriétés de la consignation :

$ESEC_HOME/wizard/syslog/syslog_log.prop

Fichier des propriétés de consignation tel qu'indiqué dans le fichier syslog.conf :

wrapper.java.additional.1=-Djava.util.logging.config.file=syslog_log.prop

Pour adapter les niveaux de consignation, modifiez la section suivante :

```
###### Configure the logging levels
# Logging level rules are read from the top down. Start
   with the most general, then get more specific.
…
######
```

Exemples d'arguments de ligne de commande

Il est possible d'exécuter le serveur proxy Syslog et le connecteur client sans se servir des scripts fournis avec le produit. Pour cela, vous devez utiliser les arguments de ligne de commande décrit dans cette section.

Proxy Syslog :

```
java –server –Xms64m –Xmx256m –
   Djava.util.logging.config.file=syslog-logger.prop -jar
   syslog.jar [-udp <port>] [-tcp <port>] [-connector
   <port>] [-private|-shared] [-log <chemin du fichier>]
   [-messageSize <nombre>]
```

Arguments valides :

`–server`	À utiliser systématiquement. Utilisé par JVM.
`–Xms64m`	Cet argument indique la taille de la mémoire initiale pour le proxy Syslog. 64 Mo recommandés.
`–Xmx256m`	Cet argument indique la taille maximale de la mémoire pour le proxy Syslog. Valeur par défaut recommandée : 256 Mo. Il permet au serveur proxy de gérer les pics de volume au niveau des données, la multiplicité des connecteurs clients ainsi que les mémoires tampons lorsque les connecteurs se connectent à nouveau. Cette valeur peut être augmentée si la mémoire disponible, les volumes de données et le nombre de connecteurs clients qui se connectent le permettent. Elle ne doit pas dépasser les 1,2 Go par serveur proxy Syslog. Ex. : –Xmx1200m.
`–Djava.util. logging.config. file`	Cette propriété indique le nom du fichier ou le chemin d'accès au fichier de configuration de la consignation des débogages. Elle doit pointer vers l'emplacement de stockage du fichier. Si aucun chemin n'est spécifié, une recherche est lancée dans le répertoire actuel depuis l'emplacement d'exécution de JVM. Exemple : %workbench_home%\syslog-logger.prop
`-udp <port>`	Port d'écoute pour les messages UDP provenant de périphériques. Valeur par défaut : 514.
`-tcp <port>`	Port d'écoute pour les connexions TCP provenant de périphériques. Valeur par défaut : 1468.
`-connector <port>`	Port d'écoute pour les connexions TCP provenant des connecteurs. Valeur par défaut : 9091.
`-private`	Écoute les connexions provenant de connecteurs sur une boucle (valeur par défaut).
`-shared`	Écoute les connexions des connecteurs à l'hôte local (valeur par défaut). Si cet argument n'est pas défini, une erreur de communication est générée.
`-log`	Nom du fichier journal dans lequel écrire.
`-help`	Message d'aide.

-version	Version du proxy (0.91-poc).
-messageSize	Nombre de messages placés en mémoire tampon lors d'une interruption temporaire de connexion et qui doivent être renvoyés plus tard. Le nombre maximal de ces messages est 5 000. Ils doivent être répertoriés sans virgules entre eux. Si la valeur de cette option n'est pas précisée ou qu'elle dépasse 5 000, la commande est définie par défaut sur 5 000.

Client du connecteur Syslog :

```
java -jar syslogconnector.jar -id <UniqueId> [-proxy
   <hôte:numéro de port>] [-facilities <type1,type2,…>] [-
   levels <niveau1, niveau2,…>] [-sender <IP
   source1[/masque de sous-réseau entier], IP
   source2[/masque de sous-réseau entier],…>] [-host <
   IP1[/masque de sous-réseau entier]|Nom d'hôte1 | Regex
   de nom d'hôte1, IP2[/masque de sous-réseau entier]|Nom
   d'hôte2 | Regex de nom d'hôte2, …>] [-log <chemin
   d'accès au fichier journal>]
```

Arguments valides :

-proxy <hôte:numéro de port>	Port de l'hôte du proxy Syslog auquel se connecter. Valeur par défaut : 127.0.0.1:9091.
-facilities <type1,type2,…>	Liste des types souhaités séparés par des virgules. Valeur par défaut : tous les types.
-levels <niveau1, niveau2,…>	Liste des niveaux de gravité souhaités séparés par des virgules. Valeur par défaut : tous les niveaux.
-sender <IP source1[/masque de sous-réseau entier], IP source2[/masque de sous-réseau entier],…>	Liste des expéditeurs souhaités séparés par des virgules. Valeur par défaut : tous les expéditeurs.
-host < IP1[/masque de sous-réseau entier]|Nom d'hôte1 | Regex de nom d'hôte1, IP2[/masque de sous-réseau entier]…>	Liste des hôtes souhaités séparés par des virgules. Valeur par défaut : tous les hôtes.
-log <chemin d'accès au fichier journal>	Nom du fichier journal dans lequel écrire.
-id <UniqueId>	Identité du connecteur (OBLIGATOIRE).
-help	Message d'aide.
-version	Version du connecteur (0.91-poc).

