# Novell® Sentinel™

5.1.3

7 juillet 2006

www.novell.com

Volume II : GUIDE DE L'UTILISATEUR 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 règlementations 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 tierces

Toutes les marques tierces 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 tierces 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.

# 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 de Novell.

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 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

# Sommaire

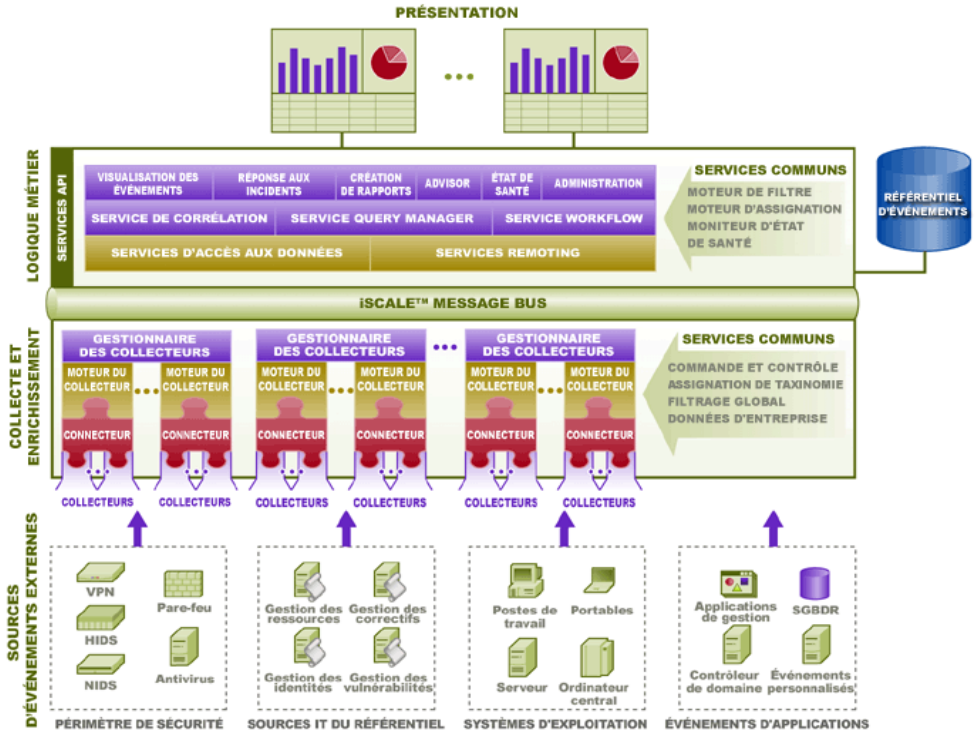
# 1 Présentation de Sentinel

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

Sentinel™ 5 est la solution d'avant-garde de gestion des informations de sécurité et de contrôle de la conformité aux réglementations. Il reçoit les informations collectées à partir de nombreuses sources à travers l'entreprise, les normalise, les classe par priorité, puis procède à la corrélation, le tout en temps réel. Sentinel est capable de collecter les données de nombreuses applications de sécurité du marché. En outre, sa souplesse permet de recueillir des données avec des dispositifs s'appuyant sur de nouvelles technologies et de nouveaux produits à mesure qu'évoluent les besoins liés aux installations et aux activités commerciales.

De nombreuses fonctions de Sentinel 5 sont le fruit d'un remodelage de l'architecture de Sentinel 4.0 et sont dictées par les besoins des clients de Novell. Alors que les menaces augmentent et que la pression en faveur d'une réglementation s'accroît, les entreprises recherchent une solution qui leur permettra :

- d'acquérir la visibilité et les informations nécessaires pour gérer un environnement de sécurité de manière plus économique ;
- de contrôler en permanence la conformité avec les règles internes et la législation (par exemple, Sarbanes-Oxley, HIPAA, GLBA, FISMA, NISPOM, DCID 6/3 et DITSCAP) ;
- d'identifier et de résoudre les incidents plus rapidement et de manière plus économique via une collecte et un traitement centralisés et automatisés des données relatives aux menaces et aux règles ;
- de fournir des mesures opérationnelles et exécutives pour évaluer en permanence la position de l'entreprise en matière de sécurité et de conformité et examiner les objectifs tactiques et stratégiques ;
- de réduire les coûts opérationnels liés au contrôle de la sécurité et de la conformité ainsi qu'à l'identification et la résolution des incidents.




Un événement est une opération ou occurrence signalée à Sentinel. Un événement reçu d'un périphérique de sécurité est nommé événement externe et un événement généré par Sentinel est nommé événement interne. Les événements peuvent être liés à la sécurité, aux performances ou aux informations. Par exemple, un événement externe peut consister en une attaque détectée par un système de détection d'intrusion, en une connexion réussie signalée par un système d'exploitation ou en une situation définie par le client (par exemple, un utilisateur qui accède à un fichier). Les événements internes sont générés par Sentinel pour indiquer un changement significatif d'état du système (par exemple, l'arrêt d'un collecteur ou la désactivation d'une règle de corrélation).

La corrélation est un processus consistant à analyser les événements de sécurité pour identifier des modèles dans un événement ou un flux d'événements. Par exemple, une règle de corrélation peut être créée pour détecter 30 événements ICMP ou plus se produisant dans un laps de temps d'une minute. Le trafic à volume élevé (inondation) d'événements ICMP peut résulter en une attaque de refus de service. La fonction de corrélation peut détecter des modèles dans un flux d'événements d'un seul périphérique, d'un groupe de périphériques similaires ou d'un ensemble arbitraire de périphériques. L'utilisateur peut ainsi mieux déterminer le risque et la gravité de l'incident.

Sentinel intègre également des informations supplémentaires aux données de flux (par exemple, des informations sur les machines situées sur le réseau et leurs services et vulnérabilités connus). Ces informations sont mises à la disposition de l'utilisateur en temps réel, ce qui rend les événements surveillés encore plus significatifs.

Le Centre de contrôle Sentinel utilise des processus d' arrière-plan pour afficher les événements en temps réel et les récapitulatifs d'événement (Active Views™), les incidents, les rapports d'historique (Analyse) et les rapports Advisor.

Les événements considérés comme revêtant une importance significative peuvent être regroupés dans un objet nommé *incident*. Un incident peut être créé manuellement par l'utilisateur ou automatiquement par le moteur de corrélation. L'incident peut comprendre des informations supplémentaires, telles que des informations sur les actifs attaqués ou sur les vulnérabilités de ces actifs, ou encore des informations sur l'attaque extraites du composant Sentinel Advisor. En outre, d'autres informations peuvent être ajoutées sous la forme de pièces jointes.

Ce guide suppose que vous maîtrisez les notions de base de la sécurité de réseau, de l'administration des bases de données et de l'environnement des systèmes d'exploitation Windows et UNIX.

Ce chapitre décrit l'architecture fonctionnelle et logique de Sentinel 5, puis ses modules-clés.

# Architecture fonctionnelle

Sentinel 5 se compose de trois sous-systèmes qui constituent le cœur de son architecture fonctionnelle :

- Plate-forme iSCALE : un framework évolutif régi par les événements.
- Intégration de la source de données : un framework de collecteur modulable.
- Intégration d'application : un framework d'application modulable.

Sentinel considère les services et les applications comme des points de terminaison de service abstraits prêts à répondre à des événements asynchrones. Les services sont des objets qui n'ont pas besoin de comprendre les protocoles ou la manière dont les messages sont acheminés vers les services pairs.

# Fonctionnalités de Sentinel

Sentinel est une application riche en fonctionnalités, destinée à l'utilisateur final et qui permet de contrôler et de gérer diverses fonctions. Voici certaines des fonctions principales :

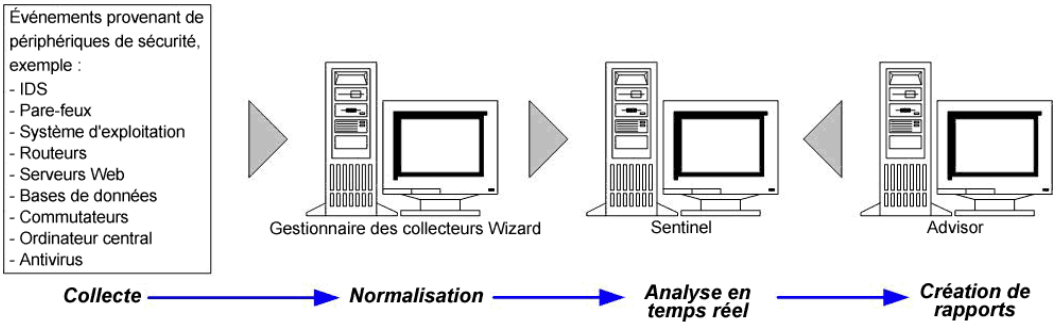
- Vues en temps réel des grands flux d'événements
- Fonctionnalités de génération de rapports basées sur les événements en temps réel et les événements d'historique
- Gestion des utilisateurs et de ce qu'ils peuvent voir et faire par attribution d'autorisations
- Possibilité de restreindre les événements auxquels les utilisateurs ont accès
- Organisation des événements en incidents pour une gestion et un suivi efficaces des réponses
- Détection de schémas dans les événements et les flux d'événements

# Présentation de l'architecture

Le système Sentinel est responsable de la réception des événements provenant du Gestionnaire des collecteurs Wizard. Les événements sont alors affichés en temps réel et consignés dans une base de données à des fins d'analyse d'historique.

À un niveau élevé, le système Sentinel utilise une base de données relationnelle et est constitué de processus Sentinel et d'un moteur de génération de rapports. Le système accepte en entrée des événements du Gestionnaire de collecteurs. Le Gestionnaire de collecteurs fait office d'interface avec les produits tiers et en normalise les données. Les données normalisées sont alors envoyées aux processus et à la base de données Sentinel.

L'analyse d'historique et la génération de rapports peuvent s'effectuer via le moteur de génération de rapports intégré de Sentinel. Le moteur de génération de rapports extrait les données de la base de données et intègre l'affichage des rapports dans le Centre de contrôle Sentinel à l'aide de documents HTML via une connexion HTTP.




Les fonctionnalités de Sentinel sont les suivantes :

- Traitement en temps réel des événements reçus du Gestionnaire des collecteurs Wizard
- Langage de corrélation basé sur les règles intuitif et flexible
- Des règles conçues en vue de performances élevées
- Architecture évolutive, multithread, distribuable et extensible

Les processus Sentinel communiquent entre eux via un intergiciel orienté message (MOM).

## Plate-forme iSCALE

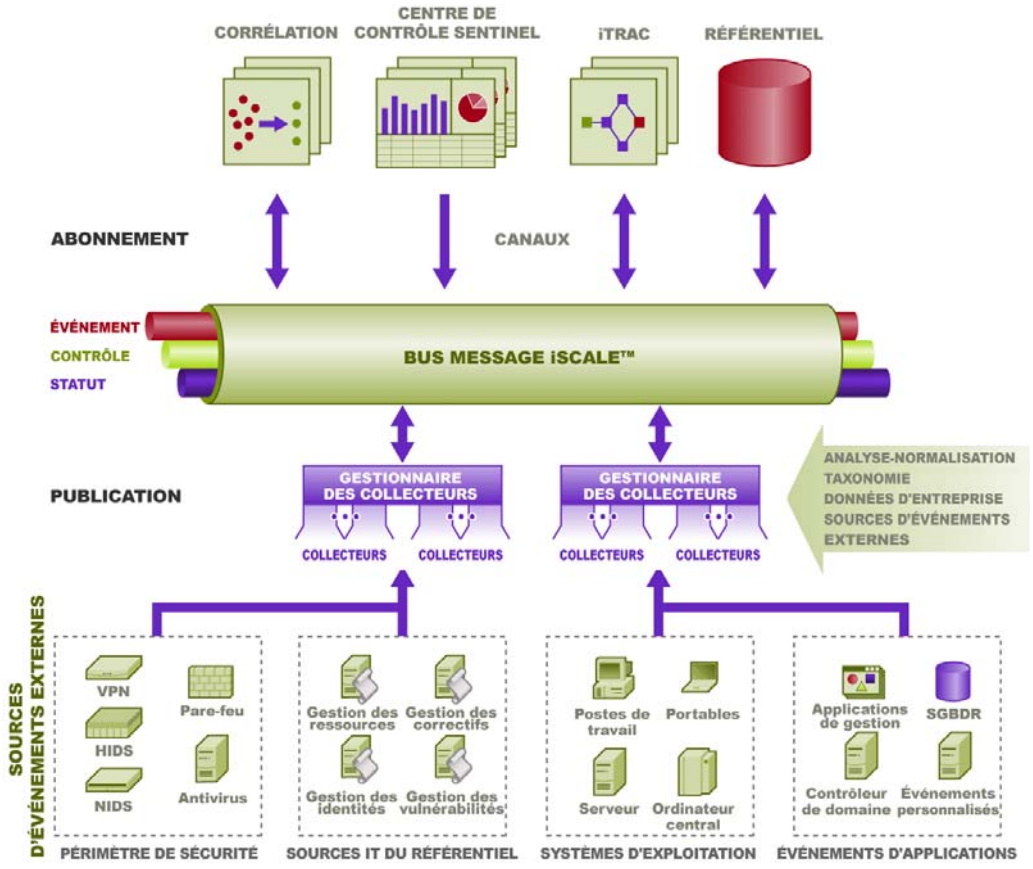
L'architecture iSCALE™ de Sentinel repose sur une architecture orientée service (SOA) basée sur les standards et combinant les avantages liés au traitement en mémoire et à l'informatique distribuée. Au cœur d'iSCALE réside un bus message spécialisé capable de traiter de gros volumes de données. Conçu de A à Z selon une approche s'appuyant sur les meilleures technologies et sur des standards, iSCALE peut évoluer de manière économique.

### Bus message

Le bus message iSCALE permet de faire évoluer des composants individuels de manière indépendante, tout en permettant une intégration basée sur les standards avec les applications externes. La clé de l'évolutivité réside dans le fait que, contrairement aux autres logiciels distribués, deux composants pairs ne communiquent jamais entre eux directement. Tous les composants communiquent via le bus message, qui est capable de déplacer des milliers de paquets de messages par seconde.

En tirant parti des fonctionnalités uniques du bus message, le canal de communication à haut débit peut maximiser et maintenir un taux de débit de données élevé à travers les composants indépendants du système. Les événements sont compressés et chiffrés en temps réel pour être acheminés efficacement et en toute sécurité du bord du réseau ou des points de collecte vers le hub du système, où s'effectue l'analyse en temps réel.

Le bus message iSCALE utilise une variété de services de mise en file d'attente qui font que la fiabilité de la communication ne se limite pas qu'aux aspects sécurité et performances de la plate-forme. Grâce à une variété de files d'attente temporaires et durables, le système offre une fiabilité et une tolérance aux pannes sans égal. Par exemple, les messages importants en transit sont enregistrés (en étant mis en file d'attente) en cas d'erreur dans le chemin de communication. Les messages mis en file d'attente sont acheminés à leur destination une fois que le système a récupéré d'une panne.




## Canaux

La plate-forme iSCALE utilise un modèle régi par les données ou les événements qui permet une évolution indépendante des composants du système entier en fonction de la charge. Ceci offre un modèle de déploiement souple, car l'environnement de chaque client varie : un site peut comporter un nombre élevé de périphériques avec peu d'événements, tandis qu'un autre moins de périphériques avec beaucoup d'événements. Les densités d'événements (à savoir le modèle de regroupement et de multiplexage des événements sur le câble à partir des points de collecte) sont différentes dans ces cas et le bus message permet une évolution cohérente des charges disparates.

iSCALE tire parti d'un environnement indépendant et multicanal qui élimine virtuellement les conflits et promeut un traitement parallèle des événements. Ces canaux et sous-canaux non seulement opèrent pour le transport des données d'événement, mais en plus permettent un contrôle précis des processus en vue de l'évolution et de l'équilibrage de charge du système dans des conditions de charge variables. L'utilisation de canaux de service indépendants (par exemple, les canaux de contrôle et les canaux de statut), outre le canal d'événement principal, permet une évolution sophistiquée et économique de l'architecture régie par les événements.

## Événement Sentinel

Sentinel reçoit les informations des périphériques, normalise ces informations en une structure nommée *Événement Sentinel* (ou *Événement*), puis envoie l'événement afin qu'il soit traité. L'événement est traité par l'affichage en temps réel, le moteur de corrélation et le serveur principal.

Un événement consiste en plus de 200 balises. Les balises sont de types différents et ont des fonctions différentes. Certaines sont prédéfinies, telles que celles relatives à la gravité, à la sévérité, à l'IP cible et au port cible. Il existe deux groupes de balises configurables : les balises réservées, destinées au fonctionnement interne de Novell en vue d'une expansion future, et les balises client, destinées aux extensions client.

Il est possible d'attribuer une nouvelle fonction aux balises en les renommant. La source d'une balise peut être *externe*, auquel cas la balise est définie explicitement par le périphérique ou le collecteur ou *référentiel* correspondant. La valeur d'une balise de référence est calculée en tant que fonction d'une ou de plusieurs autres balises à l'aide du service d'assignation. Par exemple, une balise peut être définie pour être le code de génération du bâtiment contenant l'actif mentionné comme IP cible d'un événement, ou bien encore, une balise peut être définie par le service d'assignation à l'aide d'une assignation définie par le client utilisant l'IP cible de l'événement.

### Service d'assignation

Le service d'assignation permet à un mécanisme sophistiqué de propager les données d'entreprise sur le système. Cette fonctionnalité favorise l'évolutivité et apporte des capacités d'extension en permettant un transfert intelligent des données entre différents nœuds du système distribué.

Le service d'assignation constitue une fonction de propagation des données qui permet d'effectuer des renvois entre les données de scanner de vulnérabilité et les signatures du système de détection d'intrusion, et autres données (par exemple, données d'actif, données d'entreprise, etc.). Ceci permet une notification immédiate lorsqu'une attaque tente d'exploiter un système vulnérable. Trois composants distincts fournissent cette fonctionnalité :

- La collecte des événements en temps réel à partir d'une source de détection d'intrusion.
- La comparaison de ces signatures aux dernières analyses de vulnérabilité.
- Le référencement croisé de données de flux d'attaque via Sentinel Advisor (un module facultatif qui effectue des renvois entre les signatures d'attaque IDS en temps réel et les données de scanner de vulnérabilité de l'utilisateur).

Le service d'assignation propage les informations dynamiquement à travers le système sans affecter sa charge. Lorsque d'importants jeux de données (à savoir, des assignations telles que des informations d'actif ou des informations de mise à jour de correctif) sont mis à jour sur le système, le service d'assignation propage les mises à jour à travers le système, dont la taille peut souvent atteindre des centaines de mégaoctets.

Les algorithmes du service d'assignation d'iSCALE traitent les jeux de données de référence volumineux via un système de production traitant de gros volumes de données en temps réel. Ces algorithme sont «conscients» des mises à jour et ne déplacent sélectivement que les modifications ou «jeux de données delta» du référentiel vers le bord ou le périmètre du système.

## Acheminement des assignations

Le service d'assignation utilise un modèle de mise à jour dynamique et achemine les assignations d'un point à l'autre, ce qui évite l'accumulation d'assignations statiques volumineuses dans la mémoire dynamique. Cette capacité d'acheminement s'avère particulièrement précieuse dans un système en temps réel critique tel que Sentinel, où doit exister un mouvement des données régulier, prédictif, flexible et indépendant des charges temporaires du système.

## Détection d'exploitation (service d'assignation)

Sentinel permet d'effectuer des renvois entre les signatures de données d'événement et les données de scanners de vulnérabilité. Les utilisateurs sont notifiés automatiquement et immédiatement lorsqu'une attaque tente d'exploiter un système vulnérable. Ceci est réalisé au moyen des éléments suivants :

- Données de flux Advisor
- Détection d'intrusion
- Analyse de la vulnérabilité
- Pare-feu

Advisor fournit une référence croisée entre les signatures de données d'événement et les données de scanner de vulnérabilité. Les données de flux Advisor reçoivent des données relatives aux alertes et aux attaques. Les données de flux d'alerte contiennent des informations sur les vulnérabilités et les menaces. Les données de flux d'attaque consistent en une normalisation des signatures d'événement et des plug-ins de vulnérabilité. Pour obtenir des informations sur l'installation d'Advisor, reportez-vous au *Guide d'installation de Sentinel*.

Les systèmes pris en charge sont les suivants :

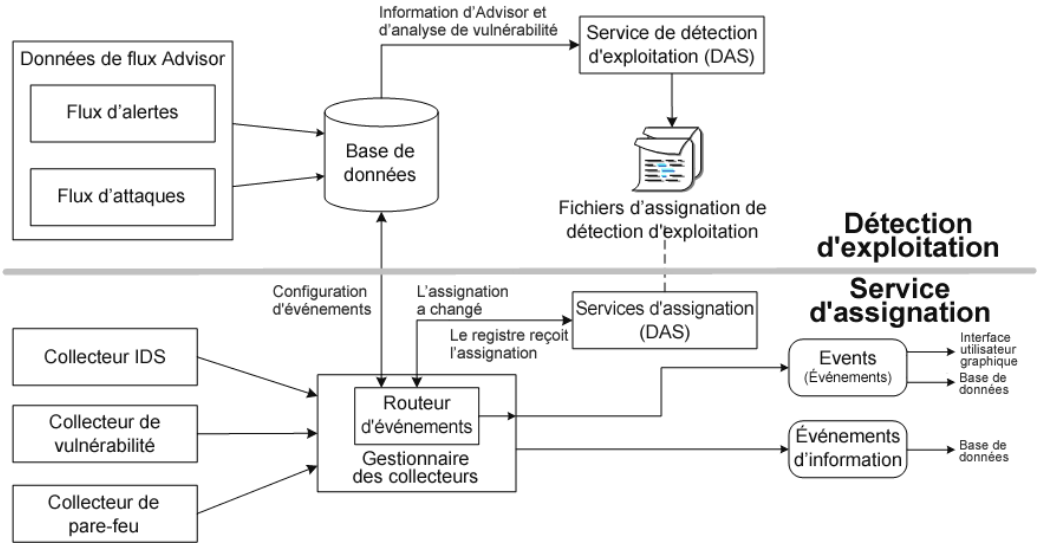
Systèmes de détection d'intrusion
- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- Intrusion.com (SecureNet_Provider)
- ISS BlackICE
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server
- ISS RealSecure Guard
- Snort
- Symantec Network Security 4.0 (ManHunt)
- Symantec Intruder Alert
- McAfee IntruShield

Scanners de vulnérabilité
- eEYE Retina
- Foundstone Foundscan
- ISS Database Scanner
- ISS Internet Scanner
- ISS System Scanner
- ISS Wireless Scanner
- Nessus
- nCircle IP360
- Qualys QualysGuard

Pare-feux
- Cisco IOS Firewall

Vous devez disposer d'au moins un scanner de vulnérabilité et soit d'un système de détection d'intrusion, soit d'un pare-feu de chaque catégorie ci-dessus. Le nom de périphérique de l'IDS et du pare-feu (rv31) doit être mis en surbrillance en gris dans l'événement comme ci-dessus. En outre, votre système de détection d'intrusion et votre pare-feu doivent renseigner correctement le champ DeviceAttackName (rt1) (par exemple, pour l'accès à Mambo uploadimage.php WEB-PHP).

Les données de flux Advisor sont envoyées à la base de données, puis au service de détection d'exploitation. Ce dernier génère un ou deux fichiers, en fonction du type des données qui ont été mises à jour.




Les fichiers d'assignation de détection d'exploitation sont utilisés par le service d'assignation pour associer les attaques aux exploitations de vulnérabilités.

Les scanners de vulnérabilité analysent le système (l'actif) pour en détecter les zones vulnérables. Le système de détection d'intrusion détecte les attaques (s'il en existe) subies par ces zones vulnérables. Les pare-feu détectent si l'une de ces zones vulnérables fait l'objet de trafic. Si une attaque est associée à une vulnérabilité, l'actif a été exploité.

Le service de détection d'exploitation génère deux fichiers situés dans :

```
$ESEC_HOME/sentinel/bin/map_data
```

Ces deux fichiers sont attackNormalization.csv et exploitDetection.csv.

Le fichier attackNormalization.csv est généré suite à :

- la réception de données de flux Advisor,
- le démarrage du service DAS (si activé dans le fichier das_query.xml ; désactivé par défaut).

Le fichier exploitDetection.csv est généré suite à l'une des opérations suivantes :

- la réception de données de flux Advisor,
- l'analyse de vulnérabilité,
- Le démarrage de Sentinel Server (si activé dans le fichier das_query.xml ; désactivé par défaut).

Par défaut, deux colonnes d'événements configurés sont utilisées pour la détection d'exploitation, ces colonnes étant référencées à partir d'une assignation (toutes les balises assignées comportent une icône de défilement).

- Vulnérabilité
- AttackId

| Severity | Vulnerability | AttackId |
|---|---|---|
| 2 | 0 | |
| 3 | 0 | |

Si la valeur du champ de vulnérabilité (*vul*) est égale à 1, l'actif ou le périphérique cible est exploité. Si elle est égale à 0, l'actif ou le périphérique cible n'est pas exploité.

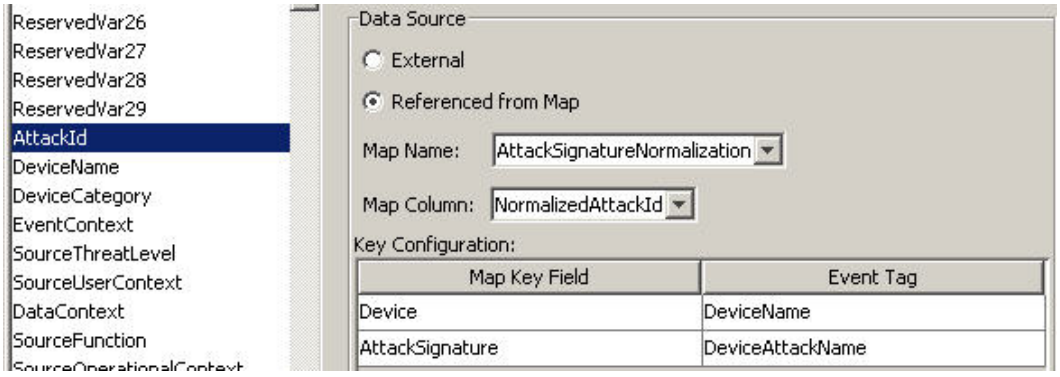
Sentinel est fourni préconfiguré avec les noms d'assignation suivants associés à attackNormalization.csv et exploitDetection.csv.

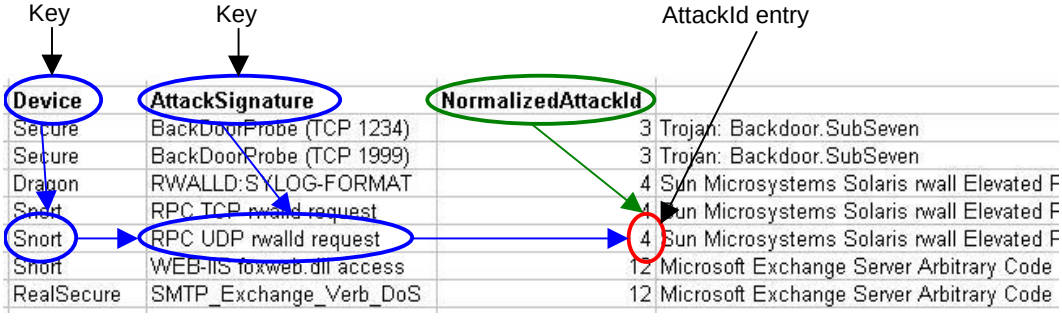
| Nom de l'assignation | Nom du fichier csv |
|---|---|
| ▪ AttackSignatureNormalization | ▪ attackNormalization.csv |
| ▪ IsExploitWatchlist | ▪ exploitDetection.csv |

Il existe deux types de sources de données :

- Externe : extrait les informations du collecteur.
- Référencé par l'assignation : extrait les informations d'un fichier d'assignation pour renseigner la balise.