Tableau des types (facility) pris en charge

Une distinction majuscule/minuscule est faite pour les noms de types (facility) pris en charge dans la ligne de commande du client du connecteur Syslog.

KERNEL	UUCP	LOCAL0
USER	CRON	LOCAL1
MAIL	SECURITY	LOCAL2
DAEMON	FTP DAEMON	LOCAL3
AUTH	NTP	LOCAL4
SYSLOG	LOG AUDIT	LOCAL5
LPR	LOG ALERT	LOCAL6
NEWS	CLOCK DAEMON	LOCAL7

Tableau des niveaux (level) pris en charge

Une distinction majuscule/minuscule est faite pour les noms des niveaux (level) pris en charge dans la ligne de commande du client du connecteur Syslog.

EMERGENCY	WARNING
ALERT	NOTICE
CRITICAL	INFORMATIONAL
ERROR	DEBUG

Remarques sur le déploiement

Messages à retransmettre au proxy Syslog

La plupart des serveurs Syslog sont capables de rediriger les messages Syslog qu'ils reçoivent vers un autre serveur Syslog, de même qu'ils peuvent traiter les messages entrants. Dans un scénario de déploiement, il est très tentant de modifier un hôte de consignation existant pour qu'il retransmette des messages au proxy Syslog. Cependant, ce choix de déploiement n'est pas si judicieux, compte tenu des comportements problématiques de certains serveurs Syslog.

Il a été constaté que les bibliothèques du serveur Syslog sous Solaris 7 et 9 et sous Linux 8 (versions représentatives d'autres versions) n'insèrent pas le nom de l'hôte ou l'adresse IP de l'hôte dans les messages qu'elles envoient de l'hôte. Le serveur Syslog de réception associe l'adresse IP source ou le nom de l'hôte (par le biais de la résolution de nom) aux messages reçus dans les fichiers journaux qu'il génère. Par exemple, lorsque Solaris 9 fait office de relais pour le proxy Syslog, il n'insère pas l'adresse IP ou le nom de l'hôte du message source dans les messages qu'il retransmet. Ce comportement n'est pas normal, car le fichier journal du système Solaris 9 contient une adresse IP et un nom d'hôte. Faute de nom d'hôte inséré dans le message, le proxy Syslog est obligé d'en déduire que le message provient du serveur de relais et non de l'hôte source effectif. Le proxy Syslog insère l'adresse IP de l'hôte relais dans chaque message reçu d'un relais Solaris 9. Les conséquences de cet état de faits ne sont pas anodines. En effet, l'origine d'un événement de sécurité n'est pas visible pour le collecteur et n'est donc pas visible non plus pour la solution Sentinel.

Il est par conséquent fortement recommandé de ne pas configurer le proxy comme destinataire des messages à retransmettre si ces derniers ne contiennent pas l'adresse IP et le nom d'hôte de la véritable source de l'événement. Cette recommandation entraîne un certain nombre d'implications logistiques importantes si le proxy doit être utilisé en environnement de production.

Exemple :

Imaginons qu'un événement « su » se produise sur l'hôte Lambda (172.16.0.70) où est exécuté Solaris 7. Lambda retransmet les messages Syslog à Delta (172.16.0.72) où est exécuté Solaris 9, qui, à son tour, sert de relais pour le proxy Syslog. Les messages suivants sont générés par le connecteur Sentinel.

Proxy :

```
<37>Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0 [« su root » s'est
   correctement exécuté pour oespadm sur /dev/pts/0]
```

Client du connecteur :

```
Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0 [« su root » s'est
   correctement exécuté pour oespadm sur /dev/pts/0]
```

Le suivi de paquet du même message arrivant d'abord sur Delta avant d'être retransmis au proxy Syslog sur pes020.esecurity.net se présente comme suit :

```
# snoop -x0 udp port 514
Using device /dev/dmfe0 (promiscuous mode) [Périphérique
   utilisé /dev/dmfe0 (mode espion)]
lambda -> delta    SYSLOG C port=42830 <37>Apr  1 18:54:11

0: 0000 83cd 1395 0040 2082 202b 0800 4500     .......@ .
   +..E.
16: 0061 fa09 4000 ff11 28d3 ac10 0046 ac10
   .aú.@...(....F..
32: 0048 a74e 0202 004d 5d7e 3c33 373e 4170
   .H.N...M]~<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    : 'su root'
   succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
```

```
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0

delta -> pes020.esecurity.net SYSLOG C port=38890 <37>Apr
   1 18:54:11

0: 000a 5e02 a335 0000 83cd 1395 0800 4500
   ..^..5........E.
16: 0061 304b 4000 ff11 f031 ac10 0048 ac10
   .a0K@....1...H..
32: 02a6 97ea 0202 004d 6a82 3c33 373e 4170
   .......Mj.<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    : 'su root'
   succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0
```

Le message suivant est enregistré pour l'hôte Delta :

```
Apr  1 18:54:11 lambda su: 'su root' succeeded for oespadm
   on /dev/pts/0 (« su root » s'est correctement exécuté
   pour oespadm sur /dev/pts/0)
```

B Configuration d'un serveur de socket sur l'hôte UNIX

REMARQUE: les termes Agent et Collecteur sont interchangeables. Le terme Collecteur sera utilisé dans la suite de cette documentation.

Un serveur de socket fournit un point limite aux connexions par socket du Gestionnaire des collecteurs Wizard sous UNIX. Par exemple, il peut être utile d'en configurer un si vous souhaitez vérifier un fichier journal ou une machine UNIX depuis un hôte Wizard distant et que vous avez besoin de traverser un pare-feu pour atteindre le port de la machine UNIX.

Les instructions suivantes vous permettent de configurer ce serveur de socket sur un hôte UNIX et de vérifier un fichier journal ASCII sur cet hôte.

Pour configurer un serveur de socket sur un hôte UNIX

1. Créez le script destiné à transmettre les données à la connexion par socket TCP. Pour cela, créez un nouveau fichier texte et copiez-y les lignes suivantes, en remplaçant la variable <fichier journal> par le chemin d'accès complet du fichier que vous souhaitez vérifier :

   ```
   #!/bin/sh
   /bin/tail -f <fichier journal>
   ```

   Enregistrez le fichier (le chemin d'accès et le nom du fichier sont choisis à titre d'exemple), sachant que ce dernier doit être conservé à un emplacement où il n'est pas susceptible d'être supprimé et qu'il doit porter un nom faisant référence à sa fonction. Exemple :

   ```
   /usr/local/bin/fichierjournalserveur
   ```

2. Pour le processus du serveur, sélectionnez un port TCP qui ne requiert pas d'autorisation particulière sur l'hôte UNIX. Le numéro de ce port sans autorisation est un numéro choisi arbitrairement entre les valeurs 1 025 et 65 535. Pour vérifier que ce numéro de port n'est pas déjà utilisé, servez-vous de la commande suivante (remplacez <numéro de port> par le port souhaité) :

   ```
   netstat -an | grep LISTEN | grep <numéro de port>
   ```

   Si une ligne semblable à la ligne ci-dessous est générée, cela signifie que le port est déjà utilisé et que vous devez en choisir un autre.

   ```
   *.5555*.*0000 LISTEN
   ```

3. Sous une session d'utilisateur root, modifiez le fichier /etc/services et ajoutez une entrée pour le nouveau service de socket à la fin du fichier. Dans l'exemple à suivre, une ligne est ajoutée pour un service intitulé « syslog_verif » et configuré pour lancer un processus d'écoute sur le port TCP 5555 :

   ```
   syslog_verif5555/tcp
   ```

4. Modifiez le fichier /etc/inetd.conf et ajoutez une entrée pour le nouveau service de socket à la fin du fichier. Dans l'exemple à suivre, une ligne est ajoutée pour un service intitulé « syslog_verif » et configuré pour exécuter le script /usr/local/bin/in.syslog_verif :

   Les éléments suivants doivent être entrés en tant que champs séparés par des tabulations sur une seule ligne du fichier, quelle que soit leur présentation dans le présent document :

   ```
   syslog_verif stream tcp nowait nobody
      /usr/local/bin/in.syslog_verif in.syslog_verif
   ```

5. Exécutez la commande suivante pour activer le processus du serveur de socket :

   ```
   kill -HUP `/bin/ps -ef | grep inetd | grep -v grep |
      awk '{print $2}'`
   ```

6. Procédez à des essais avec le serveur de socket. Pour cela, lancez des tentatives Telnet sur le port de votre choix. Si tout va bien, vous obtenez le contenu du fichier journal en retour :

   ```
   % telnet localhost 5555
   ```

   Pour quitter la session Telnet, tapez « ^] » (control-]), puis « quit » à l'invite de commande telnet.

Index