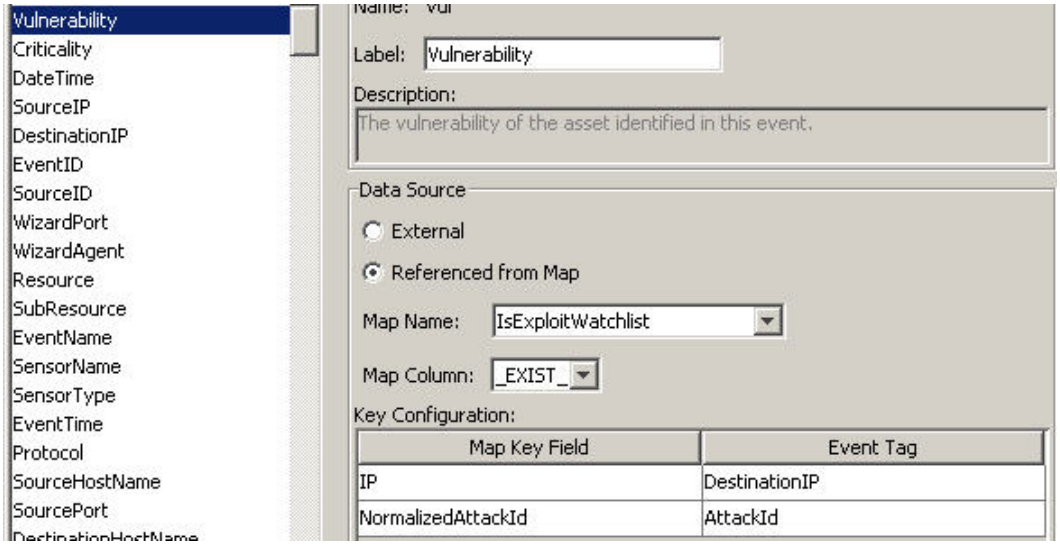
Les colonnes Device (type du périphérique de sécurité, tel que - Snort) et AttackSignature sont définies comme clés pour la balise AttackId, qui utilise la colonne NormalizedAttackID dans le fichier attackNormalization.csv. Sur une ligne où la balise d'événement DeviceName (un périphérique de détection d'intrusion, tel que Snort, les informations étant fournies par Advisor et les informations de vulnérabilité provenant de la base de données Sentinel) est la même que Device et où la balise d'événement DeviceAttackName (les informations d'attaque étant fournies pas Advisor dans la base de données Sentinel via le service de détection d'exploitation) est la même que AttackSignature, la valeur de AttackId est spécifiée à l'endroit où cette ligne croise la colonne NormalizedAttackID.




La balise Vulnerability comporte une colonne _EXIST_, ce qui signifie que la valeur résultante de l'assignation sera égale à 1 si la clé figure dans IsExploitWatchlist (fichier exploitDetection.csv) ou à 0 dans le cas contraire. Les colonnes clé de la balise Vulnerability sont IP et NormalizedAttackId. Si une même ligne comprend un événement

entrant avec une balise DestinationIP qui correspond à la colonne IP et une balise d'événement AttackId qui correspond à la colonne NormalizedAttackId, le résultat est un (1). Si aucune correspondance n'est trouvée sur la même ligne, le résultat est zéro (0).




### Intégration des sources de données

L'utilisation d'une technologie adaptable et flexible réside au cœur de la stratégie d'intégration de source de données de Sentinel, stratégie appliquée grâce à des collecteurs d'interprétation (également nommés collecteurs) qui analysent et normalisent les événements du flux de données.

Ces collecteurs peuvent être modifiés selon les besoins et ne sont liés à aucun environnement spécifique. La création, la modification, la maintenance et le déploiement des collecteurs sont simples et peuvent être effectués directement par les utilisateurs. Un environnement de déploiement intégré permet de créer des collecteurs de manière interactive via glisser-déposer à partir d'une interface utilisateur. Dans la mesure où des utilisateurs autres que les programmeurs peuvent créer des collecteurs, les besoins actuels et futurs sont satisfaits dans un environnement informatique qui évolue constamment. Le contrôle des collecteurs (par exemple, démarrage ou arrêt) s'effectue de manière centrale à partir du Centre de contrôle Sentinel.

### Intégration des applications

L'intégration des applications externes via des API standard est centrale à Sentinel. Par exemple, une API bidirectionnelle destinée aux systèmes de ticket de dépannage incluant Remedy® et ServiceDesk® de HP OpenView permet une intégration directe des systèmes externes.

L'API reposant sur les services Web permet aux systèmes externes compatibles SOAP de tirer parti d'une intégration totale au système Sentinel.

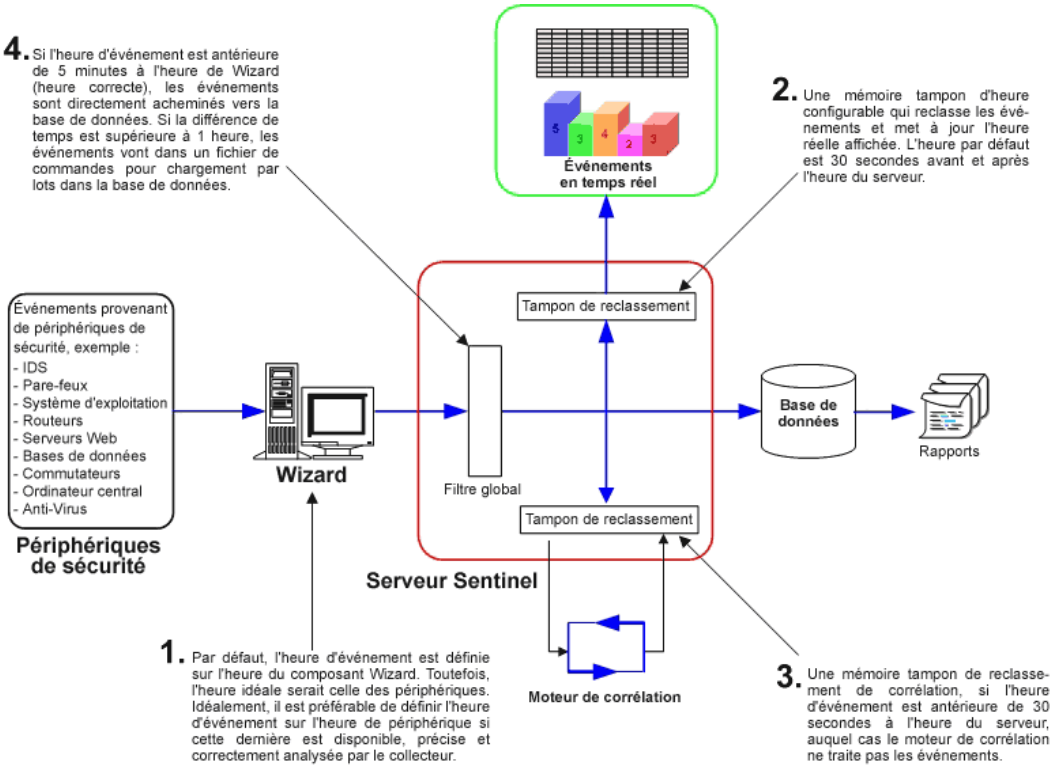
## Heure

L'heure d'un événement est déterminante pour son traitement. Elle est importante pour la génération de rapports et l'audit, ainsi que pour le traitement en temps réel. Le moteur de corrélation traite les flux d'événements classés par heure et détecte les modèles existant dans les événements, ainsi que les schémas temporaires existant dans les flux. Cependant,

le périphérique générant l'événement peut ne pas connaître l'heure réelle à laquelle l'événement est généré. Pour pallier cela, Sentinel propose deux options afin de traiter les alertes issues des périphériques de sécurité : se fier à l'heure signalée par le périphérique et utiliser cette heure comme heure de l'événement, ou ne pas se fier à l'heure signalée par le périphérique et à la place horodater l'événement à l'heure à laquelle il est traité pour la première fois par Sentinel (par le collecteur).

Sentinel est un système distribué et comprend plusieurs processus qui peuvent résider à divers endroits du réseau. En outre, le périphérique peut être à l'origine d'un certain retard. Pour pallier cela, les processus Sentinel reclassent les événements dans un flux basé sur l'heure avant de procéder au traitement.

L'illustration suivante décrit le concept de l'heure dans Sentinel.




1. Par défaut, l'heure d'événement est définie sur l'heure du composant Wizard, mais l'heure idéale serait celle des périphériques. Il est donc préférable de définir l'heure d'événement sur l'heure de périphérique si cette dernière est disponible, précise et correctement analysée par le collecteur.
2. Une mémoire tampon d'heure configurable qui reclasse les événements et met à jour l'heure réelle affichée. L'heure par défaut est 30 secondes avant et après l'heure du serveur.
3. Une mémoire tampon de reclassement de corrélation, si l'heure d'événement est antérieure de 30 secondes à l'heure du serveur, auquel cas le moteur de corrélation ne traite pas les événements.
4. Si l'heure d'événement est antérieure de 5 minutes à l'heure de Wizard (heure correcte), les événements sont directement acheminés vers la base de données.

## Événements internes ou système

Les événements internes ou système permettent de rendre compte du statut et du changement de statut du système. Le système interne génère deux types d'événements, à savoir :

- Les événements internes
- Les événements de performances

Les événements internes fournissent des informations et décrivent un état unique ou un changement de statut du système. Ils signalent les cas où un utilisateur se connecte ou n'est pas authentifié, le démarrage d'un processus ou l'activation d'une règle de corrélation. Les événements de performances sont générés périodiquement et décrivent l'utilisation moyenne des ressources par différents composants du système.

Tous les événements système renseignent les champs d'attribut suivants :

- Le champ Type de capteur (ST - Sensor Type) : pour les événements internes, ce champ est défini sur I et, pour les événements de performances, sur P.
- ID d'événement : un UUID unique de l'événement.
- Heure d'événement : l'heure à laquelle l'événement a été généré.
- Source : l'UUID du processus qui a généré l'événement.
- Nom du capteur : le nom du processus qui a généré l'événement (par exemple, DAS_Binary).
- RV32 (Catégorie de périphérique) : défini sur ESEC.
- Collecteur : « Performance » pour les événements de performances et « Internal » pour les événements internes.

Outre les attributs courants, chaque événement système définit également la ressource, la sous-ressource, la gravité, le nom de l'événement et les balises de message. Le nom d'un événement interne est suffisamment spécifique pour identifier la signification exacte de l'événement (par exemple, UserAuthenticationFailed). Les balises de message apportent des détails spécifiques. Dans l'exemple ci-dessus, la balise de message contient le nom de l'utilisateur, le nom du système d'exploitation (si ce nom est disponible), ainsi que le nom de la machine. Le nom d'un événement de performances est un nom générique qui décrit le type des données statistiques, les données elles-mêmes figurant dans la balise de message.

Les événements de performances sont envoyés directement à la base de données. Pour les afficher, effectuez une interrogation rapide.

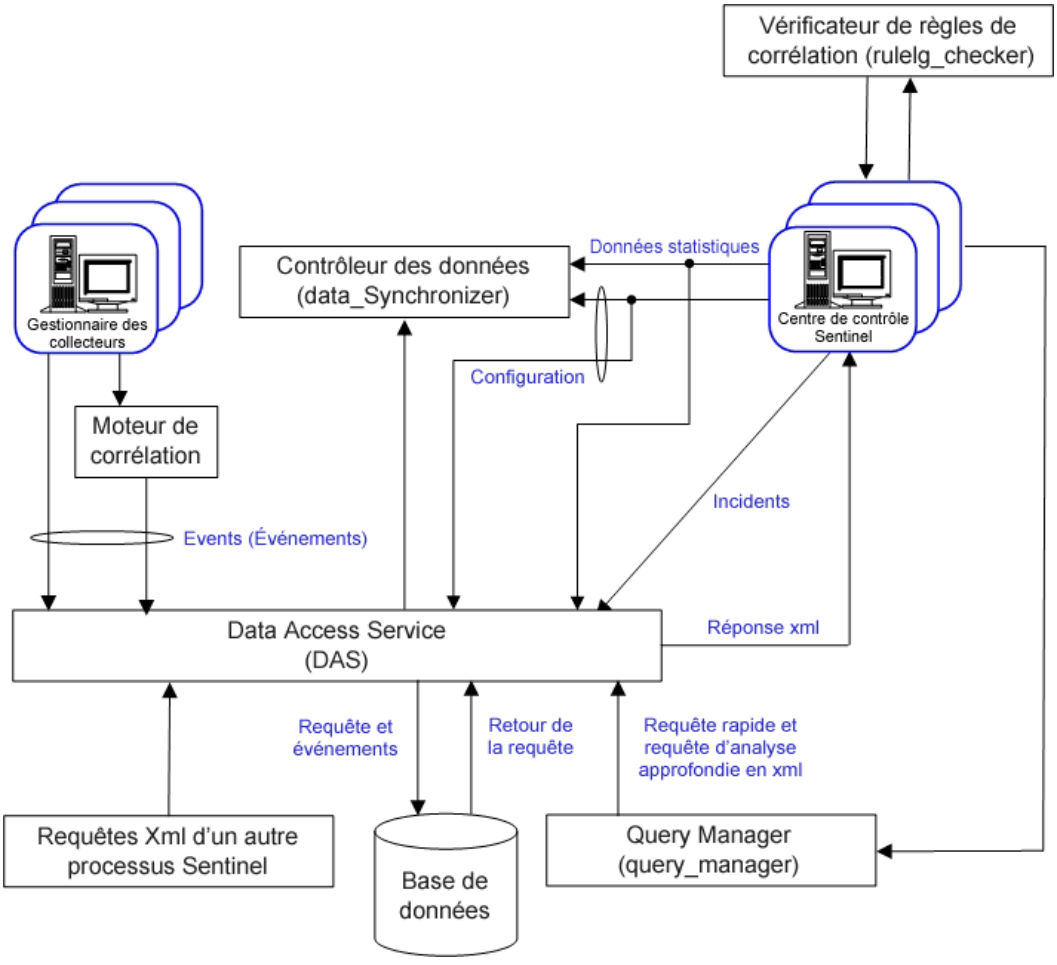
Voir l'annexe A : *Événements système*.

## Processus

Le service Windows et les processus suivants communiquent entre eux via iSCALE, l'intergiciel orienté message (MOM).

- Watchdog
- Moteur Event Statistics
- Data Synchronizer (Data Controller)
- Correlation Engine
- Processus RuleLg Checker (vérificateur de règle de corrélation)
- Data Access Service (DAS) – binaire, requête et Active Views™
- Processus Query Manager
- Sentinel Service (MSSQL uniquement) - Reportez-vous à Watchdog

L'architecture de Sentinel Server est la suivante :




## Processus Watchdog

Watchdog est un processus Sentinel qui gère d'autres processus Sentinel. Si un processus autre que Watchdog s'arrête, Watchdog le signale, puis redémarre ce processus.

Sous Windows, Watchdog constitue un service nommé Sentinel. Si ce service est arrêté, il arrête tous les processus Sentinel sur cette machine.

## Event Statistics

Le moteur Event Statistics est un composant du processus das_binary. Il gère les données utilisées par les graphiques Active Views et les tables d'événements dans le Centre de contrôle Sentinel.

Le moteur tient à jour un jeu d'événements et de données statistiques pour chaque combinaison filtre/attribut d'événement spécifiée par l'assistant Active Views. La première fois qu'un utilisateur crée une vue active avec un filtre et un attribut d'événement donnés, un nouveau jeu de données est créé. Ce jeu de données contient le nombre d'occurrences de cet attribut à des intervalles fixes, ainsi que les événements les plus récents pour chacun de ces intervalles. Chaque jeu de données est configuré pour détenir les données des dernières 24 heures.

Les intervalles sont envoyés au Centre de contrôle Sentinel après un bref délai pour stabiliser les données qui ont pu arriver tardivement en raison d'un ralentissement du réseau et d'un décalage horaire.

Les vues actives sont automatiquement partagées par plusieurs utilisateurs si l'attribut d'événement et le filtre souhaités sont les mêmes. Lorsqu'une vue active n'est plus utilisée par aucun utilisateur, elle est abandonnée au bout d'une heure. Cependant, si une vue active est enregistrée dans les préférences utilisateur, elle continue à collecter des données pendant un maximum de 100 heures.

### Processus de synchronisation des données (contrôleur des données)

Le processus de synchronisation des données (data_synchronizer) gère la modification des données de configuration par plusieurs utilisateurs. Lorsqu'un utilisateur demande à modifier des données via le Centre de contrôle Sentinel, l'enregistrement de données est verrouillé par le synchroniseur de données. Les détails relatifs à l'utilisateur qui a verrouillé les données sont publiés sur les autres Centres de contrôle Sentinel actifs et aucun autre utilisateur ne peut modifier ces données. Si un Centre de contrôle Sentinel est fermé avant qu'il ne déverrouille les données qu'il a verrouillées, le délai imparti au verrou expire.

### Processus de moteur de corrélation (correlation_engine)

Le processus Correlation Engine (correlation_engine) reçoit des événements du Gestionnaire des collecteurs Wizard et publie les événements corrélés en fonction de règles de corrélation définies par l'utilisateur.

### Processus RuleLg Checker (rulelg_checker)

Le processus du vérificateur RuleLg (rulelg_checker) valide la syntaxe des expressions de filtre et de règle de corrélation. Le Centre de contrôle Sentinel utilise ces résultats pour déterminer si un filtre ou une règle de corrélation peut être enregistrée.

### Processus DAS (Data Access Service)

Le processus DAS (Data Access Service) constitue le service de persistance de Sentinel Server et fournit une interface à la base de données. Il permet un accès régi par les données au serveur principal de la base de données.

DAS est un conteneur, composé de cinq processus différents. Chaque processus est responsable de différents types d'opérations de base de données. Ces processus sont contrôlés par les fichiers de configuration suivants :

- das_binary.xml : utilisé pour les opérations d'insertion d'événements corrélés ou non.
- das_query.xml : toutes les autres opérations de base de données.
- activity_container.xml : utilisé pour exécuter et configurer le service d'activité.
- workflow_container.xml : utilisé pour configurer le service de processus de travail (iTRAC).
- das_rt.xml : utilisé pour configurer la fonction Active Views dans la console Sentinel.

DAS reçoit les requêtes des différents processus Sentinel, les convertit en une interrogation de la base de données, traite le résultat de la base de données, puis convertit de nouveau ce résultat en une réponse. Il prend en charge les requêtes d'extraction d'événement pour l'interrogation rapide et la hiérarchisation vers le bas vers les évènements, les requêtes d'extraction des informations de vulnérabilité et des informations Advisor et les requêtes de manipulation des informations de configuration. Le service DAS traite également la consignation de tous les événements reçus du Gestionnaire des collecteurs Wizard et les requêtes d'extraction et de stockage des informations de configuration.

### Processus Query Manager (query_manager)

Le processus Query Manager (query_manager) reçoit les requêtes d'interrogation rapides et d'analyse approfondie du Centre de contrôle Sentinel et les transmet à la base de données via DAS. Les requêtes du Centre de contrôle Sentinel déterminent les événements requis d'un filtre. Si un filtre est utilisé, le Gestionnaire des requêtes extrait la définition du filtre et convertit le filtre au format XML. Il envoie ensuite la requête à DAS. Les filtres ne peuvent pas tous être convertis en requêtes traitables par la base de données. Si le filtre est entièrement converti, le Gestionnaire des requêtes indique à DAS d'envoyer directement la réponse au Centre de contrôle Sentinel. Si le filtre contient des expressions génériques qui ne peuvent pas être converties en SQL, le Gestionnaire des requêtes convertit ce qu'il peut, puis génère un critère plus restrictif qui retourne un super jeu des événements requis. Dans ce cas, le Gestionnaire des requêtes indique à DAS de lui renvoyer le résultat. Lorsqu'il reçoit la réponse, il la filtre en mémoire et envoie les événements qui passent le filtre au Centre de contrôle Sentinel.

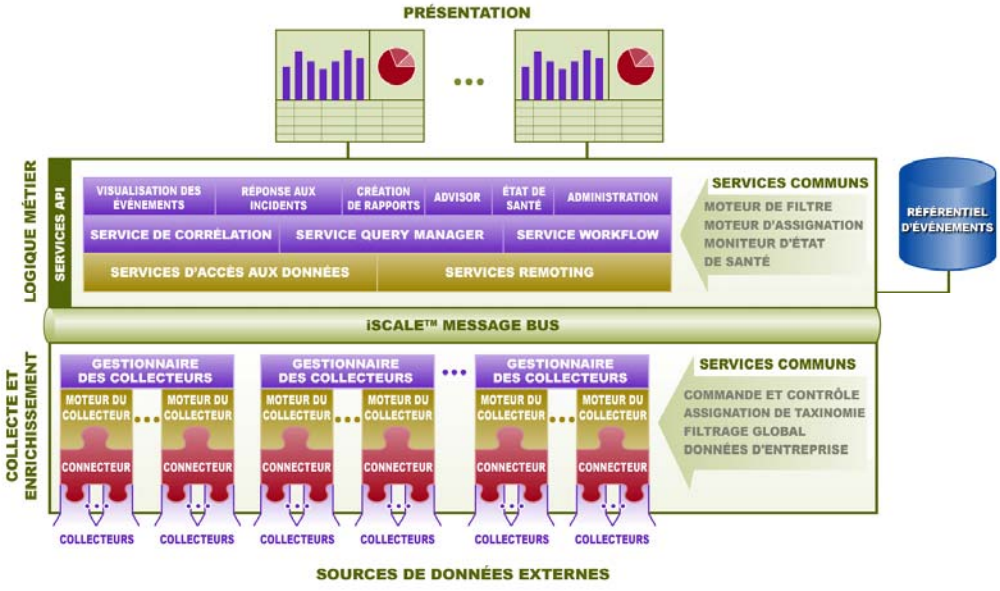
## Architecture logique

Sentinel 5 comprend trois couches logiques :

- Couche de collecte et d'enrichissement
- Couche logique métier
- Couche de présentation

La couche de collecte/d'enrichissement regroupe les événements issus de sources de données externes, convertit les formats spécifiques aux périphériques en formats Sentinel, intègre les données métier à la source des événements natifs, puis envoie les paquets d'événements au bus message. Le composant-clé dans l'exécution de cette fonction est le collecteur, aidé par un service d'assignation de taxinomie et de filtre global.

La couche de logique métier contient un jeu de composants distribuables. Le composant de base est, d'une part, un service Remoting qui apporte des fonctionnalités de messagerie aux objets de données et aux services pour permettre un accès transparent aux données sur l'ensemble du réseau et, d'autre part, un service Data Access qui est un service de gestion des objets permettant aux utilisateurs de définir des objets avec des métadonnées. D'autres services incluent Correlation, Query Manager, Workflow, Event Visualization, Incident Response, Health, Advisor, Reporting et Administration.




La couche de présentation restitue l'interface de l'application à l'utilisateur final. Un tableau de bord complet nommé Centre de contrôle Sentinel offre un outil de travail utilisateur intégré qui consiste en un tableau comprenant sept applications différentes accessibles via un même framework. Ce framework interplate-forme repose sur des standards Java™ 1.4 et offre une vue unifiée des composants de logique commerciale indépendants : graphiques interactifs en temps réel, réponse aux incidents donnant lieu à une action, flux de travail d'incidents applicable automatisé, génération de rapports, résolution des incidents au niveau d'exploitations connues, etc.

Chacune des couches est illustrée dans la figure ci-dessus et décrite en détail dans les sections suivantes.

## Couche de collecte et d'enrichissement

Les événements sont regroupés à l'aide d'un ensemble de collecteurs flexibles et configurables qui collectent les données à partir d'une multitude de capteurs, de périphériques et de sources. Les utilisateurs peuvent utiliser des collecteurs préconçus, modifier des collecteurs existants ou concevoir leurs propres collecteurs pour s'assurer que le système répond à tous les besoins.

Les données regroupées par les collecteurs sous la forme d'événements sont ensuite normalisées et converties au format XML, enrichies d'une série de métadonnées (à savoir des données relatives à des données) à l'aide d'un ensemble de services métier, puis propagées sur le serveur en vue d'une analyse informatique approfondie effectuée avec la plate-forme du bus message. La couche de collecte et d'enrichissement comprend les composants suivants :

- Connecteurs et collecteur
- Moteur et Gestionnaire des collecteurs
- Générateur de collecteurs

### Connecteurs et collecteurs

Un connecteur est un concentrateur ou adaptateur multiplex qui connecte le moteur de collecteur aux périphériques surveillés.

Les collecteurs regroupent au niveau composant les données d'événement d'une source spécifique. Sentinel 5 prend principalement en charge des connexions sans collecteur distantes aux sources. Cependant, les collecteurs peuvent être déployés sur des périphériques spécifiques où une approche distante est moins efficace.

Les collecteurs sont contrôlés à partir du Centre de contrôle Sentinel, qui régit la communication entre les collecteurs et la plate-forme Sentinel pour l'analyse en temps réel, le calcul de corrélation et la réponse aux incidents.

### Moteur et Gestionnaire des collecteurs

Le Gestionnaire des collecteurs gère les collecteurs, surveille les messages de statut du système et filtre les événements selon les besoins. Les fonctions principales du Gestionnaire des collecteurs incluent la transformation des événements, l'ajout de données métier aux événements par taxinomie, le filtrage global des événements, l'acheminement des événements et l'envoi de messages d'état de santé au serveur Sentinel.

Un moteur de collecteur constitue le composant d'interprétation qui analyse le code du collecteur.

### Générateur de collecteurs

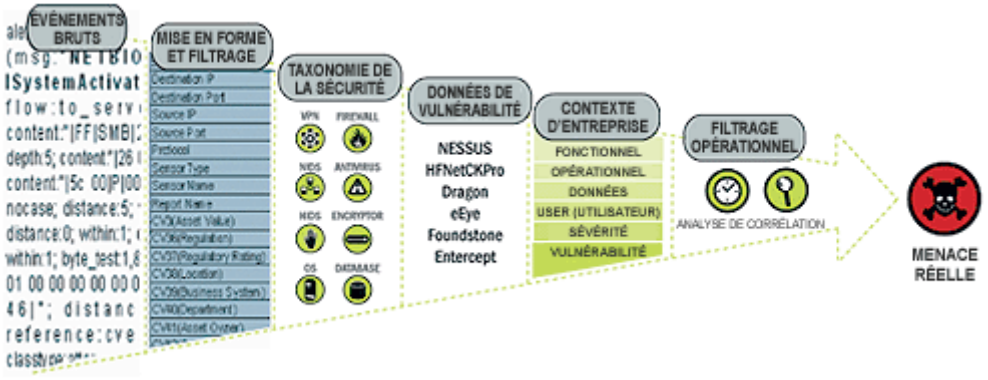
Le Générateur de collecteurs est une application autonome utilisée pour concevoir, configurer et déboguer des collecteurs. Cette application fait office d'environnement de développement intégré (IDE) : elle permet à l'utilisateur de créer des collecteurs pour analyser des données de périphériques source via un langage d'interprétation dédié conçu pour gérer la nature des événements de réseau et de sécurité.

### Services communs

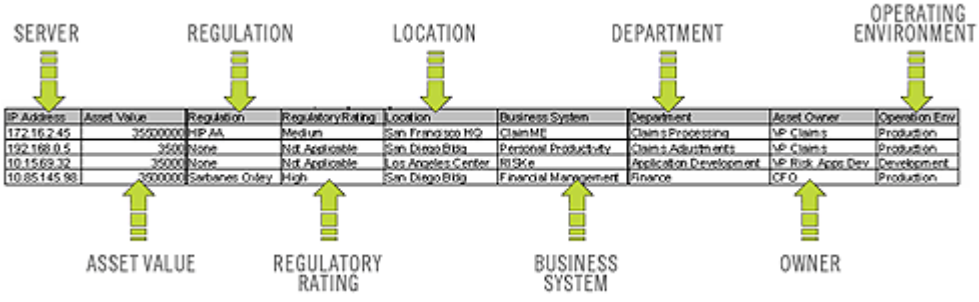
Tous les composants de cette couche de collecte et d'enrichissement décrits ci-dessus sont régis par un ensemble de services communs. Ces services sont à la base de la collecte et de l'enrichissement des données et aident à filtrer les éléments parasitaires des informations (via des filtres globaux), à appliquer des balises définies par l'utilisateur pour enrichir les informations d'événement (via des services de données métier et d'assignation de taxinomie) et à gérer les fonctions des collecteurs de données (via des services de commande et de contrôle).

**Taxinomie** : presque tous les produits de sécurité génèrent des événements dans différents formats et dont le contenu varie. Par exemple, Windows et Solaris signalent l'échec d'une connexion différemment.

La fonction de taxinomie de Sentinel traduit automatiquement les données de produit hétérogènes en termes significatifs, ce qui permet d'obtenir une vue homogène en temps réel de la sécurité de l'ensemble du réseau. Elle formate et filtre les événements de sécurité bruts avant d'ajouter un contexte d'événement au flux de données. Ce processus formate toutes les données de sécurité dans la structure la plus optimale pour qu'elles soient traitées par le moteur de corrélation Sentinel, comme l'illustre le diagramme suivant.




**Données d'entreprise** : Sentinel 5 injecte des données métier contextuelles directement dans le flux d'événements. Il englobe jusqu'à 135 champs personnalisables dans lesquels les utilisateurs peuvent ajouter des informations d'actif, telles que la division stratégique, le propriétaire, la valeur d'actif ou des données géographiques. Une fois ces informations ajoutées dans le système, tous les autres composants peuvent tirer parti du contexte supplémentaire.




**Détection d'exploitation** : la détection d'exploitation active des notifications entraînant une action immédiate pour des attaques subies par des systèmes vulnérables. Elle fournit un lien en temps réel entre les signatures du système de détection d'intrusion et les résultats d'analyse de vulnérabilité. Les utilisateurs sont automatiquement et immédiatement informés des attaques qui tentent d'exploiter les systèmes vulnérables. L'efficacité de la réponse aux incidents s'en trouve ainsi considérablement améliorée.

La détection d'exploitation fournit aux utilisateurs des mises à jour des assignations entre les signatures du système de détection d'intrusion et les signatures des scanner de vulnérabilité. Les assignations incluent une liste complète de scanners de détection d'intrusion et de vulnérabilité. Les utilisateurs n'ont qu'à télécharger les résultats d'analyse de vulnérabilité dans Sentinel. La détection d'exploitation analyse automatiquement ces résultats et met à jour les collecteurs IDS appropriés. Elle utilise les connaissances intégrées relatives au statut de vulnérabilité pour définir en temps réel la priorité des réponses aux menaces à la sécurité.

Lorsqu'une attaque est lancée contre un actif vulnérable, la fonctionnalité de détection d'exploitation alerte les utilisateurs avec le niveau de gravité correspondant de la vulnérabilité exploitée. Les utilisateurs peuvent alors prendre des mesures immédiates concernant les événements hautement prioritaires. Ceci élimine l'aspect aléatoire de la surveillance des alertes et améliore l'efficacité de la réponse aux incidents car les mesures portent alors sur les attaques connues contre les actifs vulnérables.

La fonctionnalité de détection d'exploitation permet également aux utilisateurs d'associer des signatures à des vulnérabilités ou de les dissocier pour mieux identifier les faux positifs et les négatifs et tirer parti des signatures personnalisées ou des analyses de vulnérabilité.

## Couche de logique métier

Le noyau de la plate-forme Sentinel 5 consiste en un ensemble de services partiellement reliés qui peuvent s'exécuter dans une configuration autonome ou dans le cadre d'une topologie distribuée. Cette architecture orientée service (SOA) est nommée iSCALE. Plus particulièrement, l'architecture SOA de Sentinel comprend un ensemble de moteurs, de services et d'API opérant ensemble pour permettre une montée en charge linéaire de la solution pour faire face à une augmentation du volume de données et/ou de traitement.

Les services Sentinel s'exécutent dans des conteneurs spécialisés et permettent un traitement et une évolution inégalés, car ils sont optimisés pour le transport et le calcul basés sur les messages. Les services-clés qui composent Sentinel Server incluent notamment :

- Service Remoting
- Service Data Access Service
- Service Query Manager
- Service Correlation
- Service Workflow
- Event Visualization
- Incident Response
- Reporting
- Advisor
- Health
- Administration

### Service Remoting

Le service Remoting de Sentinel 5 fournit le mécanisme par lequel le serveur et les programmes client communiquent. Ce mécanisme est généralement nommé application d'objet distribuée.

Plus particulièrement, le service Remoting apporte :

- Une localisation des objets distants : ceci s'effectue via des métadonnées qui décrivent le nom d'objet ou l'unité d'enregistrement. L'emplacement réel n'est pas nécessaire, car le bus message iSCALE ne le prend pas en compte.
- Communication avec les objets distants : les détails de la communication entre les objets distants sont traités par le bus message iSCALE.
- Acheminement et mémorisation par bloc des objets : lorsque de gros volumes de données doivent faire l'aller-retour entre le client et le serveur, ces objets sont optimisés pour charger les données à la demande.
- Rappels : il s'agit d'un modèle et  d'une couche d'abstraction intégrés au service Remoting qui permettent une communication avec les objets distants PTP.
- Statistiques et surveillance des services : des statistiques sur les performances et la charge sont générées. Elles sont destinées à l'utilisation de ces services distants.

### Service Data Access

Le service Data Access (DAS) est un service de gestion des objets qui permet aux utilisateurs de définir des objets à l'aide de métadonnées. Il gère les objets et l'accès aux objets et automatise la transmission et la persistance. Il fait également office de façade d'accès aux données à partir d'un magasin de données persistantes, tel qu'une base de données, des services d'annuaire ou des fichiers. Les tâches effectuées par le service DAS incluent un accès uniforme aux données via JDBC et, le cas échéant, des stratégies d'insertion d'événement hautes performances
à l'aide de connecteurs natifs (à savoir OCI pour Oracle 9i et ADO pour Microsoft SQL Server).

### Service Query Manager

Le service Query Manager gère les requêtes d'analyse approfondie et d'historique d'événement à partir du Centre de contrôle Sentinel. Ce service constitue un composant intégral pour mettre en œuvre l'algorithme de pagination utilisé dans la fonctionnalité de recherche de l'historique d'événement. Il convertit les filtres définis par l'utilisateur en critères valides et ajoute à ces critères des critères de sécurité avant l'extraction des événements. En outre, ce service empêche les critères de changer pendant une transaction d'historique d'événement paginé.

### Service Correlation

L'algorithme de corrélation de Sentinel 5 calcule les événements corrélés en analysant le flux de données en temps réel. Il publie les événements corrélés en fonction de règles définies par l'utilisateur avant que les événements n'atteignent la base de données. Les règles du moteur de corrélation peuvent détecter un modèle dans un événement unique d'une fenêtre d'événements s'exécutant Lorsqu'une correspondance est détectée, le moteur de corrélation génère un événement corrélé décrivant le modèle trouvé et peut générer un incident ou déclencher un processus de travail de résolution via iTRAC. Le moteur de corrélation fonctionne avec un composant de vérificateur de règle qui calcule les expressions de règle de corrélation et valide la syntaxe des filtres. Outre un jeu complet de règles de corrélation, le moteur de corrélation de Sentinel apporte des avantages spécifiques par rapport aux moteurs de corrélation basés sur la base de données.

- En s'appuyant sur un traitement en mémoire plutôt que sur des insertions et lectures de base de données, le moteur de corrélation opère en cas de volumes stables élevés et de pics d'événement lorsqu'il est attaqué, situation où les performances de corrélation sont des plus critiques.
- Le volume de corrélation ne ralentissant pas les autres composants système, l'interface utilisateur continue à réagir rapidement, en particulier en cas de gros volumes d'événements.
- Corrélation distribuée : les entreprises peuvent déployer plusieurs moteurs de corrélation, chacun sur son propre serveur, sans devoir répliquer des configurations ni ajouter des bases de données. Une montée en charge par composant apporte une évolutivité économique et améliore les performances.
- Le moteur de corrélation peut ajouter des événements aux incidents une fois un incident déterminé.

Les utilisateurs sont encouragés à utiliser la mesure ERPS (Event Rules per Second, règles d'événement par seconde). Il s'agit de la mesure du nombre d'événements qui peuvent être examinés par une règle de corrélation par seconde. Cette mesure constitue un bon indicateur de performances car elle estime l'impact sur les performances lorsque deux facteurs se croisent : événements par seconde et nombre de règles utilisées.

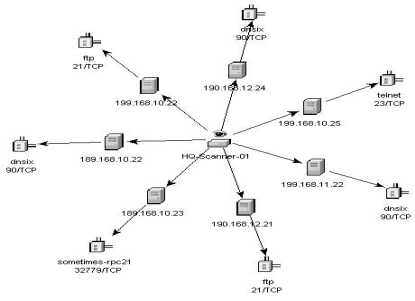
## Service Workflow (iTRAC)

Le service Workflow reçoit les déclencheurs à la création d'incidents et lance les processus de travail en fonction de modèles de processus de travail prédéfinis. Il gère le cycle de vie de ces processus en générant des éléments de travail ou en exécutant des activités. Ce service maintient également un historique des processus terminés pouvant servir à l'audit des réponses aux incidents.

## Event Visualization

Active Views™, interface utilisateur interactive de la visualisation des événements, fournit un tableau de bord intégré de gestion de la sécurité incorporant un ensemble complet d'outils d'analyse et de visualisation en temps réel qui facilitent la détection et l'analyse des menaces. Les utilisateurs peuvent surveiller les événements en temps réel et effectuer des analyses approfondies instantanées sur les dernières secondes écoulées à plusieurs heures. Des graphiques et des outils de visualisation permettent de surveiller les informations. De nombreux formats de graphiques sont disponibles : 3D à barres, des graphiques empilés 2D à barres, des graphiques en courbes, des graphiques en rubans et autres. Des informations précieuses supplémentaires peuvent être affichées sur le tableau de bord Active Views, y compris les notifications d'exploitation d'actif (détection d'exploitation), les informations d'actif et les associations graphiques entre IP source et cible pertinents.

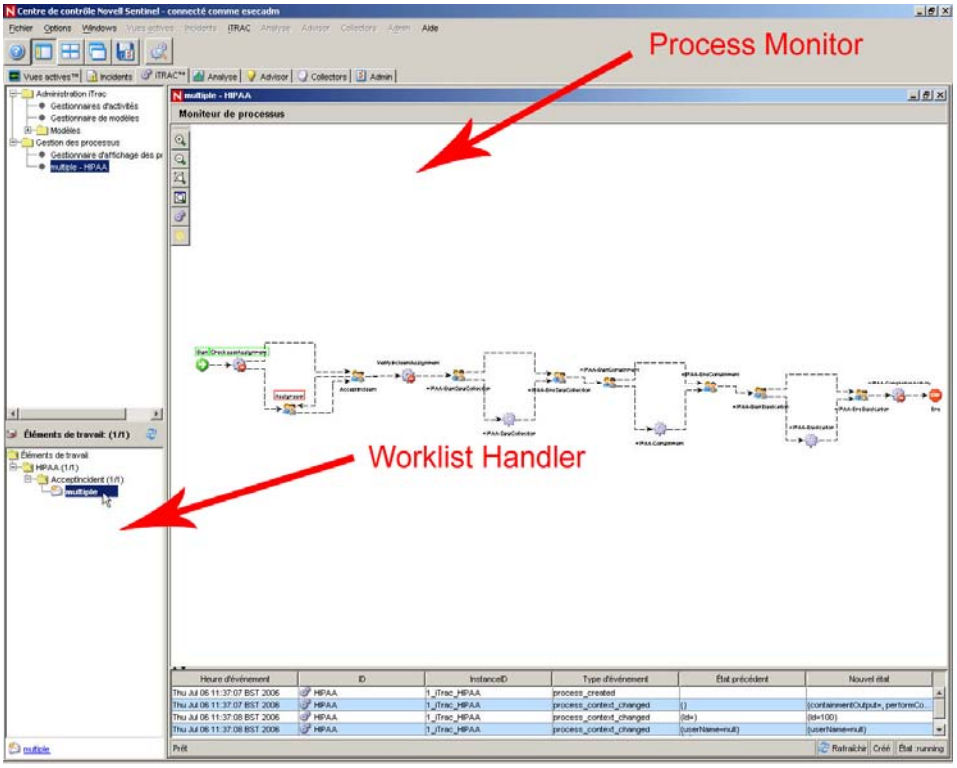
Comme Active Views s'appuie sur l'architecture iSCALE, les analystes approfondir les analyses, car Active Views offre un accès direct aux données d'événement en mémoire en temps réel, qui traite aisément des milliers d'événements par seconde sans dégrader les performances.
Les données sont conservées en mémoire et écrites dans la base de données selon les besoins (avec les charges d'événement habituelles, Active Views peut stocker jusqu'à 8 heures de données en mémoire). Cette vue ininterrompue orientée performances en temps réel est essentielle en cas d'attaque ou en état d'équilibre.



## Réponse aux incidents via iTRAC

Avec iTRAC, la gestion traditionnelle des informations de sécurité passe d'un rôle passif d'alerte et de visualisation à un rôle de réponse aux incidents donnant lieu à une action. En effet, les entreprises peuvent définir et documenter les processus de résolution des incidents puis orienter, mettre en place et suivre ces processus une fois un incident ou une violation détectée.

Sentinel 5 est fourni avec des modèles de processus prêts à l'emploi qui traitent les incidents à l'aide des directives du SANS Institute. Les utilisateurs peuvent commencer par ces processus prédéfinis et configurer des activités spécifiques pour refléter les pratiques recommandées de leur entreprise. Les processus iTRAC peuvent être automatiquement déclenchés à partir de la création d'incidents ou des règles de corrélation, ou manuellement lancés par un professionnel de la sécurité ou de l'audit autorisé. iTRAC conserve un suivi d'audit de toutes les actions pour prendre en charge la génération de rapports de conformité et l'analyse d'historique.




Une liste de travail indique à l'utilisateur toutes les tâches qui lui ont été affectées et un moniteur de processus offre une visibilité en temps réel du statut du processus pendant un cycle de vie de processus de résolution.

Le framework d'activité d'iTRAC permet aux utilisateurs de personnaliser des tâches automatiques ou manuelles pour des processus de résolution d'incident spécifiques. Les modèles de processus d'iTRAC peuvent être configurés à l'aide du framework d'activité pour correspondre aux pratiques recommandées d'une entreprise. Les activités sont exécutées directement à partir du Centre de contrôle Sentinel.

Le framework d'automatisation d'iTRAC fonctionne en utilisant deux composants-clés : le conteneur d'activités et le conteneur de processus de travail. Le premier automatise l'exécution des activités pour l'ensemble d'étapes spécifié en fonction de règles d'entrée et le

second automatise l'exécution du processus de travail en fonction d'activités répertoriées dans une liste. Les règles d'entrées reposent sur le standard XPDL (XML Processing Description Language) et fournissent un modèle formel pour exprimer les processus exécutables dans une entreprise. L'implémentation des règles et de jeux de règles métier étant basée sur des standards, les clients sont assurés de définitions de processus conformes.

### Service Reporting

Le service Reporting permet de générer des rapports, y compris des rapports d'historique et de vulnérabilité. Sentinel 5 est fourni avec des rapports prêts à l'emploi et permet aux utilisateurs de configurer leurs propres rapports à l'aide de Crystal Reports. Sentinel 5 comprend les exemples de rapports suivants, entre autres :

- Analyse des tendances
- Statut de sécurité de lignes d'activité ou d'actifs vitaux
- Types d'attaque
- Actifs visés
- Temps de réponse et résolution
- Violations de la conformité à la stratégie

### Advisor

Sentinel Advisor, un module facultatif, effectue des renvois entre les données d'alerte en temps réel de Sentinel et les vulnérabilités connues et les informations de résolution, ce qui élimine les délais s'écoulant entre la détection d'un incident et la réponse face à l'incident. Avec Advisor, les entreprises peuvent déterminer si des événements exploitent des vulnérabilités spécifiques et la manière dont ces attaques affectent leurs actifs. Advisor comprend également des informations détaillées sur les vulnérabilités que les attaques visent à exploiter, les effets potentiels des attaques réussies et les étapes nécessaires à la résolution. La mise en œuvre
et le suivi des mesures de résolution recommandées sont effectués à l'aide des processus iTRAC de réponse face aux incidents.

### Health

Le service Health permet aux utilisateurs d'obtenir une vue complète de la plate-forme Sentinel 5 distribuée. Il regroupe les informations d'état de santé de divers processus généralement distribués sur divers serveurs. Les informations d'état de santé s'affichent régulièrement sur le Centre
de contrôle Sentinel pour l'utilisateur final.

### Administration

La fonctionnalité Administration offre les outils de gestion des utilisateurs et de configuration des paramètres généralement nécessaires aux administrateurs d'application de Sentinel 5.

### Services communs

Tous les composants de cette couche de logique commerciale de l'architecture décrits ci-dessus sont régis par un ensemble de services communs. Ces services constituent une aide au filtrage précis (via le moteur de filtre) des événements vers les utilisateurs, à la surveillance continue des statistiques d'état de santé du système (via le moniteur d'état de santé) et aux mises à jour dynamiques de données système (via le service d'assignation). Ensemble, ces services sont à la base des services partiellement reliés qui permettent un traitement et une évolution sans pareil via le transport basé sur les bus message pour une analyse et un calcul en temps réel.

# Couche de présentation

La couche de présentation restitue l'interface de l'application à l'utilisateur final. Le Centre de contrôle Sentinel constitue un panneau de bord complet qui présente les informations à l'utilisateur.

# Modules de produit

## Centre de contrôle Sentinel

Le Centre de contrôle Sentinel offre un panneau de bord de gestion de la sécurité intégré et puissant. Des écrans intuitifs permettent aux analystes d'identifier rapidement les nouvelles tendances ou attaques, de manipuler les informations graphiques en temps réel et d'interagir avec ces informations et de répondre aux incidents. Les fonctions clé incluent :

- Active Views : analyse et visualisation en temps réel.
- Incidents : création et gestion des incidents.
- Analyse : définition et gestion de règles de corrélation.
- iTRAC : gestion des processus pour documenter, mettre en œuvre et suivre les processus de résolution d'incident.
- Génération de rapports : rapports et mesures d'historique

## Sentinel Wizard

Sentinel Wizard collecte les données de périphériques source et fournit un flux d'événements plus riche en intégrant une taxinomie, une détection d'exploitation et des données d'entreprise au flux de données avant que les événements ne soient corrélés, analysés et envoyés à la base de données. Un flux d'événements plus riche signifie que les données sont corrélées dans le contexte d'entreprise requis pour identifier et résoudre les menaces internes ou externes et les violations de la stratégie. Dans une configuration quelconque, un ou plusieurs assistants peuvent être déployés, ce qui permet aux clients de déployer des composants de produit dans leur infrastructure en fonction de la topologie de leur réseau.

## Sentinel Advisor

Sentinel Advisor, un module facultatif, effectue des renvois entre les données d'alerte en temps réel de Sentinel et les vulnérabilités connues et les informations de résolution.

# Sommaire

Ce guide contient les chapitres suivants :

- Chapitre 11 : Utilitaires
- Chapitre 12 : Démarrage rapide
- Annexe A : Événements système

# 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
```

# Autres références Novell

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

- Guide d'installation de Sentinel™ 5
- Guide de l'utilisateur de Sentinel™
- Guide de l'utilisateur du composant Wizard de Sentinel™ 5
- Guide des références utilisateur de Sentinel™ 5
- Guide de l'intégration de tiers de Sentinel™ 5
- 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 24h/24 et 7j/7, appelez au numéro suivant : 800-858-4000

# 2 Navigation au sein du Centre de contrôle Sentinel

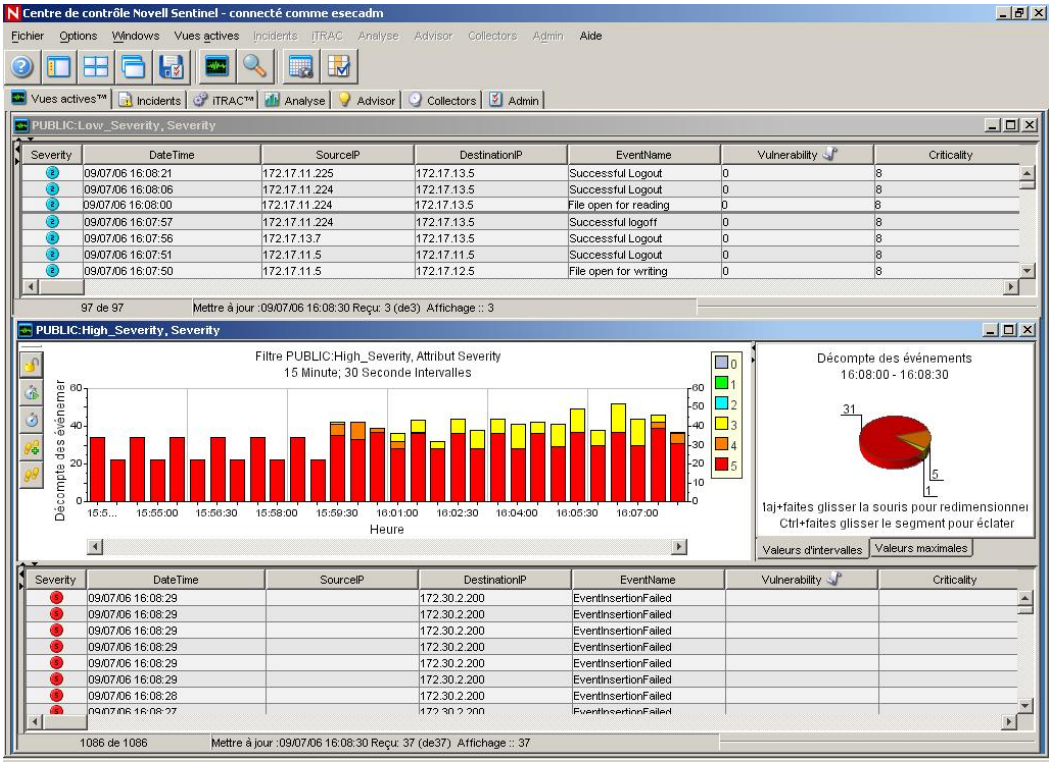
**REMARQUE** : les termes Agent et Collecteur sont interchangeables. Le terme Collecteur sera utilisé dans la suite de cette documentation.

Le Centre de contrôle Sentinel se compose des éléments suivants :

- Barre de menus
- Barre d'outils
- Onglets

En outre, ce chapitre aborde les sujets suivants :

- Démarrage du Centre de contrôle Sentinel
- Changement de l'apparence du Centre de contrôle Sentinel
- Enregistrement des préférences utilisateur
- Changement du mot de passe Sentinel



# Démarrage du Centre de contrôle Sentinel

## Démarrage du Centre de contrôle Sentinel sous Windows

Démarrage de la console Sentinel à partir de Windows

1. Cliquez sur *Démarrer > Novell > Centre de contrôle Sentinel* ou cliquez sur l'icône du *Centre de contrôle Sentinel* sur le bureau.
2. Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur OK.

## Démarrage du Centre de contrôle Sentinel sous UNIX

Démarrage du Centre de contrôle Sentinel sous UNIX

1. En tant qu'utilisateur esecadm, accédez avec la commande cd au répertoire :

   ```
   $ESEC_HOME/sentinel/console
   ```

2. Exécutez la commande suivante :

   ```
   ./run.sh
   ```

3. Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur OK.

# Barre de menus

Sous la barre de titre figurent dix menus. En partant d'en haut à gauche de la fenêtre, ces menus sont : Fichier, Options, Fenêtres, Vues actives, Incidents, iTRAC, Advisor, Collecteurs, Admin et Aide.

Les options des menus Fichier, Options, Fenêtres et Aide sont toujours disponibles. D'autres options sont disponibles en fonction de l'onglet actif et des autorisations dont vous disposez.

## Menu Fichier

- Enregistrer les préférences
- Quitter

## Menu Options

- Changer le mot de passe
- Placement de la tabulation
  - Haut
  - Bas
- Arrimer le navigateur
- Afficher le navigateur

## Menu Fenêtres

- Tout organiser en cascade
- Tout organiser en mosaïque
  - Ajuster en mosaïque
  - Mosaïque horizontale
  - Mosaïque verticale

- Tout réduire
- Tout restaurer
- Tout fermer

### Active Views™

- Propriétés
- Créer une vue active
- Requête d'événement
- Événement en temps réel
  - Instantané
  - Gérer les colonnes

### Incidents

- Afficher le gestionnaire de vues d'incidents
- Créer un incident
- Configuration du visualiseur de pièces jointes

### iTRAC™

- Afficher le gestionnaire de processus

### Analyse

- Créer un rapport

### Advisor

- Créer un rapport

### Collecteurs

- Afficher le Gestionnaire des vues du collecteur

### Admin

- Configuration de rapport
- Règles de corrélation
- Gestionnaire de moteurs de corrélation
- Configuration du filtre global
- Configuration du menu
- Configuration du filtre
- Configuration de l'utilisateur

### Aide

- Aide
- À propos de Sentinel

## Barre de menus

Cinq boutons de barre d'outils système sont affichés en permanence. D'autres boutons s'affichent en fonction de la fenêtre ou de l'onglet actif et des autorisations dont vous disposez.

## Barre d'outils système

Les cinq boutons de barre d'outils système sont les suivants.

-  Afficher l'aide de Sentinel
-  Afficher/Masquer la fenêtre de navigation
-  Afficher toutes les fenêtres en mosaïque
-  Afficher toutes les fenêtres en cascade
-  Enregistrer les préférences utilisateur

## Onglet Active Views™

Lorsque l'onglet ActiveViews™ est actif, les boutons suivants sont disponibles.

-  Active Views
-  Lancer la requête d'événement

### Fenêtre Décompte des événements sur un certain laps de temps

Lorsqu'une fenêtre Décompte des événements sur un certains laps de temps est active, les boutons suivants sont disponibles.

-  Instantané d'une table de décompte des événements sur un certain laps de temps
-  Gestion des colonnes d'une table de décompte des événements sur un certain laps de temps

### Graphique Décompte des événements sur un certain laps de temps

Lorsque le graphique Décompte des événements sur un certain laps de temps est actif, il comprend les boutons suivants.

- Verrouiller/Déverrouiller le graphique
- Augmenter l'intervalle d'affichage
- Réduire l'intervalle d'affichage
- Augmenter le temps d'affichage
- Réduire le temps d'affichage

Lorsque vous cliquez sur le bouton Verrouiller, les boutons suivants sont disponibles :

- Verrouiller/Déverrouiller le graphique
- Augmenter l'intervalle d'affichage
- Réduire l'intervalle d'affichage
- Augmenter le temps d'affichage
- Réduire le temps d'affichage
- Zoom avant

- Zoom arrière
- Hiérarchisation vers le bas vers les événements
- Enregistrer en tant que fichier HTML

### Fenêtre Instantané

Lorsque la fenêtre Instantané est active, les boutons suivants sont disponibles.

-  Gérer les colonnes

## Onglet Incidents

Lorsque l'onglet Incidents est actif, les boutons suivants sont disponibles.

-  Afficher le gestionnaire de vues d'incidents
-  Créer un nouvel incident
-  Configurer les visualiseurs de pièces jointes

### Incident

Lorsqu'un incident est ouvert, les boutons suivants sont disponibles.

-  Gérer les colonnes d’événements associés

## iTRAC

Lorsque l'onglet iTRAC est actif, les boutons suivants sont disponibles.

-  Afficher le gestionnaire d'affichage des processus

## Onglet Analyse et Advisor

Lorsque l'onglet Analyse ou Advisor est actif, les boutons suivants sont disponibles.

-  Créer un rapport

## Onglet Collecteurs

Lorsque l'onglet Collecteurs est actif, les boutons suivants sont disponibles.

-  Afficher le Gestionnaire des vues du Gestionnaire des collecteurs
-  Afficher le Gestionnaire des vues du collecteur

## Onglet Admin

Lorsque l'onglet Admin est actif, les boutons suivants sont disponibles.

-  Afficher la configuration de rapport
-  Afficher les règles de corrélation
-  Afficher le gestionnaire de moteurs de corrélation
-  Afficher la configuration du filtre global
-  Afficher la configuration du menu
-  Afficher le gestionnaire de filtres
-  Afficher le gestionnaire d'utilisateurs
-  Gestionnaire de vues du serveur

### Fenêtre Gestionnaire de filtres

Lorsque la fenêtre Gestionnaire de filtres est active, les boutons suivants sont disponibles.

-  Créer un filtre
-  Supprimer le filtre sélectionné (actif lorsqu'un filtre est sélectionné)

### Menu Configuration du menu

Lorsque la fenêtre Configuration du menu est active et que vous êtes en mode modification, les boutons suivants sont disponibles.

-  Créer un nouvel élément de menu
-  Supprimer l'élément de menu
-  Activer l'élément de menu
-  Désactiver l'élément de menu

# Onglets

Selon les autorisations dont vous disposez, le Centre de contrôle Sentinel affiche les onglets suivants. Vous devez disposer des autorisations appropriées pour pouvoir afficher chaque onglet.

- Active Views™
- Incidents
- iTRAC™
- Analyse
- Advisor
- Collecteurs
- Admin

Pour plus d'informations sur les onglets, reportez-vous au chapitre correspondant à chaque onglet.

# Changement de l'apparence du Centre de contrôle Sentinel

Vous pouvez changer l'apparence du Centre de contrôle Sentinel. Vous pouvez effectuer notamment les opérations suivantes :

- Changer la position des onglets
- Afficher ou masquer la fenêtre de navigation
- Arrimer ou faire flotter la fenêtre de navigation
- Affichage des fenêtres en cascade
- Affichage des fenêtres en mosaïque
- Réduction et restauration de toutes les fenêtres
- Fermeture simultanée de toutes les fenêtres

## Définition de la position des onglets

Pour définir la position des onglets

1. Cliquez sur *Options* > *Placement de la tabulation.*
2. Sélectionnez Haut ou Bas.

## Afficher ou masquer la fenêtre de navigation

Pour afficher ou masquer la fenêtre de navigation

1. Cliquez sur *Options* > *Afficher le navigateur (activé ou désactivé).*

## Arrimer ou faire flotter la fenêtre de navigation

Pour arrimer ou faire flotter la fenêtre de navigation

1. Cliquez sur *Options* > *Arrimer le navigateur (activé ou désactivé).*

## Affichage des fenêtres en cascade

Pour afficher les fenêtres en cascade

1. Cliquez sur Fenêtres > Tout organiser en cascade. Toutes les fenêtres ouvertes du panneau droit s'affichent en cascade.

## Affichage des fenêtres en mosaïque

Pour afficher les fenêtres en mosaïque

1. Cliquez sur Fenêtres > Tout organiser en mosaïque.
2. Sélectionnez, au choix :
   - Ajuster en mosaïque
   - Mosaïque verticale
   - Mosaïque horizontale

## Réduction et restauration de toutes les fenêtres

Pour réduire toutes les fenêtres

1. Cliquez sur Fenêtres > Tout réduire. Toutes les fenêtres ouvertes du panneau droit sont réduites.

## Pour restaurer toutes les fenêtres dans leur taille d'origine

Pour restaurer toutes les fenêtres dans leur taille d'origine

1. Cliquez sur *Fenêtres* > *Tout restaurer*. Toutes les fenêtres ouvertes du panneau droit sont restaurées dans leur taille d'origine.

## Pour restaurer une fenêtre spécifique

To restore an individual window

1. Cliquez sur la fenêtre réduite. La fenêtre est restaurée dans sa taille d'origine.

## Fermeture simultanée de toutes les fenêtres

To close all windows

1. Cliquez sur Fenêtres > Tout fermer.

# Enregistrement des préférences utilisateur

Vous devez disposer de l'autorisation Save Workspace (Enregistrement de l'espace de travail).

Les préférences pouvant être enregistrées sont les suivantes :

- Les fenêtres permanentes, qui peuvent être recréées, car elles ne dépendent pas de données disponibles lors de leur création. Par exemple, les préférences d'affichage de récapitulatif et de vues actives peuvent être enregistrées. Cependant, les fenêtres temporaires (par exemple, les instantanés et les interrogations rapides) ne peuvent pas être enregistrées. Toutes les fenêtres répertoriées dans le navigateur sont enregistrées, mais aucune des fenêtres secondaires que vous ouvrez en double-cliquant sur un élément qu'elles contiennent n'est enregistrée.
- La position des fenêtres.
- La taille des fenêtres, y compris de la fenêtre d'application.
- La position des onglets.
- La fenêtre de navigation arrimée ou flottante et affichée ou masquée.

Pour enregistrer vos préférences

1. Cliquez sur Fichier > Enregistrer les préférences ou sur Enregistrer les préférences.

# Changement du mot de passe du Centre de contrôle Sentinel

**REMARQUE** : pour satisfaire les exigences strictes en matière de configuration de la sécurité certification CC (Common Criteria ou Critères communs), Novell requiert un mot de passe fort doté des caractéristiques suivantes :

1. Choisissez des mots de passe comportant au moins 8 caractères qui incluent 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 pas être un mot (cela ne peut pas être un mot du dictionnaire ni un mot d'argot courant).

4. Votre mot de passe ne doit pas contenir de mot 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 facile à mémoriser et complexe à la fois. Par exemple, Mfa5!As (mon fils a 5 ans) OU J!hb1tE75 (j'habite à Paris).

Pour changer le mot de passe du Centre de contrôle Sentinel

1. Cliquez sur Options > Changer le mot de passe.
2. Entrez l'ancien mot de passe.
3. Entrez le nouveau mot de passe une première fois, puis une deuxième fois pour le vérifier.

**REMARQUE** : Novell recommande vivement d'utiliser des mots de passe comportant au moins 8 caractères, dont des caractères alphanumériques.

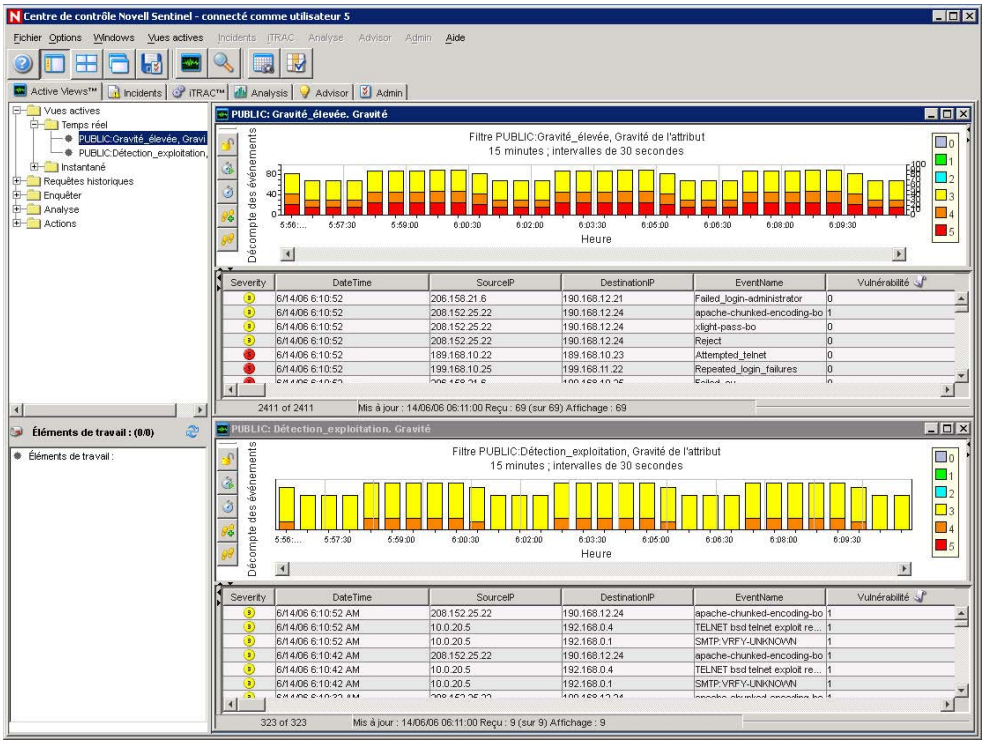
4. Cliquez sur *OK*.

# 3 Onglet Active Views™

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

Vous devez disposer de l'autorisation appropriée pour utiliser l'onglet Active Views™. Si tel n'est pas le cas, aucune autorisation liée aux opérations effectuées à l'aide de cet onglet ne sera disponible.

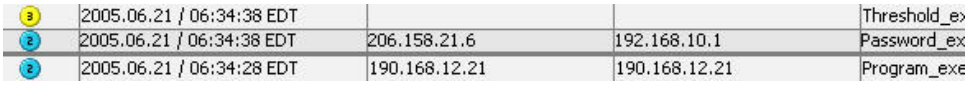
Dans l'onglet Active Views, vous pouvez surveiller, pratiquement en temps réel, les événements à mesure qu'ils se produisent et exécuter des requêtes sur ces événements. Vous pouvez les surveiller dans un tableau ou les représenter sous forme de graphique 3D à barres, de graphique 2D empilé à barres, de graphique en courbes ou en rubans.



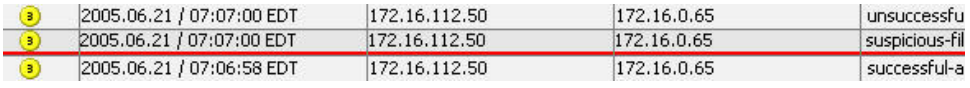

## Onglet Vues actives

Les vues d'événements sont présentées sous forme de tables. La configuration d'une vue active est déterminée par le fichier das_rt.xml. Il existe deux types de vues actives. Une table en temps quasi réel des événements comporte une représentation graphique des événements et un instantané de chaque événement.

- Table en temps quasi réel des événements
  - Cette table peut contenir jusqu'à 750 événements par période de 30 secondes.
  - Par défaut, le client gère les événements mis en cache pour une période de 24 heures. Vous pouvez modifier cette configuration à l'aide des Propriétés de vues actives.
  - Par défaut, la table des événements affiche un maximum de 30 000 événements. Vous pouvez modifier cette configuration à l'aide des Propriétés de vues actives.
  - Par défaut, la table des événements est rafraîchie toutes les 30 secondes (délai d'envoi). Ceci est représenté par une ligne grise dans la table des événements.




Lorsqu'il y a plus de 750 événements par période de 30 secondes, une ligne rouge de séparation apparaît pour indiquer qu'il y a plus d'événements qu'il n'est affiché.




  - Après que l'utilisateur a enregistré ses préférences, la table continue à recueillir des données pendant 4 jours. Par exemple, si vous enregistrez vos préférences, puis que vous vous déconnectez et vous reconnectez le jour suivant, la vue active affichera les données comme si vous ne vous étiez jamais déconnecté.
  - Si une vue active est créée et non enregistrée, elle continuera à recueillir des données pendant une heure. Si pendant cette période, une vue active identique est créée, cette vue active affichera les données pour l'heure qui vient de s'écouler.
- Instantané : les instantanés sont des vues horodatées d'une table d'événements en temps réel.

Chaque vue active est unique, car elle comporte :

- un filtre qui lui est propre ;
- l'attribut axe z ;
- le filtre de sécurité attribué à l'utilisateur.

L'onglet Vues actives vous permet d'effectuer les opérations suivantes :

- Reconfigurer des vues actives
- Créer un incident
- Fermer un instantané ou une fenêtre du navigateur visuel
- Créer un incident
- Utiliser des options du menu personnalisé avec des événements
- Supprimer un instantané ou une fenêtre du navigateur visuel
- Enquêter sur un ou plusieurs événements
- Assigner des graphiques
- Afficher les données Advisor
- Gérer les colonnes
- Envoyer des messages électroniques sur les événements et les incidents
- Afficher ou masquer les détails des événements
- Prendre un instantané d'une fenêtre du navigateur visuel
- Afficher des événements qui ont déclenché un événement corrélé
- Visualiser des vulnérabilités
- Afficher des données de l'actif
- Utiliser HP OpenView Operations et Service Desk
- Utiliser Remedy

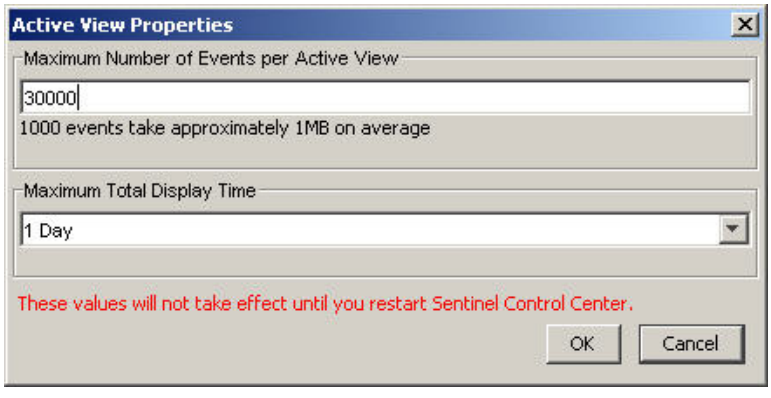
Vous avez la possibilité, en tant qu'utilisateur, de changer les valeurs (le nom des colonnes) pour afficher des noms logiques qui seront utilisés à tous les niveaux du système. Vous pouvez appliquer au flux d'événements des attributs appropriés à votre activité. Pour plus d'informations, reportez-vous au *Chapitre 10 : Gestionnaire de données Sentinel* du *Guide d'utilisation du composant Wizard* et au *Guide des références utilisateur de Sentinel*.

# Reconfiguration du nombre maximal des événements dans les vues actives et de la valeur du cache

Les propriétés des vues actives vous permettent de configurer le nombre maximal d'événements qui peuvent être affichés dans les vues actives et la durée de leur mise en cache. Par défaut, le nombre maximal d'événements dans une vue active est 30 000. La durée de mise en cache par défaut dans une vue active est 24 heures.

Pour reconfigurer le nombre maximal d'événements et la valeur de la mise en cache dans les vues actives

1. Cliquez sur l'onglet Active Views.
2. Cliquez sur Active Views > Propriétés.
3. Changez les valeurs.




Pour que les nouvelles valeurs prennent effet, vous devez redémarrer le Centre de contrôle Sentinel.

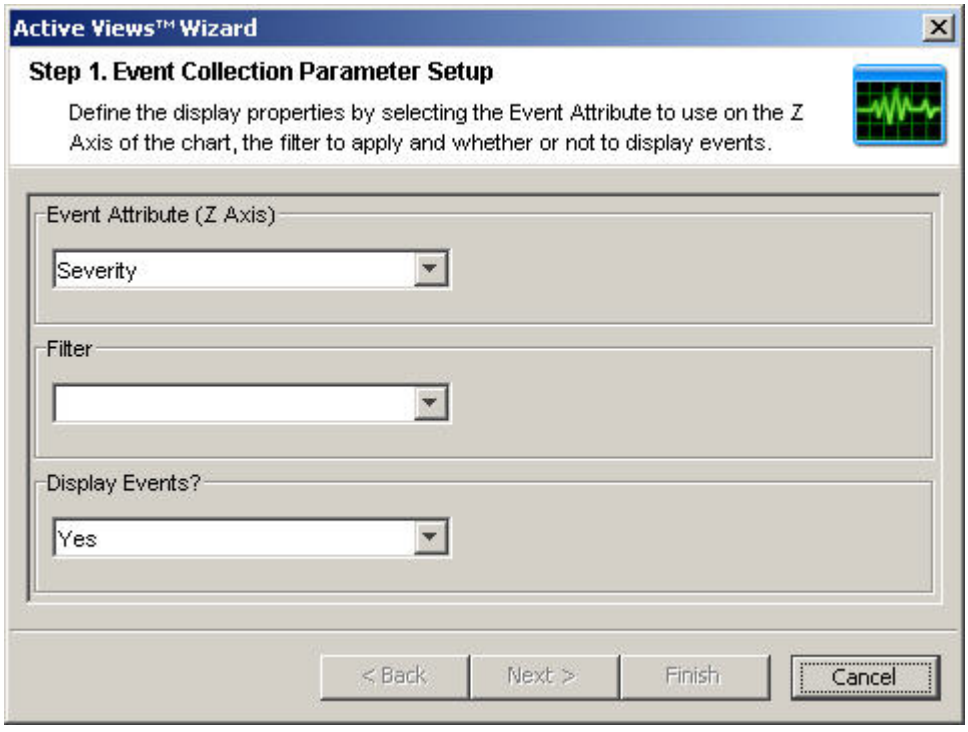
# Pour afficher les événements en temps réel

Pour afficher les événements en temps réel

1. Cliquez sur l'onglet Active Views.
2. Cliquez sur Active Views > Créer une vue active ou cliquez sur Créer une vue active.

3. Dans la fenêtre Assistant de visualisation des événements, cliquez sur les flèches vers le bas pour sélectionner l'attribut axe z, le filtre et l'affichage des événements (Oui ou Non).

**REMARQUE** : dans la fenêtre de sélection de filtres, vous avez la possibilité de créer votre propre filtre ou de sélectionner l'un des filtres déjà créés. Sélectionnez le filtre *Tout* pour que tous les événements apparaissent dans cette fenêtre. Lorsque vous créez une vue active, si le filtre assigné à la vue active est changé ou supprimé après la création de la vue active, la vue active n'est pas modifiée.




Après avoir effectué les sélections appropriées, cliquez sur *Suivant* ou *Terminer*. Si vous cliquez sur *Terminer*, les valeurs par défaut suivantes seront choisies :

- Affichage et taux de rafraîchissement de 30 secondes
- Temps d'affichage de 15 minutes
- Axe Y pour le nombre d'événements
- Type de graphique : empilé 2D à barres

4. Si vous cliquez sur Suivant, cliquez sur les flèches pour sélectionner ce qui suit :
   - Affichage et taux de rafraîchissement : fréquence en secondes à laquelle les événements sont mis à jour
   - Temps d'affichage : durée d'affichage du graphique
   - Axe Y : nombre total d'événements ou nombre d'événements par seconde

   Cliquez sur *Suivant*.
5. Sélectionnez le type du graphique. Cliquez sur Suivant.
   - Type de graphique : 3D à barres, empilé 2D à barres, en courbes ou en rubans

6. En plus de sélectionner un filtre, vous pouvez également affiner votre table d'événements. Choisissez les conditions suivantes :

- Aucun
- est exactement
- n'est pas
- est < (est inférieur à)
- est <= (est inférieur ou égal à)
- est > (est supérieur à)
- est >= (est supérieur ou égal à)
- contient
- ne contient pas
- est vide
- n'est pas vide

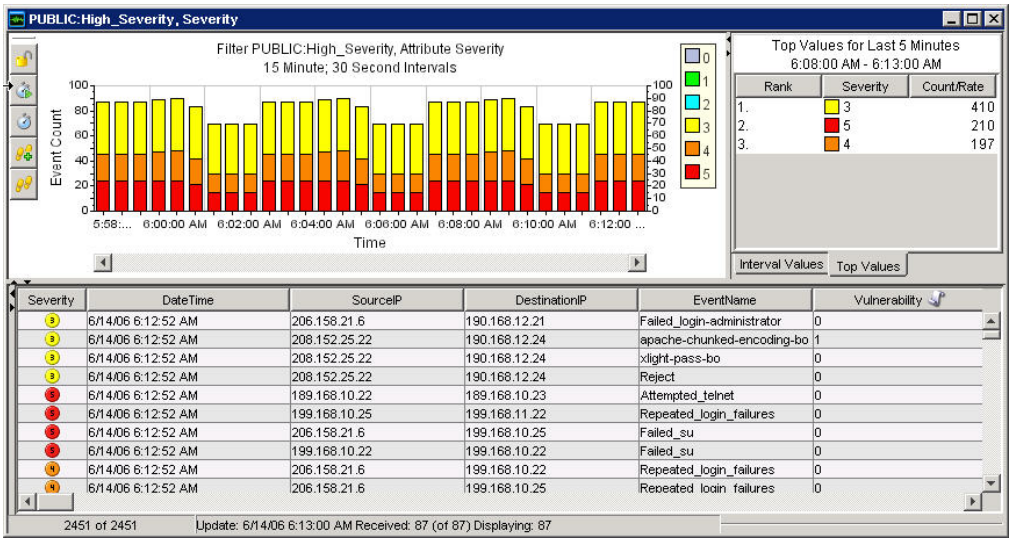
Une fois que vous avez créé vos critères, cliquez sur *Ajouter à la liste*. Cliquez sur *Terminer*.

---

**REMARQUE** : après avoir créé la vue, vous pouvez modifier ou supprimer les critères d'affinement de la table des événements en cliquant avec le bouton droit dans la zone de graphique, puis en sélectionnant des propriétés. Pour plus d'informations, reportez-vous à Pour redéfinir les paramètres, le type des graphiques ou la table des événements d'une vue active.

---

Le graphique est semblable à celui-ci :




---

**REMARQUE** : propriétés de la vue active : la fonction Affiner la table des événements ne modifie en rien la représentation graphique.

---

Les cinq boutons à gauche du graphique effectuent les fonctions suivantes :

- Verrouiller/déverrouiller le graphique : utilisé pour effectuer une analyse, un zoom avant, un zoom arrière, un zoom sur une sélection et enregistrer un graphique en tant que fichier HTML.

- Augmenter l'intervalle d'affichage : augmente l'intervalle du temps d'affichage des événements entrants.

- Réduire l'intervalle d'affichage : réduit l'intervalle du temps d'affichage des événements entrants.

- Augmenter le temps d'affichage : augmente l'intervalle de temps sur l'axe x.

- Réduire le temps d'affichage : réduit l'intervalle de temps sur l'axe x.

Lorsque vous cliquez sur le bouton *Verrouiller*, les boutons suivants sont disponibles :

- Verrouiller/déverrouiller le graphique : utilisé pour effectuer une analyse,
- un zoom avant, un zoom arrière, un zoom sur une sélection et enregistrer
- un graphique en tant que fichier HTML.

- Zoom avant : permet d'effectuer des zooms avant sans changer les paramètres de temps du graphique

- Zoom arrière : permet d'effectuer des zooms arrière sans changer les paramètres de temps du graphique

- Zoom sur la sélection : permet d'effectuer un zoom sur les intervalles de temps des événements sélectionnés.

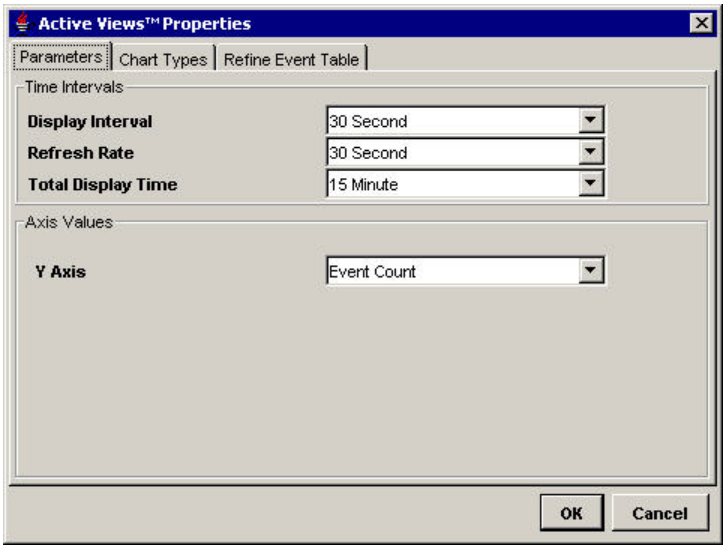
- Enregistre les détails du navigateur dans un fichier HTML avec les graphiques sous forme d'images et les événements sous forme de table.

## Pour redéfinir les paramètres, le type des graphiques ou la table des événements d'une vue active

Lorsque vous affichez une vue active, vous pouvez redéfinir les paramètres et le type des graphiques et, si la vue ne contient que des événements qui vous intéressent, vous pouvez filtrer d'autres événements sans avoir besoin de créer une autre vue active et de filtrer les événements.

Pour redéfinir les paramètres, le type des graphiques ou la table des événements d'une vue active

1. Dans une vue active comportant un graphique, cliquez avec le bouton droit et sélectionnez Propriétés.

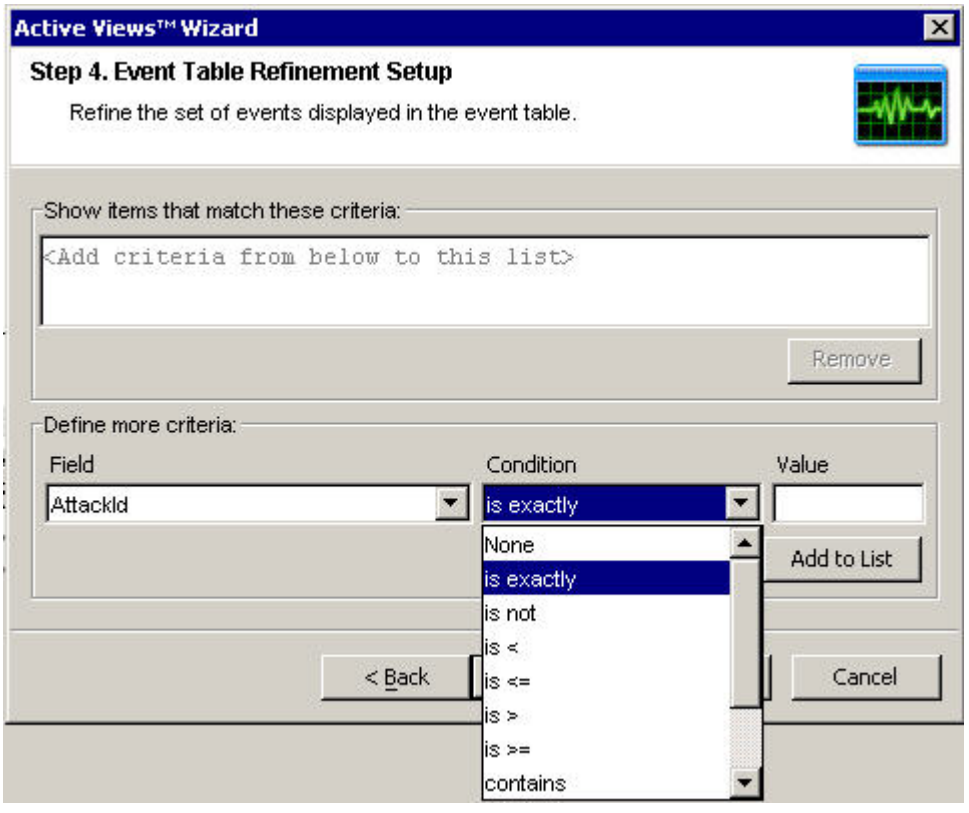



Sous l'onglet Paramètres, vous pouvez définir :

- Afficher l'intervalle : la durée entre chaque intervalle
- Taux de rafraîchissement : fréquence en secondes à laquelle les événements sont mis à jour
- Temps d'affichage total : durée d'affichage du graphique
- Axe Y : nombre total d'événements ou nombre d'événements par seconde

Sous l'onglet Types de graphiques, vous pouvez sélectionner un graphique à barres 3D, un graphique empilé à barres 2D, un graphique en courbes ou en rubans.


L'onglet Affiner la table des événements vous permet de filtrer le champ des événements dans la vue active.



Par exemple, vous pouvez filtrer les événements en indiquant une entrée spécifique dans Champ, par exemple DeviceAttackName est exactement Back_Door_Probe (TCP 3128). Il en résulte une table avec des événements contenant uniquement DeviceAttackName équivalant à Back_Door_Probe (TCP 3128).

| | | |
|---|---|---|
| 206.158.21.6 | 192.168.10.25 | TCP_back_door_probe |
| 206.158.21.6 | 192.168.10.25 | TCP_back_door_probe |
| | | |
| f 564) | (DeviceAttackName is exactly Back_Door_Probe (TCP 3128)) | |

Lorsque vous affinez une table d'événements, les critères du filtre apparaissent en bas à droite de la table.

## Faire pivoter un graphique 3D à barres ou un graphique en rubans

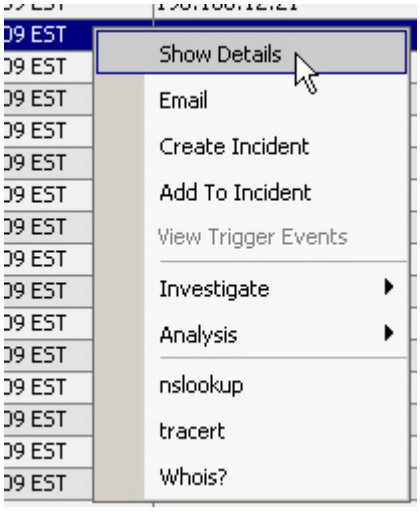
Pour faire pivoter un graphique 3D à barres ou un graphique en rubans

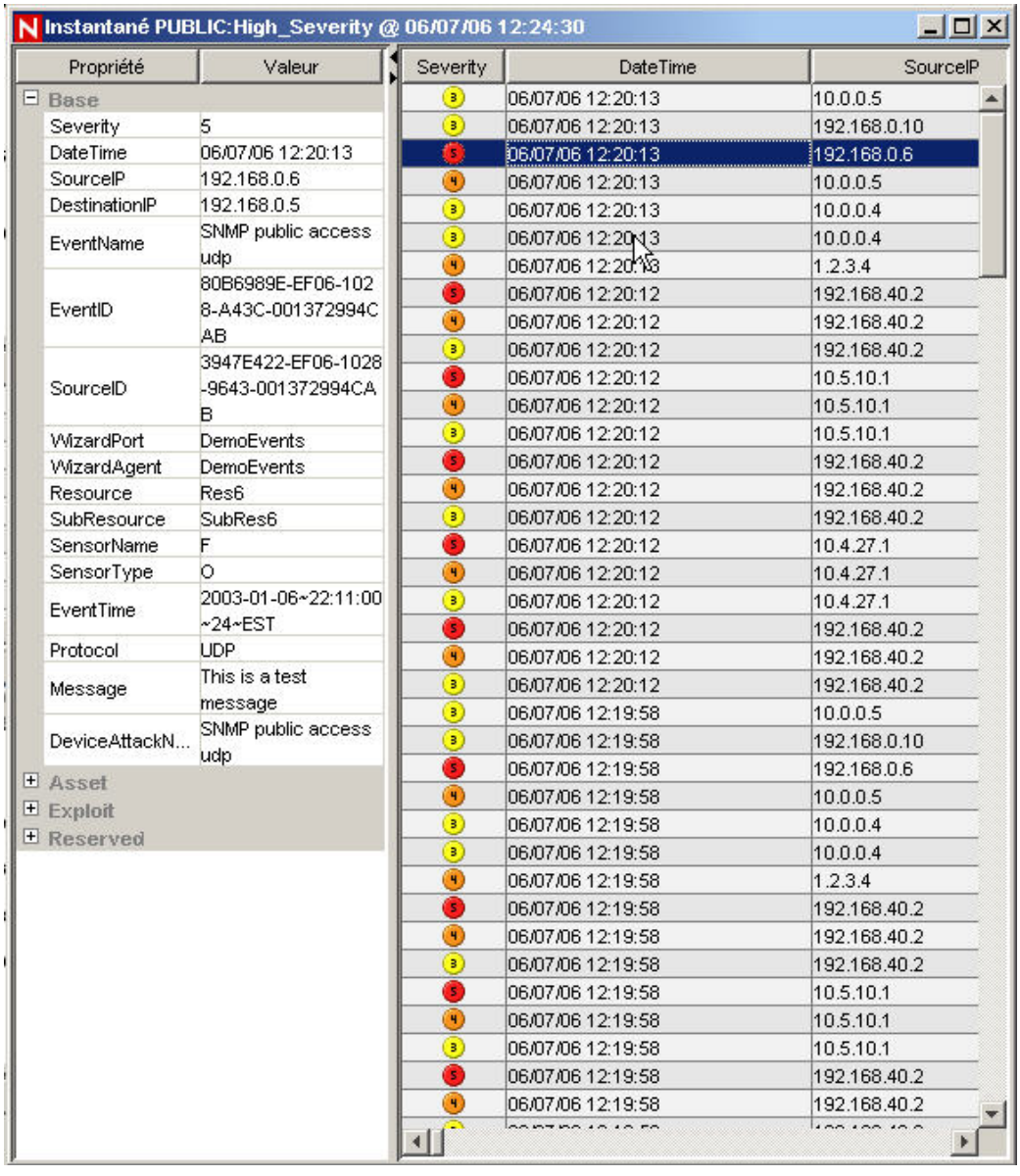
1. Cliquez n'importe où dans le graphique et maintenez enfoncé le bouton droit de la souris.
2. Repositionnez le graphique comme vous le souhaitez en déplaçant la souris tout en maintenant son bouton droit enfoncé.

# Afficher et masquer les détails des événements

Pour afficher les détails des événements

1. In an Event Real Time table of the Visual Navigator or Snapshot, double-click or right-click an event and click Show Details. Les détails d'un événement s'afficheront dans le panneau de gauche de la table en temps réel des événements.






2. Si vous voulez que les détails s'affichent la prochaine fois que vous ouvrez le Centre de contrôle Sentinel, cliquez sur Fichier > Enregistrer les préférences ou cliquez sur Enregistrer les préférences utilisateur.

Pour masquer les détails des événements

1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, dont les détails sont affichés dans le panneau de gauche, cliquez avec le bouton droit sur un événement, puis cliquez sur Afficher les détails. La fenêtre des détails de l'événement se ferme.
2. Si vous ne voulez pas que les détails s'affichent la prochaine fois que vous ouvrez le Centre de contrôle Sentinel, cliquez sur Fichier > Enregistrer les préférences ou cliquez sur Enregistrer les préférences utilisateur.

# Envoi de messages électroniques sur les événements et les incidents

La fonctionnalité d'envoi de courriers électroniques est activée dans le fichier execution properties lors de l'installation. Ce fichier, qui est modifiable après l'installation, est situé aux
emplacements suivants:

Sous Windows :

```
%ESEC_HOME%\sentinel\config
```

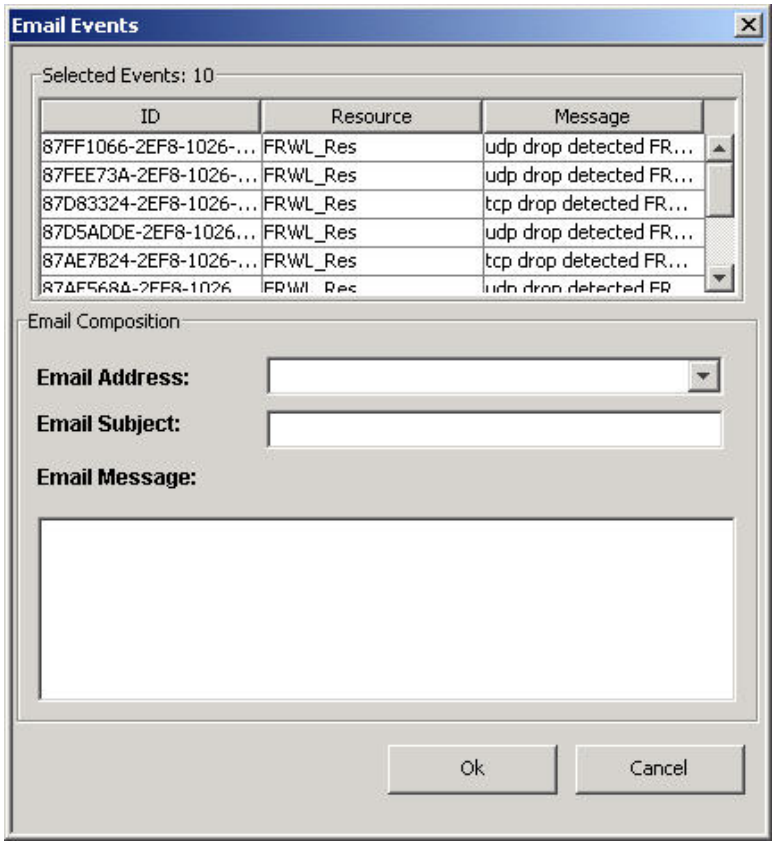
Sous UNIX :

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

Pour plus d'informations, reportez-vous à la section consacrée à la configuration de la messagerie  Sentinel du Chapitre 11 : *Utilitaires.*

Pour envoyer un message concernant un événement par message électronique

1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, sélectionnez un événement ou un groupe d'événements, cliquez avec le bouton droit sur celui-ci, puis sélectionnez Courrier électronique.




2. Entrez les informations suivantes :
   - Adresse électronique
   - Objet du message électronique
   - Message électronique
3. Cliquez sur OK.

Pour envoyer un message concernant un incident par message électronique

1. Après avoir enregistré l'incident, cliquez sur l'onglet Incidents, puis sur Incidents > Afficher le gestionnaire de vues d'incidents.
2. Double-cliquez sur All Incidents (Tous les incidents).
3. Double-cliquez sur un incident.
4. Double-cliquez sur Incident de message électronique  .
5. Entrez :
   - Adresse électronique
   - Objet du message électronique
   - Message électronique
6. Cliquez sur OK. Le message électronique comportera une pièce jointe au format HTML qui répertorie les détails de l'incident, les informations relatives aux événements, aux actifs, aux vulnérabilités et à l'Advisor ainsi que l'historique de l'incident.

# Création d'un incident

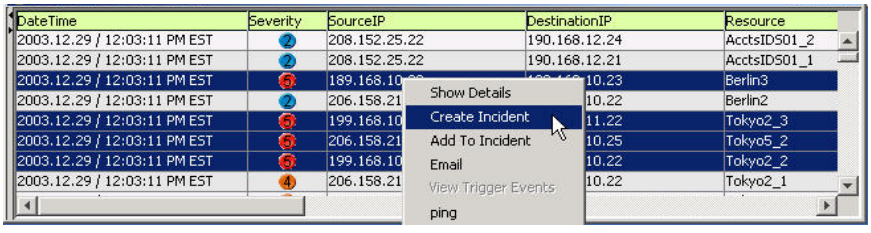
Vous devez disposer de l'autorisation Create Incident(s) (Création d'incidents) pour pouvoir utiliser cette fonction.

Cette fonction permet de regrouper des événements en un ensemble présentant un intérêt particulier (un groupe d'événements similaires ou un ensemble d'événements différents qui correspondent à un sujet particulier, par exemple une attaque).

**REMARQUE** : si les événements ne sont pas affichés dans un nouvel incident, cela est probablement dû à un décalage entre l'affichage des événements dans la fenêtre des événements en temps réel et leur insertion dans la base de données. Si cela se produit, l'insertion des événements d'origine dans la base de données et l'affichage de l'incident peuvent prendre quelques minutes.

Pour créer un incident

1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, sélectionnez un événement ou un groupe d'événements, cliquez avec le bouton droit sur celui-ci, puis sélectionnez Créer un incident.




La fenêtre Nouvel incident comporte les onglets suivants :

- Événements : indique les événements qui constituent l'incident.
- Actifs : affiche les actifs concernés par l'incident.
- Vulnérabilité : affiche les vulnérabilités d'actifs associées à l'incident.
- Advisor : affiche les informations sur les alertes et sur les attaques des actifs.
- Workflow : cet onglet vous permet d'assigner un processus de travail (iTrac).
- Historique : affiche l'historique de l'incident.
- Pièces jointes : vous pouvez joindre à l'incident des documents ou des fichiers texte comportant des informations pertinentes.

Dans la boîte de dialogue Créer un incident, entrez ce qui suit :

- Titre
- État
- Gravité
- Priorité
- Catégorie
- Responsable : compte d'utilisateur assigné à l'incident.
- Description
- Résolution

2. Cliquez sur Enregistrer. L'incident est ajouté sous l'onglet Incidents du Centre de contrôle Sentinel.

# Affichage des événements qui ont déclenché un événement corrélé

Pour afficher les événements qui ont déclenché un événement corrélé, vous devez cliquer avec le bouton droit sur un événement corrélé. Dans la table des événements dans laquelle vous sélectionnez l'événement, consultez le panneau récapitulatif, situé à droite, dont la propriété SensorType a la valeur C (C : événement corrélé) ou W (W : liste de surveillance).

Pour afficher les événements qui ont déclenché un événement corrélé

1. Dans une table en temps réel des événements du navigateur visuel, de l'instantané ou d'une requête d'événement, cliquez avec le bouton droit sur un événement corrélé, puis sélectionnez Afficher les événements déclencheurs. Une fenêtre s'ouvre affichant les événements qui ont déclenché la règle de corrélation, ainsi que le nom de cette règle.


# Enquêter sur un ou plusieurs événements

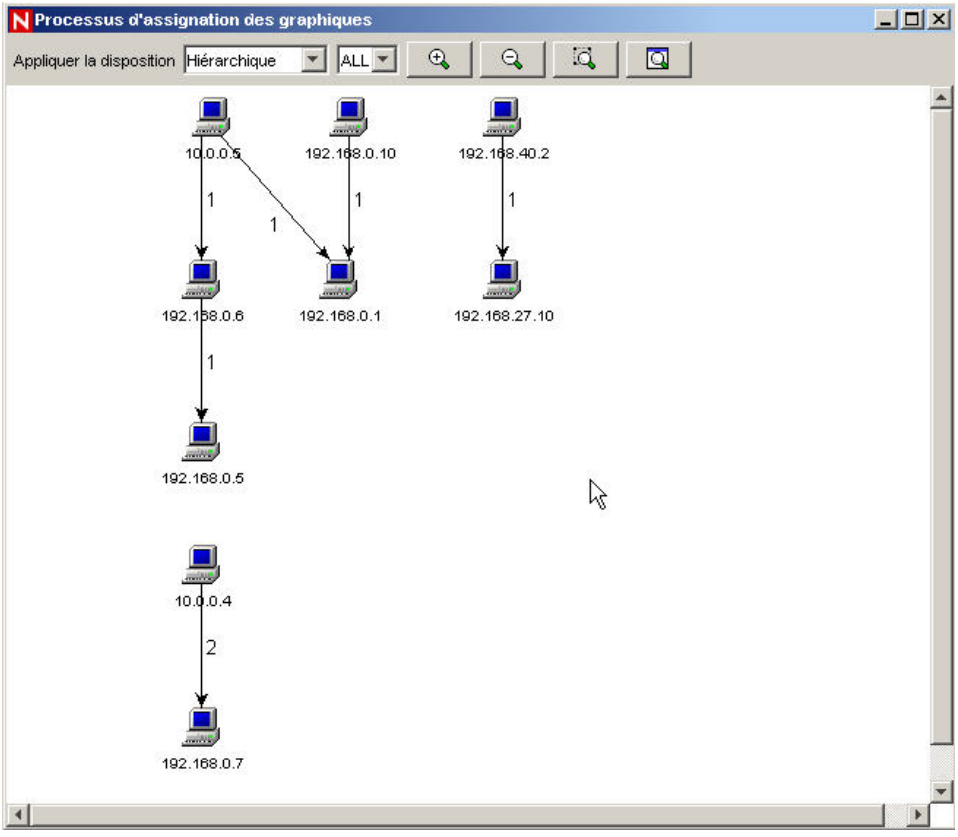
Cette fonction vous permet d'effectuer les actions suivantes :

- Afficher sous forme de graphique les champs source (IP, port, événement, type de capteur, nom du collecteur, etc.) assignés aux champs cibles (IP, port, événement, type de capteur, nom du collecteur, etc.) des événements sélectionnés.
- Réaliser une requête d'événement portant sur la dernière heure d'un événement :

**REMARQUE** : une requête ne peut pas porter sur un champ null (vide).

  - Adresses IP cibles
  - Adresses IP source
  - Nom de l'événement

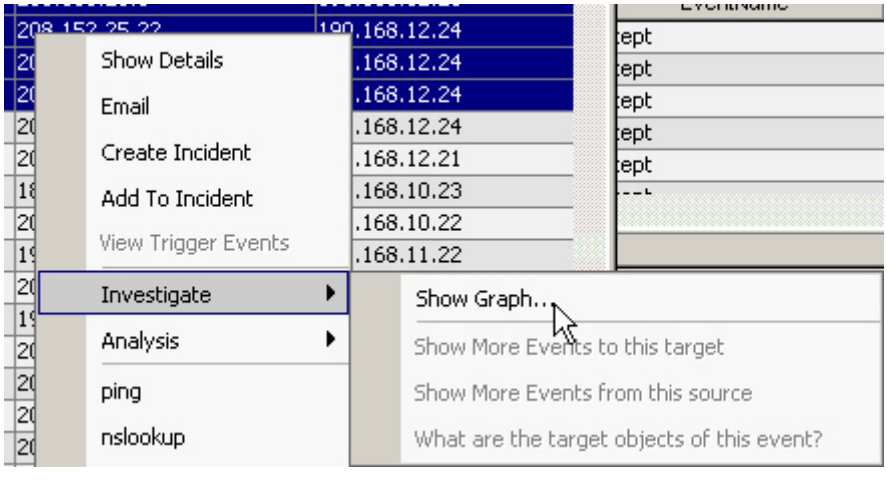
Voici une illustration de la correspondance entre les adresses IP source et les adresses IP cibles.




## Fonctionnalité Enquêter : Processus d'assignation des graphiques

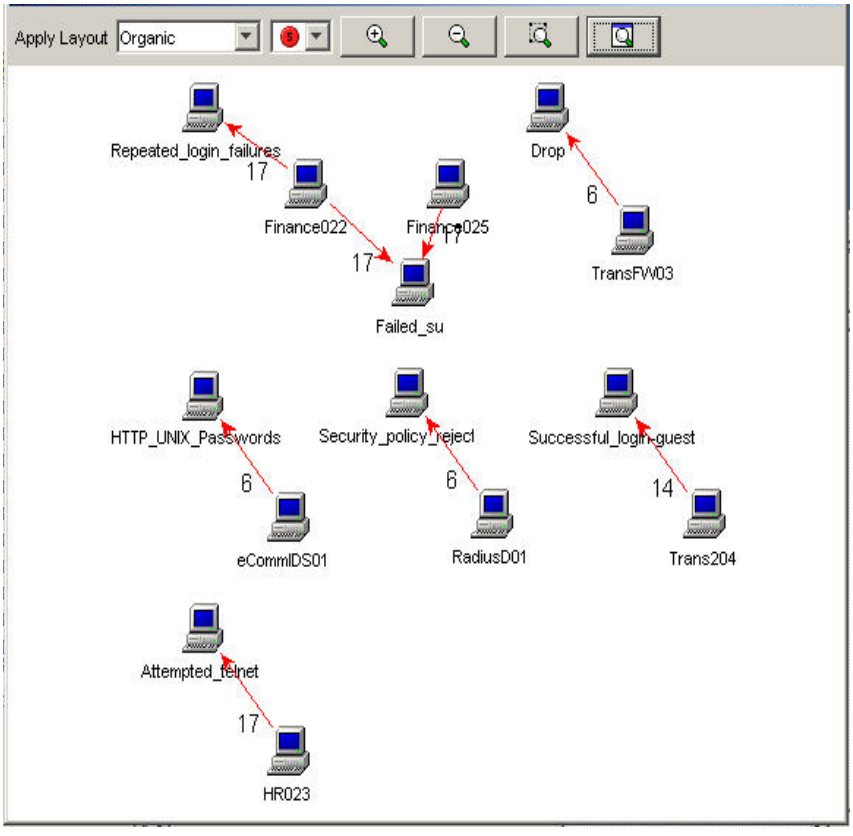
Pour créer une assignation de graphique

1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, cliquez avec le bouton droit sur un ou plusieurs événements > Enquêter > Afficher le graphique.



Voici une représentation graphique du nom du capteur en nom d'événement de gravité 5 en disposition organique. Vous pouvez afficher un graphique dans quatre formats différents :

- Circulaire
- Hiérarchique
- Organique
- Orthogonal




## Fonctionnalité Enquêter : Requête d'événement

Cette fonctionnalité vous permet d'effectuer une requête sur un événement qui s'est produit au cours de l'heure écoulée.

Pour effectuer une requête d'événement avec la fonctionnalité Enquêter

1. Dans une fenêtre de navigateur visuel ou de l'instantané, cliquez avec le bouton droit sur un événement > Enquêter <sélectionnez l'une des trois options suivantes>.

| Option | Fonction |
|---|---|
| Afficher plus d'événements vers cette cible | Adresse IP cible |
| Afficher plus d'événements depuis cette source | Adresse IP source |
| Quels sont les objets cible de cet événement ? | Nom de l'événement |

# Analyse : Affichage des données Advisor

Advisor fait le lien entre les signatures d'attaques IDS en temps réel et sa base de connaissances de vulnérabilités. Les données de flux Advisor reçoivent des données relatives aux alertes et aux attaques. Le flux de données d'alerte contient des informations sur les vulnérabilités et les

virus alors que le flux de données d'attaque répertorie les exploitations associées aux vulnérabilités.

Les systèmes de détection d'intrusion pris en charge sont les suivants :

- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- ISS BlackICE PC Protection
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server Sensor
- ISS RealSecure Guard
- Snort/Sourcefire
- Symantec ManHunt
- Symantec Intruder Alert
- McAfee IntruShield

Le collecteur IDS alimente le champ DeviceAttackName (rt1) d'un événement. Advisor utilise ces informations pour générer des informations relatives aux attaques et aux vulnérabilités. Voici quelques exemples de vulnérabilités :

- FINGER : Cfinger Search Probe (sonde de recherche Cfinger)
- SMTP : SmartServer3 MAIL FROM Buffer Overflow (débordement de mémoire tampon de SmartServer3 MAIL FROM)
- HTTP : Dragon Fire IDS Web Interface Remote Execution (exécution à distance de l'interface Web Dragon Fire IDS)
- FTP :MKDIR-DOS
- hp-printer-flood (inondation d'imprimante HP)
- wh00t-backdoor (`porte dérobée` wh00t)
- nt-telnet
- FINGER / tentative d'exécution
- tellurian-tftpdnt-filename-bo
- FTP MKD Stack Overflow (dépassement de pile FTP MKD)

Pour afficher les données Advisor

1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, cliquez avec le bouton droit sur un événement ou une série d'événements > Analyse > Données Advisor. Si le champ DeviceAttackName est correctement rempli, un rapport similaire à celui présenté ci-dessous s'affiche. L'exemple suivant concerne une attaque de vol de cookie nommée WEB-MISC amazon 1-click.


# Analyse : Affichage des données de l'actif

Cette fonctionnalité vous permet d'afficher les données relatives à un actif et d'enregistrer ces données dans un rapport d'actif au format HTML. Pour afficher ces données, vous devez exécuter le collecteur de gestion d'actifs. Vous pouvez afficher les données suivantes :

**Matériel**

- Adresse MAC
- Nom
- Type
- Fournisseur
- Produit
- Version
- Valeur
- Sévérité
- Sensibilité
- Environnement
- Emplacement

**Réseau**

- Adresse IP
- Nom d'hôte

**Logiciel**

- Nom
- Type
- Fournisseur
- Produit
- Version

**Contacts**

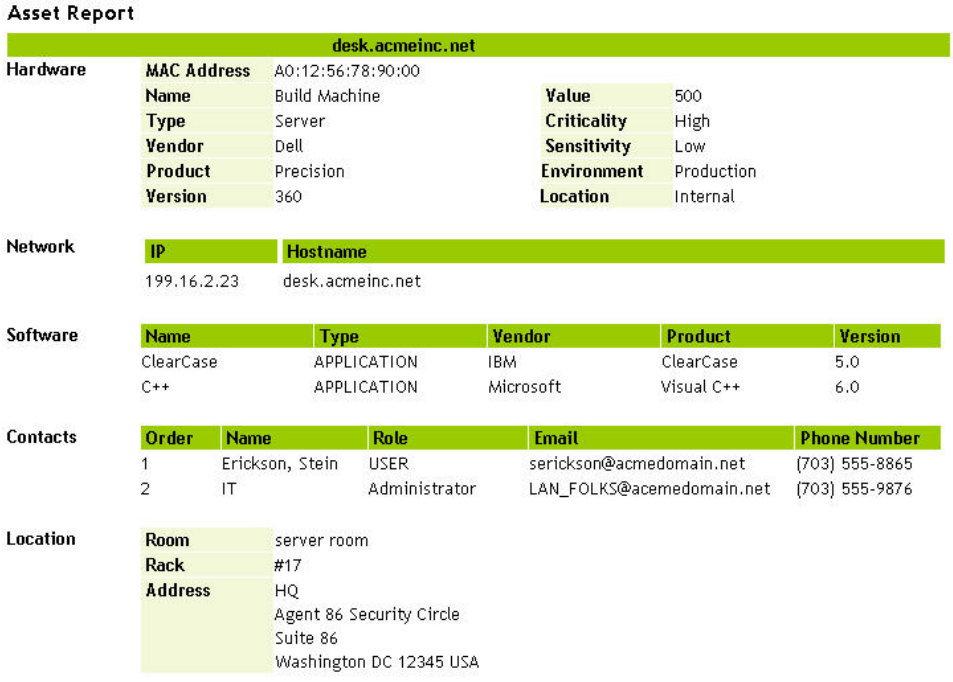
- Ordre
- Nom
- Rôle
- Adresse électronique
- Numéro de téléphone

**Emplacement**

- Salle
- Rack
- Adresse

Pour afficher des données d'actif

1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, cliquez avec le bouton droit sur un ou plusieurs événements > *Analyse* > *Données de l'actif*. Une fenêtre similaire à celle ci-dessous apparaît.



**Asset Report**

| | | | | | |
|---|---|---|---|---|---|
| | **desk.acmeinc.net** | | | | |
| **Hardware** | **MAC Address** | A0:12:56:78:90:00 | | | |
| | **Name** | Build Machine | **Value** | 500 | |
| | **Type** | Server | **Criticality** | High | |
| | **Vendor** | Dell | **Sensitivity** | Low | |
| | **Product** | Precision | **Environment** | Production | |
| | **Version** | 360 | **Location** | Internal | |

| | | |
|---|---|---|
| **Network** | **IP** | **Hostname** |
| | 199.16.2.23 | desk.acmeinc.net |

| | | | | | |
|---|---|---|---|---|---|
| **Software** | **Name** | **Type** | **Vendor** | **Product** | **Version** |
| | ClearCase | APPLICATION | IBM | ClearCase | 5.0 |
| | C++ | APPLICATION | Microsoft | Visual C++ | 6.0 |

| | | | | | |
|---|---|---|---|---|---|
| **Contacts** | **Order** | **Name** | **Role** | **Email** | **Phone Number** |
| | 1 | Erickson, Stein | USER | serickson@acmedomain.net | (703) 555-8865 |
| | 2 | IT | Administrator | LAN_FOLKS@acemedomain.net | (703) 555-9876 |

| | | |
|---|---|---|
| **Location** | **Room** | server room |
| | **Rack** | #17 |
| | **Address** | HQ<br>Agent 86 Security Circle<br>Suite 86<br>Washington DC 12345 USA |

# Analyse : Visualisation des vulnérabilités

Novell est doté de collecteurs capables de traiter les analyses de vulnérabilités réalisées avec Nessus, ISS, Foundstone, eEye et Qualys. La fonctionnalité de visualisation des vulnérabilités fournit une représentation graphique des données d'événements en temps réel sur des systèmes vulnérables. Vous pouvez afficher les données de vulnérabilité d'un événement en cours ou d'un événement qui s'est produit à l'heure spécifiée.

Cette fonctionnalité récupère et affiche les données de vulnérabilité relatives à l'adresse IP cible des événements sélectionnés. Pour plus d'informations, reportez-vous à la documentation consacrée au collecteur, disponible au format PDF à l'emplacement suivant : %ESEC_HOME%\wizard\elements\<nom collecteur>\doc. L'un des collecteurs d'analyses doit être chargé et actif pour obtenir des données de vulnérabilité.

**REMARQUE** : le collecteur de vulnérabilités est un collecteur d'informations et non un collecteur d'événements.

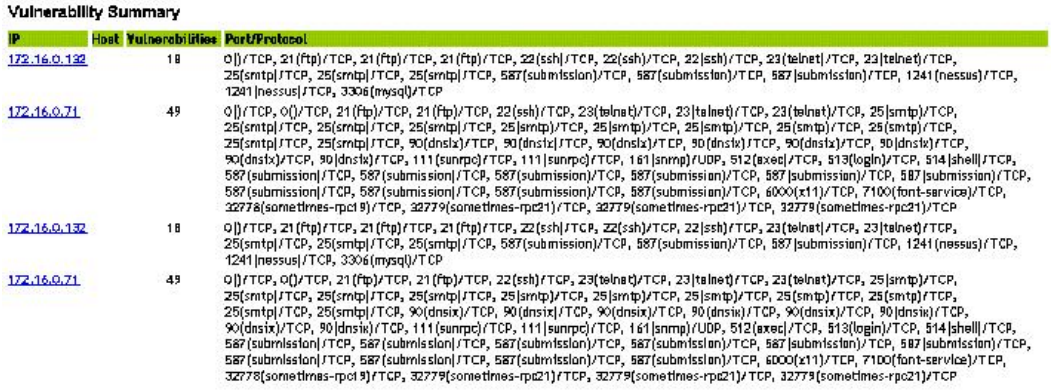
Vous pouvez visualiser les données de vulnérabilité dans les formats suivants :

- HTML
- Graphique
  - Circulaire (organique)
  - Hiérarchique
  - Tous
  - Événements mappés en nœuds
  - Orthogonal

La vue HTML a l'aspect d'un rapport :

- IP
- Hôte
- Vulnérabilité
- Port/Protocole

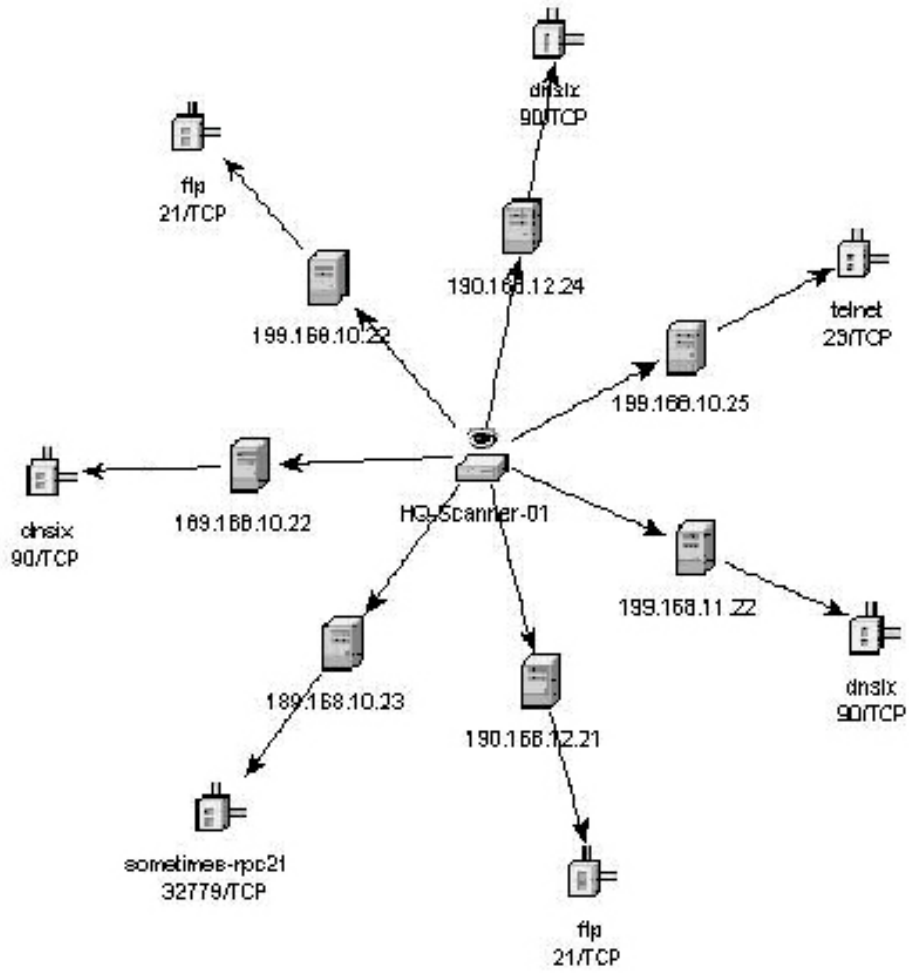
Voici un exemple d'analyse Nessus.



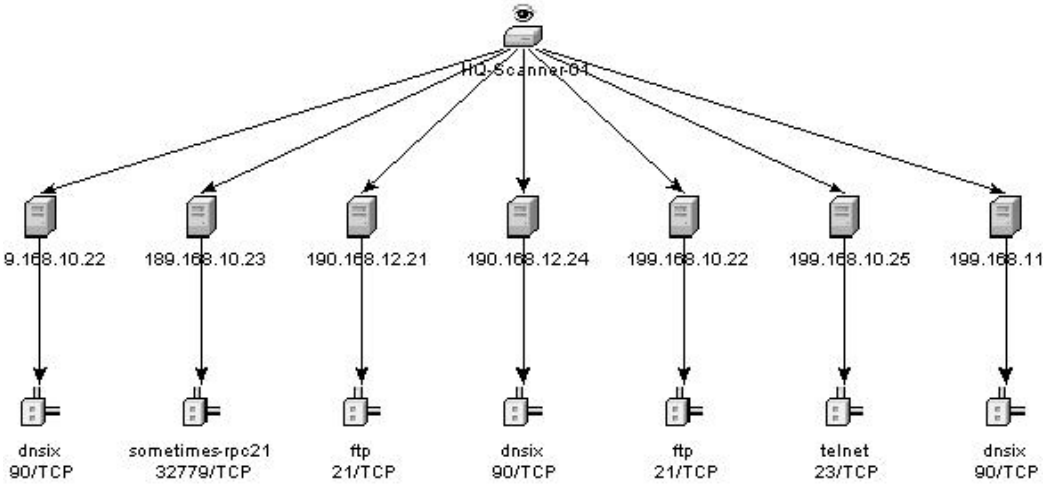
**Vulnerability Summary**

| IP | Host | Vulnerabilities | Port/Protocol |
|---|---|---|---|
| 172.16.0.132 | | 18 | 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 22(ssh)/TCP, 22\|ssh)/TCP, 23(telnet)/TCP, 23\|telnet)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 587(submission)/TCP, 587(submission)/TCP, 587\|submission)/TCP, 1241(nessus)/TCP, 1241\|nessus)/TCP, 3306(mysql)/TCP |
| 172.16.0.71 | | 49 | 0()/TCP, 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 23(telnet)/TCP, 23\|telnet)/TCP, 23(telnet)/TCP, 25\|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25\|smtp)/TCP, 25\|smtp)/TCP, 25\|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90\|dnsix)/TCP, 90\|dnsix)/TCP, 90\|dnsix)/TCP, 111(sunrpc)/TCP, 111\|sunrpc)/TCP, 161\|snmp)/UDP, 512(exec\|/TCP, 513(login)/TCP, 514\|shell\|/TCP, 587(submission\|/TCP, 587(submission\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587(submission)/TCP, 587\|submission)/TCP, 587\|submission)/TCP, 587(submission\|/TCP, 587(submission\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 6000(x11)/TCP, 7100(font-service)/TCP, 32778(sometimes-rpc19)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP |
| 172.16.0.132 | | 18 | 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh\|/TCP, 22(ssh)/TCP, 22\|ssh)/TCP, 23(telnet\|/TCP, 23\|telnet)/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587\|submission)/TCP, 1241(nessus)/TCP, 1241\|nessus\|/TCP, 3306(mysql)/TCP |
| 172.16.0.71 | | 49 | 0()/TCP, 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 23(telnet)/TCP, 23\|telnet)/TCP, 23(telnet)/TCP, 25\|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25\|smtp)/TCP, 25\|smtp)/TCP, 25\|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90\|dnsix)/TCP, 90\|dnsix)/TCP, 90\|dnsix)/TCP, 111(sunrpc)/TCP, 111\|sunrpc)/TCP, 161\|snmp)/UDP, 512(exec\|/TCP, 513(login)/TCP, 514\|shell\|/TCP, 587(submission\|/TCP, 587(submission\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587(submission)/TCP, 587\|submission)/TCP, 587\|submission)/TCP, 587(submission\|/TCP, 587(submission\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 6000(x11)/TCP, 7100(font-service)/TCP, 32778(sometimes-rpc19)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP |

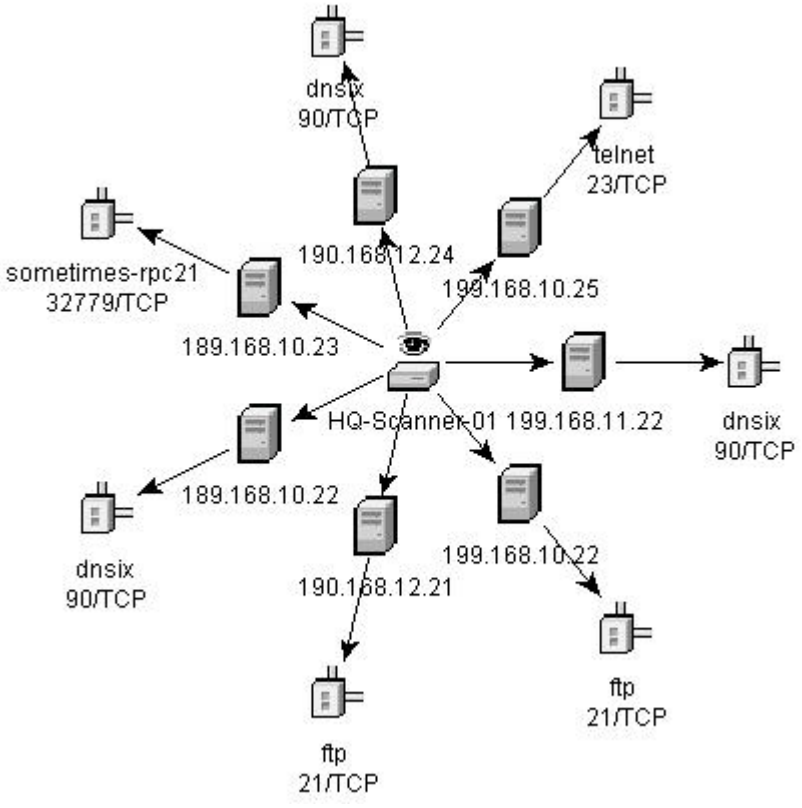
L'affichage graphique permet de visualiser la manière dont les vulnérabilités sont liées à un événement émanant d'un port commun. Voici quatre exemples de vues disponibles.


dnsix
90/TCP
ftp
21/TCP
190.168.12.24
199.168.10.22
telnet
23/TCP
199.168.10.25
dnsix
90/TCP
189.168.10.22
HQ-Scanner-01
199.168.11.22
dnsix
90/TCP
189.168.10.23
190.168.12.21
sometimes-rpc21
32779/TCP
ftp
21/TCP

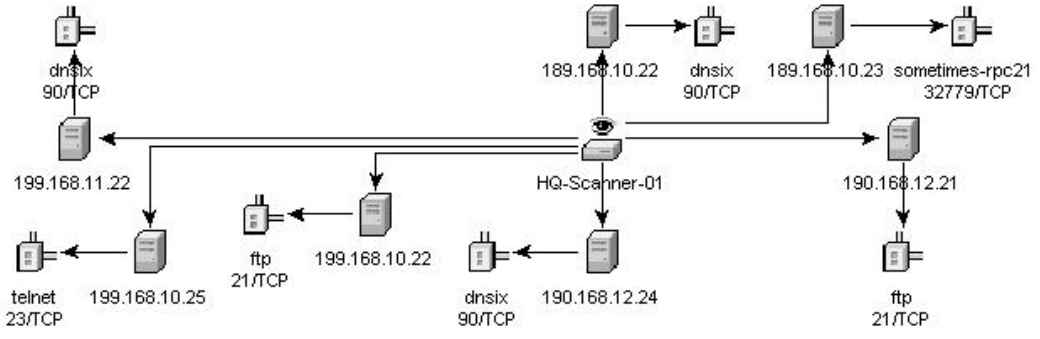
**Organique**


HQ-Scanner-01
9.168.10.22
189.168.10.23
190.168.12.21
190.168.12.24
199.168.10.22
199.168.10.25
199.168.11
dnsix
90/TCP
sometimes-rpc21
32779/TCP
ftp
21/TCP
dnsix
90/TCP
ftp
21/TCP
telnet
23/TCP
dnsix
90/TCP

**Hiérarchique**




**Circulaire**




**Orthogonal**

Un affichage graphique se compose de quatre volets. Ces types sont les suivants :

- Volet graphique
- Arborescence
- Volet de contrôle
- Volet des détails/événements

Le volet d'affichage associe les vulnérabilités à la combinaison port/protocole d'une ressource (adresse IP). Par exemple, si une ressource fait l'objet de cinq combinaisons port/protocole uniques vulnérables, cinq nœuds seront liés à cette ressource. Les ressources sont regroupées sous le nom
du programme d'analyse qui les a analysées et a signalé les vulnérabilités. Si deux programmes d'analyse différents sont utilisés (ISS et Nessus), deux nœuds indépendants comporteront les vulnérabilités qui leur sont associées.

**REMARQUE** : l'assignation d'événements ne se produit qu'entre les événements sélectionnés et les données de vulnérabilité renvoyées.

Dans l'arborescence, les données obéissent à la même hiérarchie que celle des graphiques. L'arborescence permet également aux utilisateurs d'afficher ou de masquer les nœuds à n'importe quel niveau de la hiérarchie.

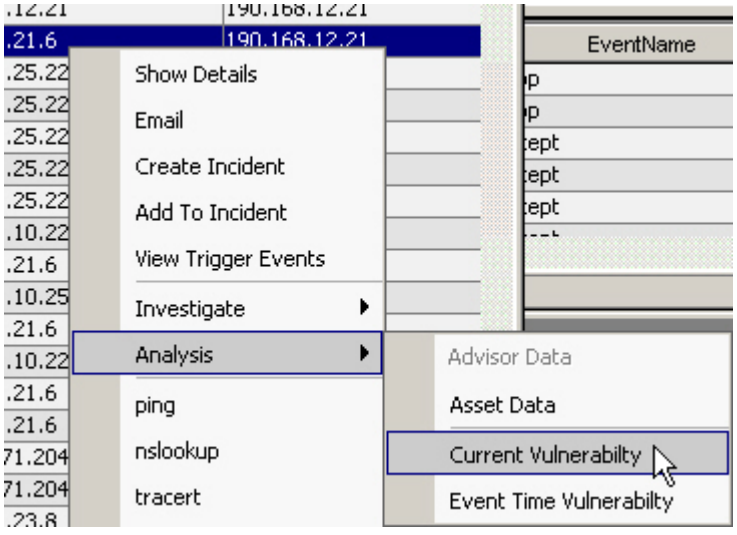
Le volet de contrôle donne accès à toutes les fonctionnalités de l'affichage. Cela inclut :

- les quatre algorithmes différents à afficher,
- la possibilité d'afficher tous les nœuds ou uniquement ceux auxquels des événements sont assignés,
- la possibilité d'effectuer des zooms avant et arrière sur les zones sélectionnées du graphique.

Le volet des détails/événements comporte deux onglets. Lorsque l'onglet Détails est sélectionné, le fait de cliquer sur un nœud affiche les détails qui lui sont associés. Lorsque l'onglet Événements est sélectionné, le fait de cliquer sur un événement associé à un nœud affiche le nœud sous forme
de tableau dans une fenêtre Événement en temps réel ou Requête d'événement.

Pour obtenir une visualisation des vulnérabilités

1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, cliquez avec le bouton droit sur un événement ou une série d'événements, puis cliquez sur :
   - Analyse
     - Vulnérabilité actuelle : interroge la base de données en vue de rechercher les vulnérabilités actives à la date et à l'heure actuelles.
     - Vulnérabilité d'heure d'événement : interroge la base de données en vue de rechercher les vulnérabilités actives à la date et à l'heure où l'événement sélectionné s'est produit.




2. Au bas de la fenêtre des résultats de la requête, cliquez sur l'une des options suivantes :
   - Événement du graphique de vulnérabilité
   - Rapport des vulnérabilités
3. (Pour Événement du graphique de vulnérabilité) Au sein de l'affichage, vous pouvez effectuer les opérations suivantes :
   - Déplacer les nœuds et leurs étiquettes
   - Afficher le graphique avec l'un des quatre algorithmes de présentation proposés
   - Afficher tous les nœuds ou uniquement ceux auxquels des événements sont assignés
   - Filtrer l'arborescence lorsque les résultats comportent un nombre important de ressources vulnérables
   - Effectuer un zoom avant et arrière sur les zones sélectionnées

# Intégration de tiers

Grâce à l'intégration de tiers, vous pouvez envoyer des événements d'un affichage, y compris des incidents et les objets associés, vers l'un des deux logiciels tiers suivants :

- HP Service Desk
- Remedy

Pour envoyer un ou plusieurs événements vers un logiciel tiers

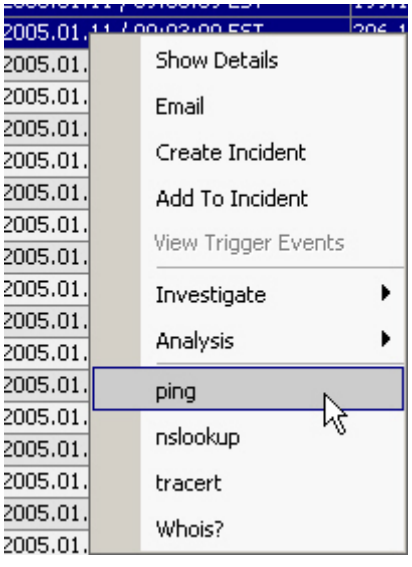
1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, selon le logiciel tiers installé, cliquez avec le bouton droit sur un événement, puis cliquez sur Envoyer l'événement et sélectionnez l'une des destinations suivantes :
   - HP Service Desk
   - Remedy

# Utilisation des options du menu personnalisé avec des événements

Pour appliquer une option du menu personnalisé sur des événements

1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, sélectionnez un événement ou un groupe d'événements, cliquez avec le bouton droit sur celui-ci, puis sélectionnez une option. Une boîte de dialogue s'ouvre. Elle contient les informations relatives à l'option de menu ou vous permet de sélectionner les informations requises pour effectuer une action. Les options par défaut du menu personnalisé sont les suivantes :
   - ping
   - nslookup
   - traceroute
   - Whois?

   Vous pouvez également assigner une autorisation utilisateur pour afficher les vulnérabilités et exécuter des opérations HP. Vous pouvez ajouter des options à partir de la fenêtre Configuration du menu disponible depuis l'onglet Admin.

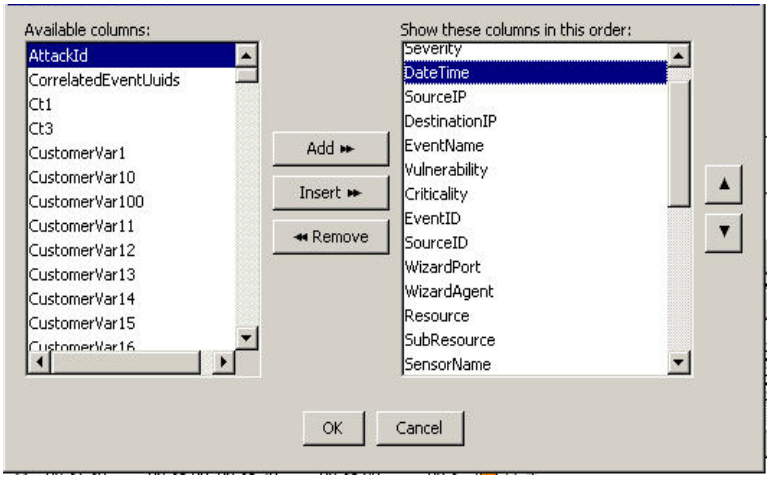



# Gestion des colonnes dans une fenêtre d'instantané ou de navigateur visuel

Pour sélectionner et organiser les colonnes d'une fenêtre d'instantané ou de navigateur visuel

1. Dans une fenêtre d'instantané ou de navigateur visuel, cliquez sur Vue active > Événement en temps réel > Gérer les colonnes ou cliquez sur Gérer les colonnes de la table en temps réel des événements.

2. Avec les boutons Ajouter et Supprimer, déplacez les titres de colonnes entre les listes Colonnes disponibles et Afficher les colonnes dans cet ordre. Vous pouvez utiliser le bouton Insérer pour placer un élément de colonne disponible à un emplacement spécifique. Par exemple, dans l'illustration ci-dessous, cliquer sur Insertion place AttackId au-dessus de DateTime.




Les flèches vers le haut et vers le bas permettent d'organiser l'ordre des colonnes telles que vous voulez qu'elles s'affichent dans la table en temps réel des événements. L'ordre de bas en haut des titres de colonnes de la boîte de dialogue Gérer les colonnes détermine l'ordre de gauche à droite des colonnes dans la table en temps réel des événements.

3. Dans la boîte de dialogue Gérer les colonnes, cliquez sur OK.
4. Si vous voulez que les colonnes s'affichent la prochaine fois que vous ouvrez le Centre de contrôle Sentinel, cliquez sur Fichier > Enregistrer les préférences ou cliquez sur Enregistrer les préférences utilisateur.

# Prise d'un instantané d'une fenêtre de navigateur visuel

Vous devez disposer de l'autorisation Snapshot (Instantané) pour pouvoir utiliser cette fonctionnalité.

Cette fonctionnalité est utile pour analyser les événements présentant un intérêt car le navigateur visuel s'actualise automatiquement et les alertes peuvent ne plus apparaître à moins de faire défiler l'écran. En outre, dans une fenêtre d'instantané, vous pouvez trier les colonnes.

### Pour prendre un instantané d'une table en temps réel des événements

1. Dans une fenêtre de navigateur visuel, cliquez sur Vue active > Événement en temps réel > Instantané ou, dans la barre de menus, cliquez sur Prendre un instantané de la table en temps réel des événements.

Une fenêtre d'instantané s'ouvre et est ajoutée à la liste de dossiers Instantanés sous Event Views (Vues d'événements) dans le navigateur. L'affichage graphique n'est pas inclus dans l'instantané.

## Tri des colonnes d'un instantané

Pour trier les colonnes d'un instantané

1. Cliquez une fois sur un en-tête de colonne pour trier les valeurs dans l'ordre croissant et deux fois pour trier les valeurs dans l'ordre décroissant.

## Fermeture d'un instantané ou d'une fenêtre de navigateur visuel

Pour fermer un instantané ou une table en temps réel des événements

1. Dans une fenêtre d'instantané ou de navigateur visuel, cliquez sur Fichier > Enregistrer les préférences pour que la table soit disponible au prochain démarrage du Centre de contrôle Sentinel.
2. Fermez la table en cliquant sur le bouton Fermer (en haut à droite de la fenêtre sous Windows ou en haut à gauche de la fenêtre sous UNIX).

## Suppression d'un instantané ou d'une fenêtre de navigateur visuel

Pour supprimer un instantané ou une fenêtre de navigateur visuel

1. Dans une fenêtre d'instantané ou de navigateur visuel, fermez la fenêtre en cliquant sur le bouton Fermer (en haut à droite de la fenêtre sous Windows ou en haut à gauche de la fenêtre sous UNIX).
2. Cliquez sur Fichier > Enregistrer les préférences ou sur Enregistrer les préférences utilisateur.

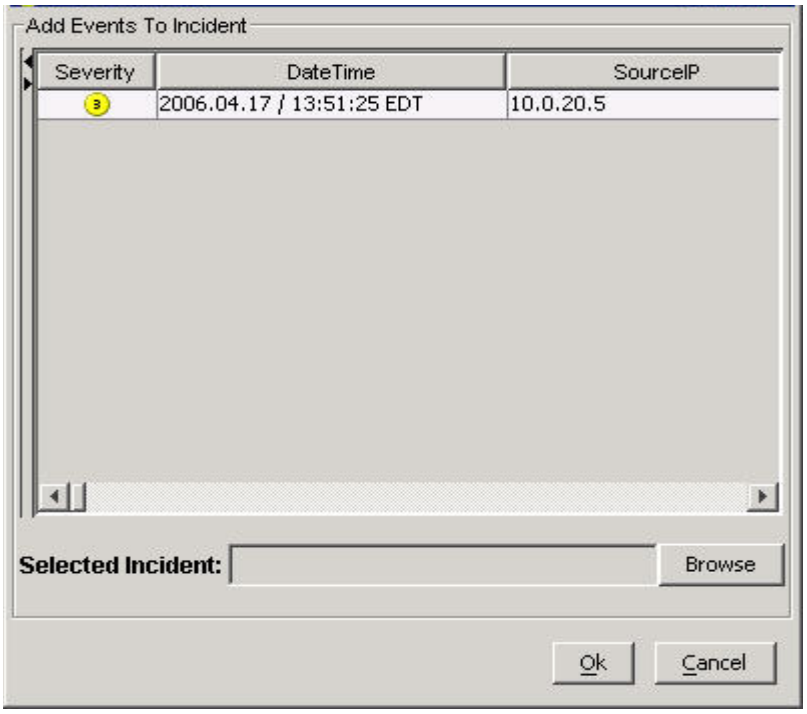
   Après avoir fermé, puis rouvert le Centre de contrôle Sentinel, la vue ou l'instantané ne s'affichera plus.

## Ajout d'événements à un incident

Vous devez disposer des autorisations Modify Incident(s) (Modification d'incidents) et Assign Incident(s) (Assignation d'incidents) pour pouvoir utiliser cette fonctionnalité.

Pour ajouter des événements à un incident

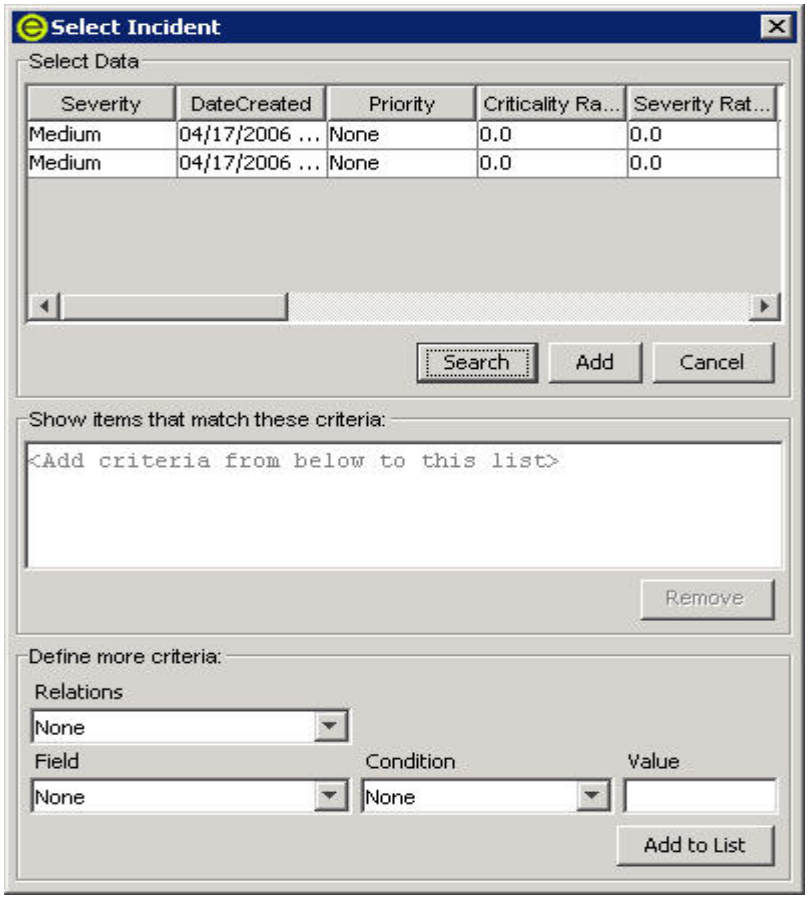
1. Dans une table en temps réel des événements du navigateur visuel ou de l'instantané, sélectionnez un événement ou un groupe d'événements, cliquez avec le bouton droit sur celui-ci pour l'afficher, puis sélectionnez Ajouter à l'incident.
2. Dans la boîte de dialogue Ajouter à l'incident, cliquez sur le bouton Parcourir.




3. Cliquez sur Parcourir pour afficher la liste des incidents disponibles.

**REMARQUE** : vous pouvez définir des critères pour faciliter la recherche d'incidents spécifiques.

4. Cliquez sur Rechercher pour afficher une liste d'incidents.




5. Sélectionnez un incident et cliquez sur Ajouter.
6. Cliquez sur OK. L'événement ou les événements sélectionnés sont ajoutés à l'incident dans la fenêtre de navigation des incidents.

**REMARQUE** : si les événements ne sont pas affichés dans un nouvel incident, cela est probablement dû à un décalage entre l'affichage des événements dans la fenêtre des événements en temps réel et leur insertion dans la base de données. Si cela se produit, l'insertion des événements d'origine dans la base de données et l'affichage de l'incident peuvent prendre quelques minutes.

# 4 Onglet Incidents

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

Vous devez disposer de l'autorisation appropriée pour pouvoir utiliser l'onglet Incidents. Si tel n'est pas le cas, aucune autre autorisation liée aux opérations effectuées à l'aide de cet onglet ne sera disponible.

Ce chapitre traite des incidents. Un incident est constitué d'un ou de plusieurs événements qui présentent un intérêt.

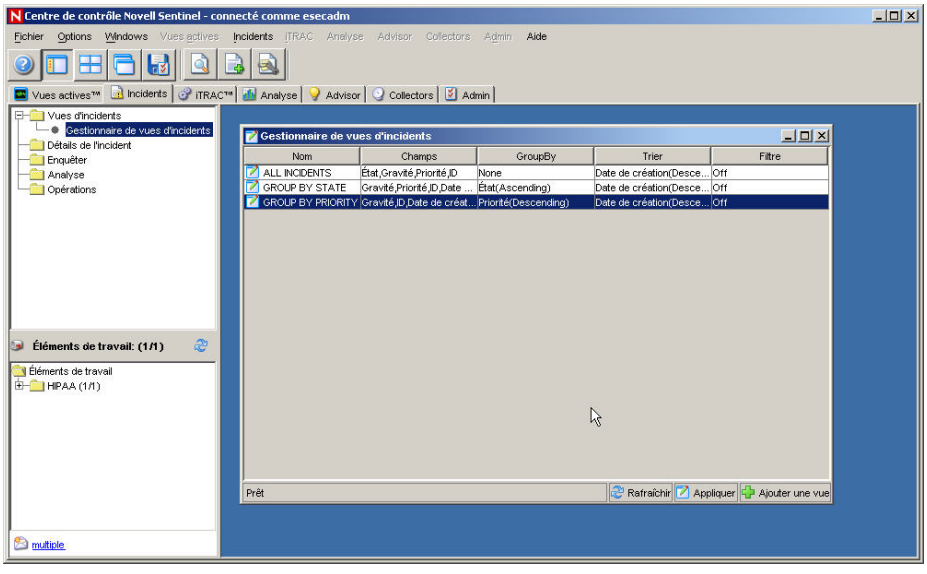
Les incidents peuvent être créés :

- dans la fenêtre Temps réel, vous pouvez sélectionner des événements individuels pour créer un nouvel incident ou les ajouter à un incident existant ;
- automatiquement à partir de règles de corrélation déclenchées.

## Onglet Incidents : Description

Vous pouvez effectuer plusieurs actions sur les incidents :

- Envoi d'un incident par courrier électronique
- Modification d'un incident
- Affichage d'un incident
- Affichage d'un incident
- Ajout d'une vue d'incident



## Relation entre événements et incidents

Un événement est une opération ou une occurrence détectée par un dispositif ou un programme de sécurité. Les événements sont considérés comme « sans état ».

Un incident est constitué d'un ou de plusieurs événements jugés importants (une attaque possible). Les incidents sont associés à des « états » dans la mesure où ils doivent faire l'objet d'une réponse et être fermés.

## Affichage d'un incident

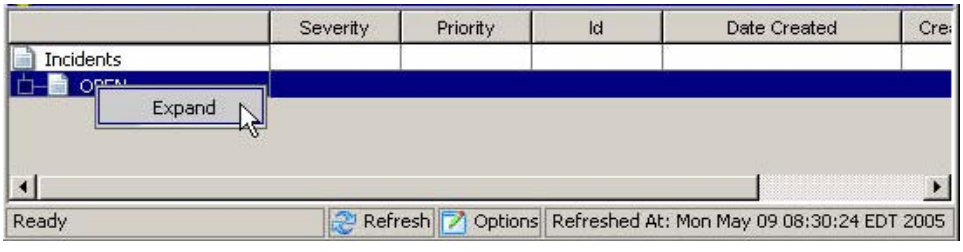
Vous devez disposer de l'autorisation View Incident(s) (Affichage des incidents).

### Pour afficher un incident

1. Cliquez sur l'onglet *Incidents*.
2. Cliquez sur *Incidents* > *Afficher le gestionnaire de vues d'incidents*

   ou sur *Gestionnaire de vues d'incidents*.  .
3. Dans la fenêtre Gestionnaire de vues d'incidents, les vues suivantes sont disponibles :
   - Tous les incidents
   - Regrouper par État
   - Regrouper par Priorité

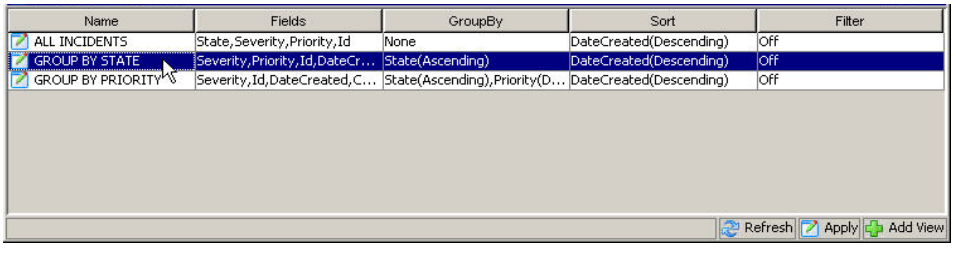
   Double-cliquez sur le nom d'une vue.
4. Cliquez avec le bouton droit > *Agrandir* pour afficher les incidents.



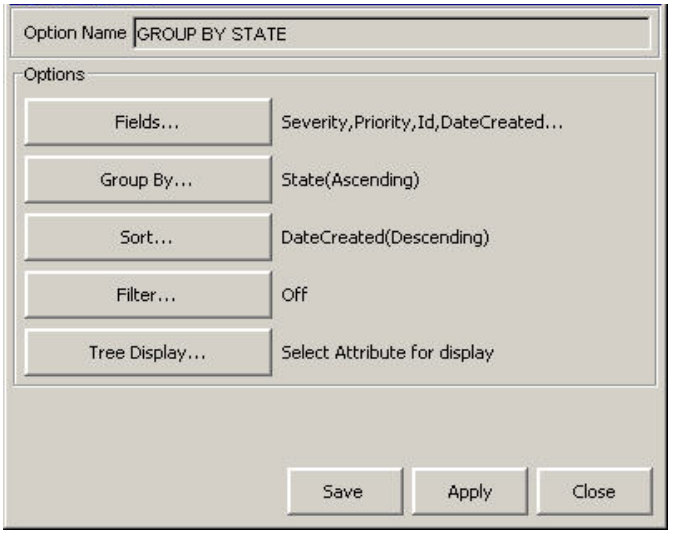

### Pour définir l'option de vue d'un incident

1. Cliquez sur l'onglet *Incidents.*
2. Cliquez sur *Incidents* > *Afficher le gestionnaire de vues d'incidents*

   ou sur *Afficher le gestionnaire de vues d'incidents.*  .
3. Dans la fenêtre Gestionnaire de vues d'incidents, double-cliquez sur le nom d'une vue :



4. Cliquez sur *Options*.

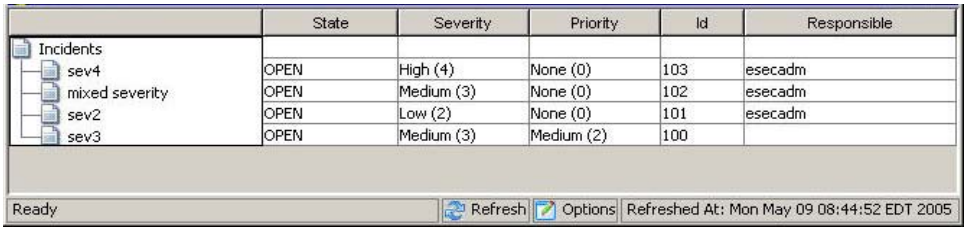

Dans cette fenêtre, vous pouvez également définir les options suivantes :

- Champs...
- Regrouper par...
- Trier...
- Filtre...
- Tree Display (Affichage de l'arborescence)

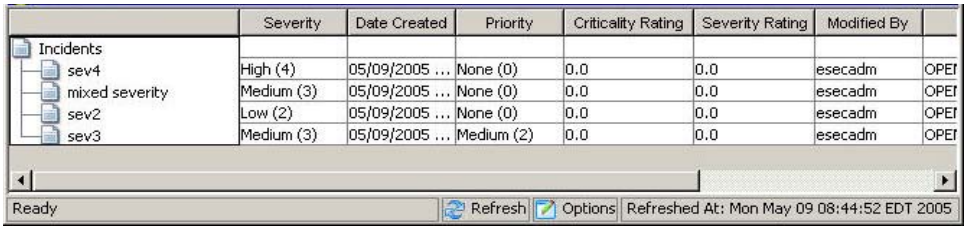
Cliquez sur *Appliquer* puis sur *Enregistrer*.

5. Dans la fenêtre Gestionnaire de vues d'incidents, double-cliquez sur le nom d'une vue :

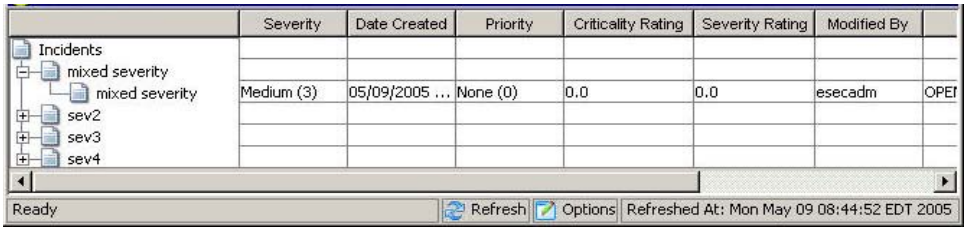
La vue par défaut de la fenêtre Tous les incidents est la suivante.



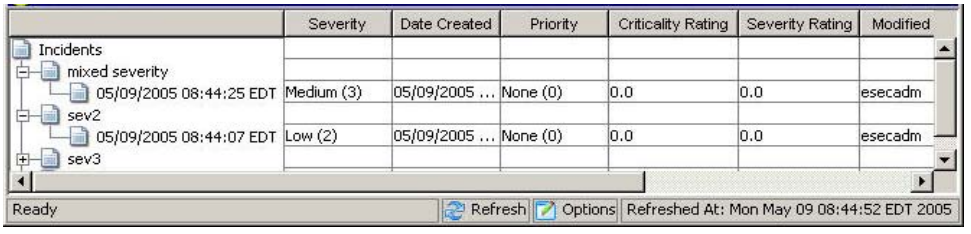

Voici à présent une vue triée par gravité, dont les quatre premières colonnes ont été définies avec l'option Champs (gestion de colonnes) sur Gravité, Date de création, Priorité et Taux de sévérité.




Voici une vue regroupée par titre.




Voici une arborescence triée par date de création.



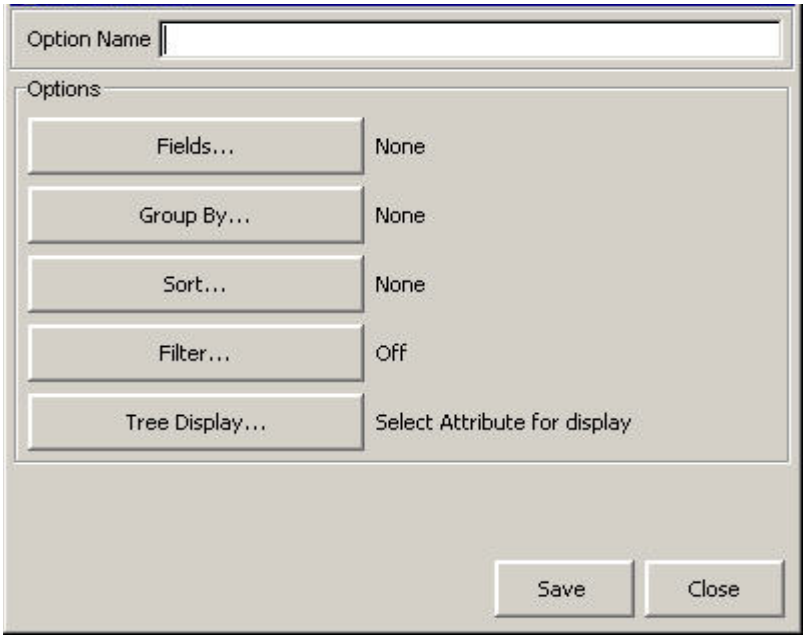

## Ajout d'une vue d'incident

Lorsque vous ajoutez une vue d'incident, plusieurs options sont disponibles :

- Champs...
- Regrouper par...
- Trier...
- Filtre...
- Affichage sous forme d'arborescence

Pour ajouter une vue d'incident

1. Dans le gestionnaire de vues d'incidents, cliquez sur *Ajouter une vue*.




2. Remplissez le champ Nom d'option, sélectionnez les options voulues, puis cliquez sur *Enregistrer*.

## Champs et détails d'incidents

### Champs d'incidents

- Titre : nom de l'incident sélectionné.
- État
  - Open
  - Acknowledged
  - Assigned
  - Investigating
  - False Positive
  - Verified
  - Approved
  - Closed
- Gravité
  - Aucun (0)
  - Trivial (1)
  - Bas (2)
  - Moyen (3)
  - Élevé (4)
  - Grave (5)
- Priorité
  - Faible (1)
  - Moyen (2)
  - Élevé (3)
  - Urgent (4)
  - Top (5)
- Catégorie : (facultatif) champ de saisie de texte qui peut être utilisé pour identifier plus précisément l'incident.
- Responsable : compte d'utilisateur assigné à l'incident.
- Description : champ de saisie de texte.
- Résolution : champ de saisie de texte.

### Détails d'incidents

- Événements : événements associés à l'incident.
- Actifs : liste de tous les actifs associés à l'incident.
- Vulnérabilité : affiche les vulnérabilités associées à l'incident.
- Advisor : affiche les informations concernant l'attaque associées à l'incident.
- Processus de travail : affiche le processus de travail associé à l'incident Sous cet onglet, vous pouvez définir les options suivantes :
  - Aucun
  - Processus de conformité HIPAA
  - Processus SANS Incident Response
  - Processus Sarbanes Oxley FTP Compliance
  - Réponse automatique
- Historique : historique des incidents (liste de toutes les opérations dont un incident a fait l'objet, notamment la date et l'heure de l'intervention de l'utilisateur ainsi que des informations succinctes).
- Pièces jointes : vous pouvez joindre à l'incident des informations pertinentes (des fichiers texte ou des documents).
- Données externes

---

**REMARQUE** : lorsque des événements sont ajoutés à un incident, toutes les données relatives aux actifs, à la vulnérabilité ou à l'Advisor sont ajoutées à l'onglet correspondant (Actifs, Vulnérabilité ou Advisor). Ces données correspondent aux noms DIP/Hôte cible des événements associés.

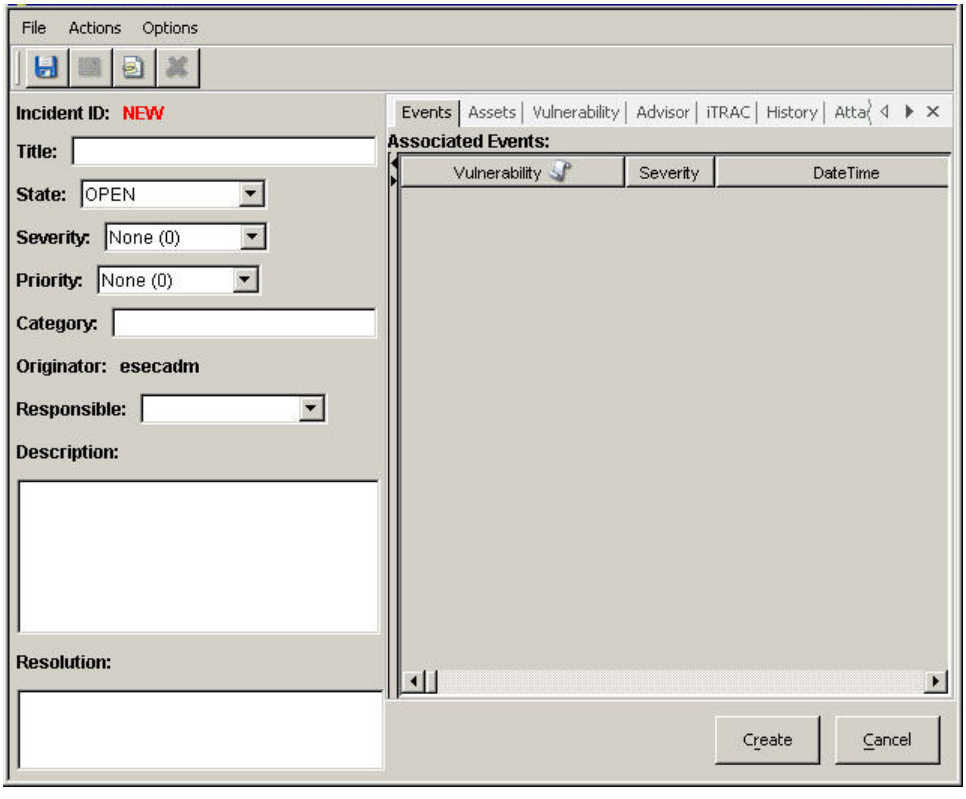
---

**REMARQUE** : les boutons *Ajouter* et *Supprimer* de l'onglet Actifs, Vulnérabilité ou Advisor vous permettent d'ajouter ou de supprimer manuellement des données relatives à un actif,
une vulnérabilité ou un composant Advisor.

## Création d'un incident

Création d'un incident

1. Cliquez sur l'onglet *Incidents*.
2. Cliquez sur *Incidents* > *Créer un incident ou sur le bouton Créer un nouvel incident.*




Dans la boîte de dialogue Créer un incident, entrez les informations dans les champs vides.

3. Cliquez sur *Enregistrer*.

## Affichage et enregistrement de pièces jointes

Pour afficher une pièce jointe

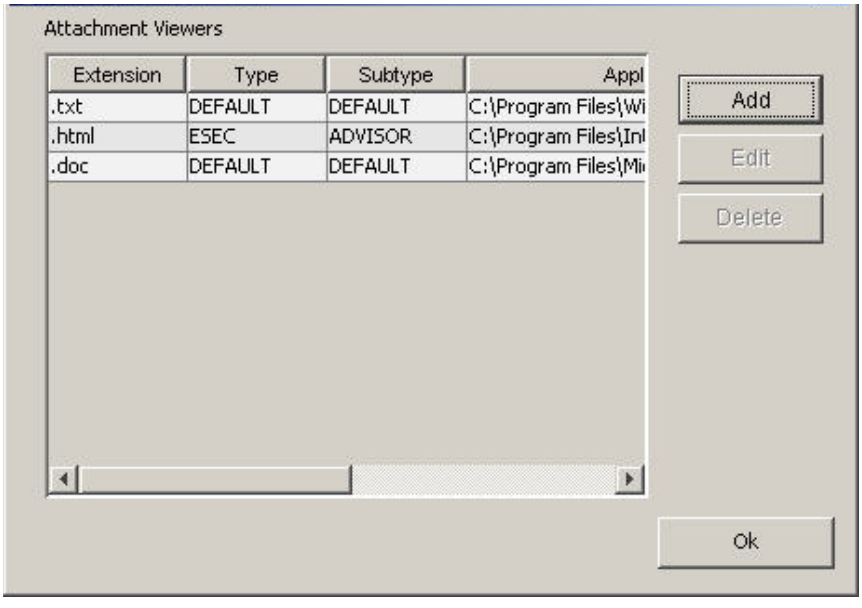
1. Cliquez avec le bouton droit sur une pièce jointe > Afficher ou Enregistrer la pièce jointe.

**REMARQUE** : pour visualiser une pièce jointe, vous devez configurer un visualiseur. Si une pièce jointe n'est pas associée à un type de fichier, une invite s'affiche vous demandant avec quel programme le fichier doit être ouvert. Les pièces jointes sont enregistrées dans la base de données Sentinel.

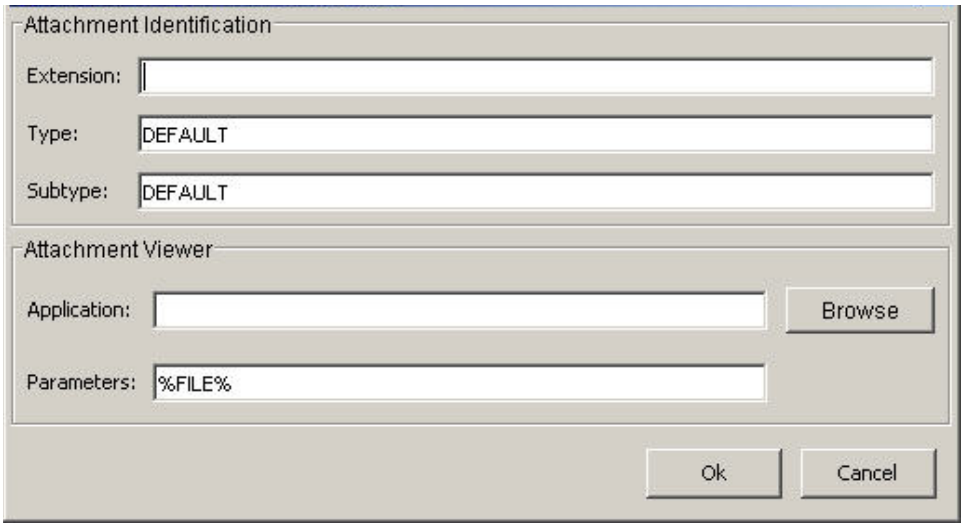
### Configuration du visualiseur de pièces jointes

Configuration du visualiseur de pièces jointes

1. Cliquez sur l'onglet *Incidents*.
2. Cliquez sur *Incidents* > *Configuration du visualiseur de pièces jointes* ou sur *Configurer le visualiseur de pièces jointes*.




3. Cliquez sur *Ajouter*.




Entrez le type d'extension (tel que .doc, .xls, .txt, .html), cliquez sur *Parcourir* ou tapezle nom de l'application qui permet de lancer le type de fichier (notepad.exe pour Bloc-notes, par exemple).

4. Cliquez sur *OK*.

## Envoi d'un incident par courrier électronique

La fonctionnalité d'envoi de courriers électroniques est activée dans le fichier execution properties lors de l'installation. Pour configurer ce fichier, reportez-vous au *Chapitre 11 : Utilitaires*.

Envoi d'un incident par courrier électronique

1. Cliquez sur l'onglet Incidents.
2. Dans le navigateur, développez le dossier Incidents, s'il est disponible, ou cliquez sur Incidents > View Incidents List (Afficher la liste des incidents). Vous pouvez également cliquer sur View Incidents List (Afficher la liste des incidents).

    .
3. Double-cliquez sur le nom d'une vue d'incident.
4. Double-cliquez sur un incident.
5. Double-cliquez sur Incident de message électronique  .
6. Entrez :
   - Adresse électronique
   - Objet du message électronique
   - Message électronique
7. Cliquez sur *OK*. Le message électronique comportera une pièce jointe au format HTML qui répertorie les détails de l'incident, les informations relatives aux événements, aux actifs, aux vulnérabilités et à l'Advisor ainsi que l'historique de l'incident.

## Modification d'un incident

Pour modifier un incident

1. Cliquez sur l'onglet *Incidents*.
2. Cliquez sur *Incidents* > *Afficher le gestionnaire de vues d'incidents*

   ou sur *Afficher le gestionnaire de vues d'incidents*.  .
3. Double-cliquez sur une vue d'incident.
4. Double-cliquez sur un incident.
5. La fenêtre Détails de l'incident s'ouvre.
6. Vous pouvez également modifier les champs suivants d'un incident :
   - Titre
   - État
   - Gravité
   - Priorité
   - Catégorie
   - Responsable
   - Description
   - Résolution
7. Sous l'onglet Pièces jointes, vous pouvez ajouter des pièces jointes ou en supprimer.
8. Cliquez sur Enregistrer.

## Suppression d'un incident

**REMARQUE** : pour supprimer un incident joint à un processus de travail (iTRAC), vous devez d'abord mettre fin au processus iTRAC.

Pour supprimer un incident

1. Cliquez sur l'onglet *Incidents*.
2. Cliquez sur *Incidents* > *Afficher le gestionnaire de vues d'incidents*

   ou sur *Afficher le gestionnaire de vues d'incidents*.  .
3. Double-cliquez sur une vue d'incident.
4. Dans la fenêtre Vue de l'incident, cliquez avec le bouton droit sur un incident, puis cliquez sur Supprimer.

   **REMARQUE** : pour supprimer un incident joint à un processus de travail (iTRAC), vous devez d'abord mettre fin au processus iTRAC. Pour ce faire, vous pouvez utiliser le Gestionnaire d'affichage des processus disponible depuis l'onglet iTRAC. Pour plus d'informations, reportez-vous au *Chapitre 5 : Onglet iTRAC*.
5. Dans la fenêtre de confirmation, cliquez sur *Oui*.

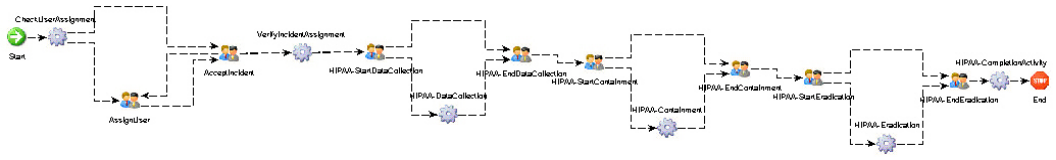
# 5 Onglet iTRAC™

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

iTRAC (flux de travail) permet d'automatiser des procédures et de réagir face à des incidents. Sentinel propose un système de gestion iTRAC qui permet d'automatiser des processus dans le cadre de procédures. Le framework d'activités de Sentinel est lié au système iTRAC. Celui-ci fournit des activités qui peuvent être réalisées automatiquement à chaque étape du processus iTRAC.

Les modèles (définition du processus) et l'exécution du processus forment ensemble le système de gestion du processus de travail.

## Modèles (définition du processus)




Le modèle est l'élément qui contrôle le flux des tâches d'exécution au sein d'iTRAC. Il se compose d'un réseau d'activités liées entre elles, de critères de transition entre les activités et d'informations relatives à chaque activité. Les modèles sont dotés d'attributs modifiables par l'utilisateur.

iTRAC permet de définir des attributs de timeout dans un modèle iTRAC.

Une activité est une unité de travail indépendante qui fait partie du processus iTRAC. Elle est traitée soit par des utilisateurs/rôles (activité manuelle) soit par des applications (activité automatique).

Les activités, qu'elles soient manuelles ou automatiques, sont associées à des timeouts que vous pouvez activer/désactiver.

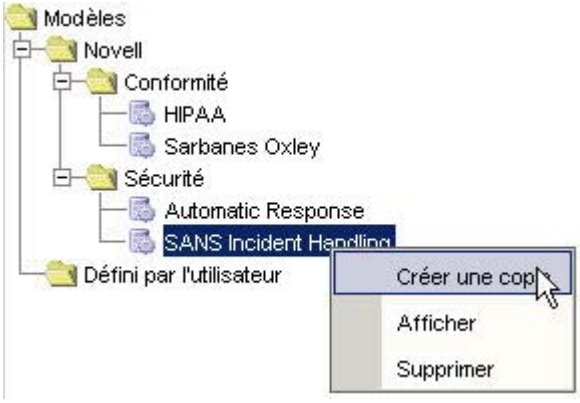
Les activités manuelles, outre les attributs de timeout, permettent de configurer l'attribut de ressource qui détermine l'utilisateur/le rôle qui exécute l'activité.

Les activités automatiques, outre les attributs de timeout, peuvent être configurées à partir du framework d'activité Sentinel à exécuter.

### Gestionnaire de modèles

Le système iTRAC vous permet de créer des modèles, de configurer les attributs de processus et d'activités dans des modèles existants et de supprimer des modèles à partir de la fenêtre Gestionnaire de modèle disponible depuis l'onglet iTRAC.

Vous pouvez accéder au Gestionnaire de modèles en cliquant sur le nœud Gestionnaire de modèles dans l'arborescence du navigateur de l'onglet iTRAC.




## Modèles par défaut

iTRAC est fourni avec quatre modèles par défaut comportant des activités automatiques et manuelles. Les valeurs des attributs de processus et d'activité de ces modèles sont prédéfinies et peuvent être adaptées en fonction des besoins. Les modèles par défaut sont les suivants :

1. HIPAA
2. Sarbanes Oxley
3. SANS Incident Handling
4. Réponse automatique

### Création de modèles

1. Cliquez sur l'onglet iTRAC.
2. Dans le navigateur, cliquez sur Administration iTRAC > Gestionnaire de modèles.
3. Sélectionnez un processus existant (HIPAA, Sarbanes Oxley, SANS ou un processus défini par l'utilisateur), cliquez avec le bouton droit sur celui-ci, puis cliquez sur Créer une copie.
4. Entrez un nom.
5. Si vous sélectionnez un timeout, vous devez entrer une adresse de messagerie ainsi qu'une heure. L'heure est exprimée en nombres entiers. Vous pouvez sélectionner des minutes, des secondes, des heures ou des jours.
6. Entrez une description. Reportez-vous à Modification de modèles existants pour modifier les attributs de processus et d'activité. Cliquez sur OK.
7. Dans le Personnalisateur de modèles, cliquez sur Enregistrer.

### Modification de modèles existants

Lorsque vous modifiez un modèle existant, vous pouvez modifier les attributs de processus ou d'activité.

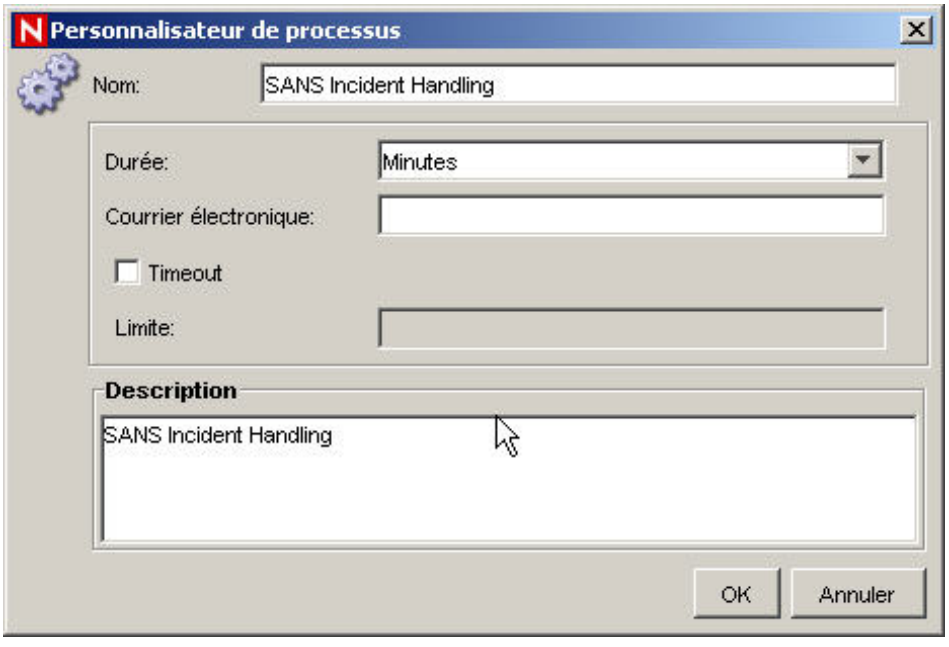
Vous pouvez modifier les attributs de processus suivants :

- Nom
- Limite de timeout et activation/désactivation du timeout
- Description

## Modification des attributs de processus

1. Cliquez sur l'onglet iTRAC.
2. Dans le navigateur, cliquez sur Administration iTRAC > Gestionnaire de modèles.
3. Sélectionnez un modèle existant, cliquez avec le bouton droit sur celui-ci, puis cliquez sur Afficher. Dans la fenêtre du modèle, cliquez sur le bouton Détails du processus.

4. Dans la boîte de dialogue Personnalisateur de processus, vous pouvez modifier les attributs suivants :
   - Nom
   - Durée (minutes, secondes, heures et jours)
   - Timeout (s'il est activé, vous devez entrer une adresse de messagerie et une heure)
   - Description



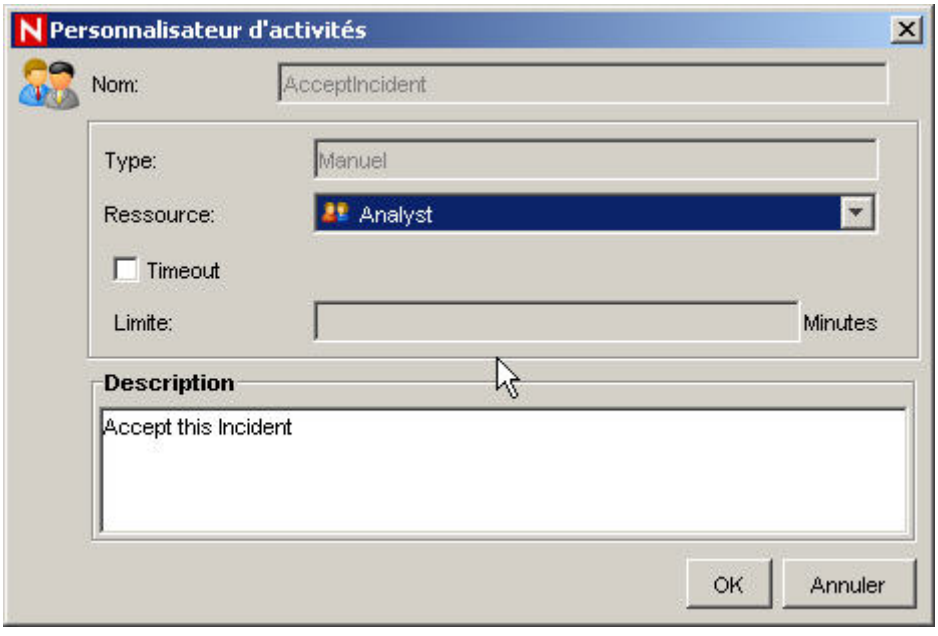

## Modification d'activités manuelles

Vous pouvez modifier les champs Ressource (utilisateur/rôle), Timeout et Description des activités manuelles.

1. Cliquez sur l'onglet *iTRAC*.
2. Dans le navigateur, cliquez sur *Administration iTRAC > Gestionnaire de modèles*.
3. Sélectionnez un modèle existant, cliquez avec le bouton droit sur celui-ci, puis cliquez sur *Afficher*.
4. Le modèle s'affiche dans une fenêtre distincte.
5. Pour le modifier, double-cliquez sur l'une des icônes d'activité manuelle dans le modèle et effectuez vos modifications.

**REMARQUE** : vous pouvez modifier les activités manuelles suivantes.

- AssignUser
- AcceptIncident
- ConfirmStartDataCollection
- ConfirmEndDataCollection
- ConfirmStartContainment
- ConfirmEndContainment
- ConfirmStartEradication
- ConfirmEndEradication



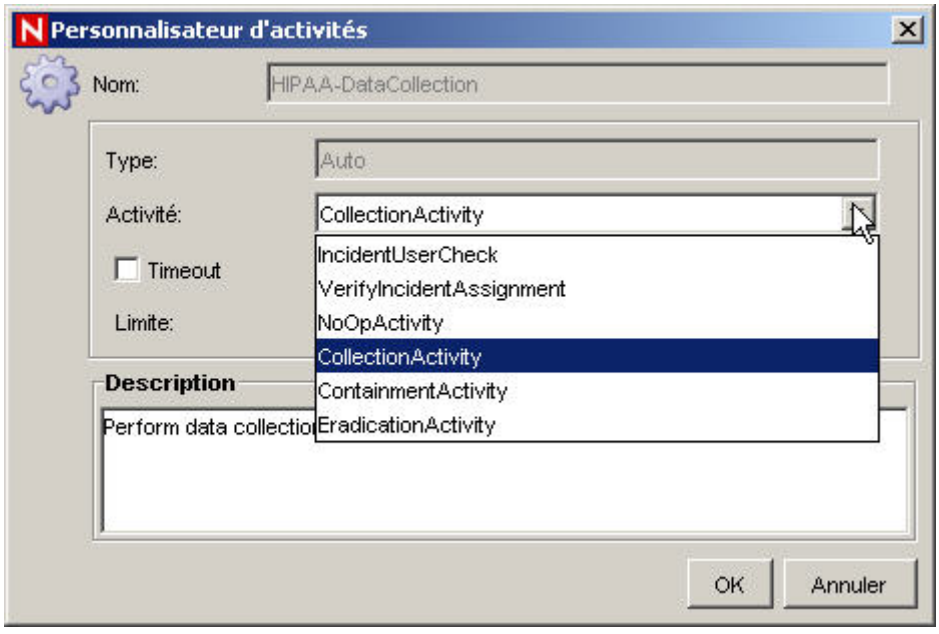

## Modification d'activités automatiques

Vous pouvez modifier les champs Activité, Timeout et Description des activités automatiques.

1. Pour effectuer une modification, double-cliquez sur l'une des icônes d'activité automatique dans le modèle.
2. Le menu déroulant dans la boîte de dialogue Personnalisateur d'activités répertorie toutes les activités susceptibles d'être utilisées en tant qu'activités automatiques. Ces activités sont créées à l'aide du framework d'activités.

**REMARQUE** : vous pouvez modifier les activités automatiques suivantes.

- DataCollection
- Containment
- Eradication




Suppression de modèles

1. Cliquez sur l'onglet iTRAC.
2. Dans le navigateur, cliquez sur Administration iTRAC > Gestionnaire de modèles.
3. Sélectionnez un modèle existant, cliquez avec le bouton droit sur celui-ci, puis cliquez sur Supprimer.
4. Cliquez sur Oui dans le menu contextuel.

# Exécution du processus

L'exécution du processus est la durée pendant laquelle le processus est opérationnel et au cours de laquelle des instances de processus sont créées et gérées.

Lorsqu'un processus iTRAC est exécuté ou instancié au sein du serveur iTRAC, une instance de processus est créée, gérée et terminée par le serveur iTRAC conformément à la définition du processus. À mesure que le processus s'approche de son terme, il exécute diverses activités définies dans le modèle de processus de travail en fonction de critères qui régissent les transitions entre ces activités. Le serveur de processus de travail iTRAC ne traite pas les activités manuelles et automatiques de la même façon.

Un processus iTRAC étant dépendant d'un incident Sentinel, une instance de processus ne peut pas exister en l'absence d'incident associé. En revanche, un incident peut exister sans être associé au serveur de processus de travail. Seul un incident peut être associé à une instance de processus iTRAC.

## Instanciation d'un processus

Il est possible de créer une instance d'un processus iTRAC au sein du serveur iTRAC en associant un incident à un processus iTRAC. Pour cela, trois méthodes existent :

- Associer un processus iTRAC à un incident au moment de la création de l'incident
- Associer un processus iTRAC à un incident après la création de l'incident
- Associer un processus iTRAC à un incident par l'intermédiaire d'une corrélation

Reportez-vous au chapitre consacré à l'onglet Incidents pour plus de détails sur l'association d'un processus à un incident.

## Exécution d'une activité automatique

Lorsqu'une instance de processus exécute une activité automatique, elle exécute l'activité associée définie dans le modèle. L'activité associée est créée à l'aide du framework d'activités. Le serveur iTRAC exécute l'activité, stocke les résultats des variables de processus et passe à l'activité suivante du modèle iTRAC.

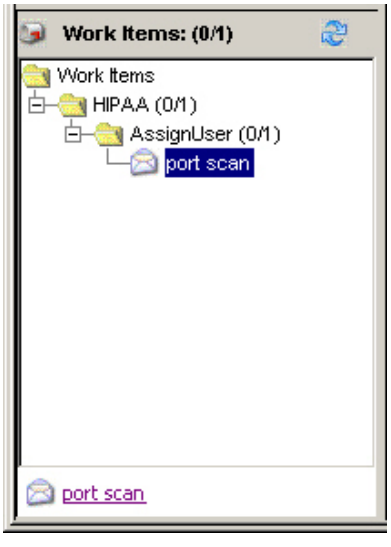
Par exemple, l'activité du framework d'activités peut consister à exécuter une commande ping sur un serveur et à joindre les résultats à l'incident associé.

## Exécution d'une activité manuelle

Lorsqu'il rencontre une activité manuelle, le serveur iTRAC envoie des notifications sous la forme d'éléments de travail à la ressource assignée. Si cette ressource est un utilisateur, l'élément de travail n'est envoyé qu'à cet utilisateur. Si l'activité a été assignée à un rôle, l'élément de travail est envoyé à tous les utilisateurs associés à ce rôle. Le serveur iTRAC attend ensuite que l'utilisateur termine l'élément de travail avant de passer à l'activité suivante.

## Listes d'éléments de travail

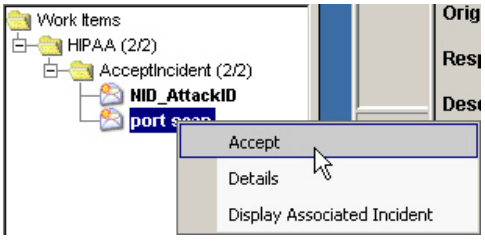
Les éléments de travail sont présentés à l'utilisateur dans une liste de travail qui répertorie tous les détails relatifs aux éléments de travail qui reviennent à cet utilisateur. Il s'agit en fait d'une liste de tâches destinée à l'utilisateur.



Cette liste est consultable à partir de n'importe quel onglet de l'interface Sentinel. Les éléments de travail sont regroupés par processus et activité. Les éléments de travail en caractères gras sont ceux qui n'ont pas encore été acceptés par l'utilisateur.

La liste des éléments de travail vous permet d'intervenir sur des éléments individuels.

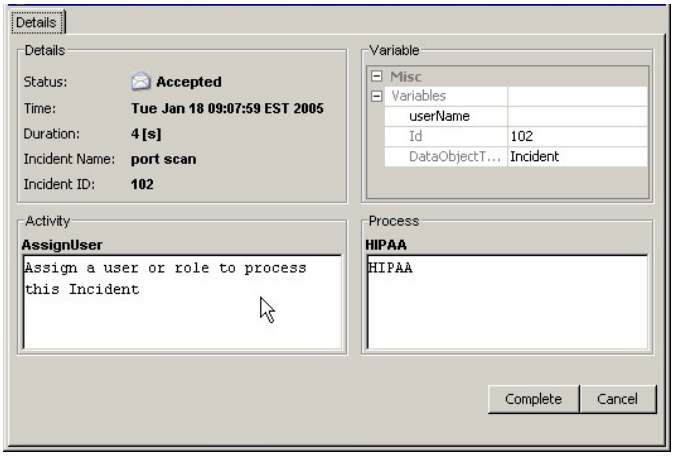
- Pour afficher les détails relatifs à l'élément de travail, double-cliquez sur l'élément ou cliquez avec le bouton droit sur celui-ci, puis cliquez sur Détails.
- Pour accepter des éléments de travail encore non acceptés, cliquez sur ceux-ci avec le bouton droit, puis cliquez sur Accepter.
- Pour afficher les détails relatifs à l'incident associé, cliquez avec le bouton droit sur ceux-ci, puis sur Afficher.




## Éléments de travail

Un élément de travail est une tâche qu'un utilisateur doit réaliser dans le cadre de l'activité manuelle en cours d'exécution au sein d'un processus iTRAC. C'est l'utilisateur qui a la charge de son contrôle et de sa progression.

Le serveur iTRAC attend que l'utilisateur termine la tâche avant de passer à l'activité suivante au sein de l'instance de processus.




La boîte de dialogue Détails présentée ci-dessus affiche les informations suivantes :

- Détails relatifs à l'élément de travail
- Variables relatives à l'élément de travail
- Description de l'activité
- Description du processus

Toute intervention sur un élément de travail implique les trois étapes suivantes :

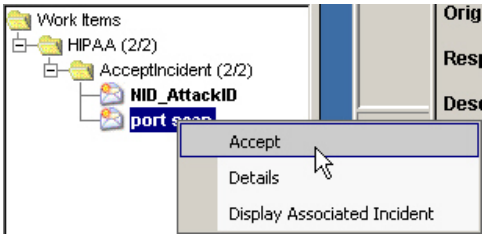
- Acceptation de l'élément de travail
- Mise à jour des variables relatives à l'élément de travail
- Arrêt de l'élément de travail

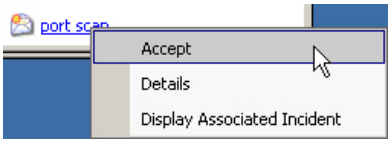
## Acceptation d'un élément de travail

Un élément de travail peut être assigné à tous les utilisateurs affectés à un même rôle ou à un seul d'entre eux. Un élément de travail doit être accepté par l'utilisateur avant qu'il puisse faire l'objet d'une autre action. Lorsqu'un utilisateur accepte un élément de travail, il en devient le propriétaire. En outre, l'élément de travail est supprimé de la liste de travail des autres utilisateurs auxquels il était assigné.

Acceptation d'éléments de travail

1. Dans la liste de travail, vous pouvez cliquez avec le bouton droit sur un élément et choisir l'une des options suivantes :



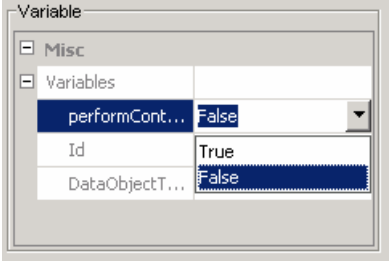

   - Accepter (lorsque le processus est à une étape d'acceptation)
   - Vous pouvez également afficher la fenêtre Détails, puis cliquer sur le bouton Accepter.

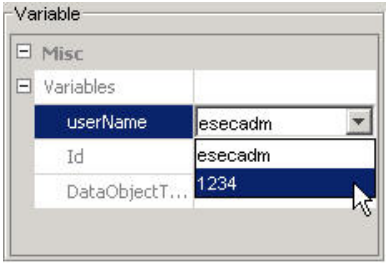
## Mise à jour des variables relatives à l'élément de travail

Le serveur iTRAC se sert des éléments de travail pour obtenir des informations auprès des utilisateurs. Ces informations sont consignées dans des variables et déterminent la prochaine activité de processus devant avoir lieu. Les variables sont accessibles uniquement après acceptation de l'élément de travail.

iTRAC prend en charge les variables en lecture et les variables actualisables. Les premières permettent d'informer l'utilisateur, par exemple du statut d'une activité ou de l'ID d'un incident.

Les secondes servent à accepter les informations entrées par l'utilisateur. Actuellement dans iTRAC, deux types de variables actualisables existent : les listes définies par l'utilisateur et les listes booléennes.



Mise à jour des variables

1. Cliquez avec le bouton droit ou double-cliquez sur l'élément de travail à afficher dans la boîte de dialogue Détails.
2. Seules les variables actualisables sont modifiables. Les variables en lecture seule ne le sont pas.
3. Cliquez sur la liste déroulante et sélectionnez la valeur qui convient.

## Arrêt de l'élément de travail

L'arrêt de l'élément de travail signale au serveur iTRAC que la tâche est terminée. Les variables actualisables que comporte l'élément de travail sont traitées par le serveur en vue de passer à l'activité suivante en fonction de certains critères. L'élément de travail est supprimé de la liste de travail de l'utilisateur. Un élément de travail doit être accepté avant d'être terminé.

Arrêt d'éléments de travail

1. Cliquez avec le bouton droit ou double-cliquez sur l'élément de travail à afficher dans la boîte de dialogue Détails.
2. Dans la boîte de dialogue, cliquez sur le bouton Terminé.

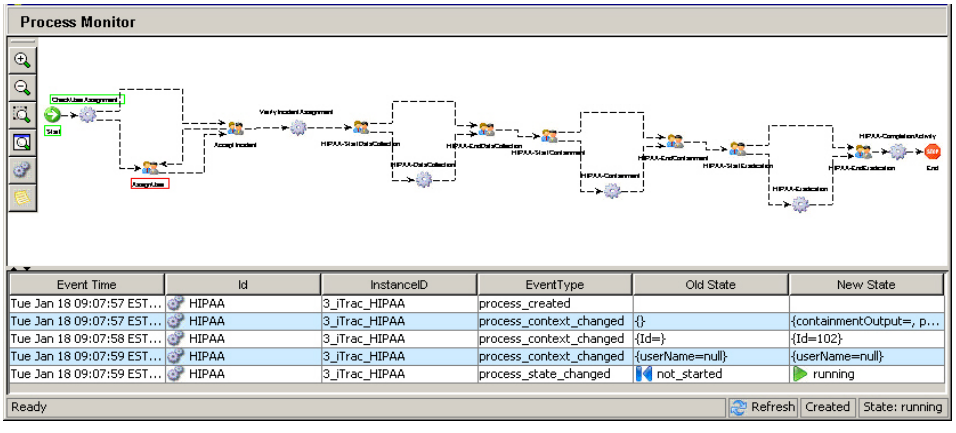
# Gestion des processus

La fonction Gestion des processus vous permet :

- d'afficher le statut d'un processus (Traiter le moniteur) ;
- de démarrer un processus ;
- de mettre fin à un processus.

## Traiter le moniteur

La fonction Traiter le moniteur permet de surveiller la progression d'un processus. À mesure qu'une instance du processus passe d'une activité à une autre, l'utilisateur peut en suivre une représentation graphique en cliquant sur le bouton Rafraîchir. Cette fonction fournit galement un suivi d'audit de toutes les opérations réalisées par le serveur iTRAC lors de l'exécution du processus.

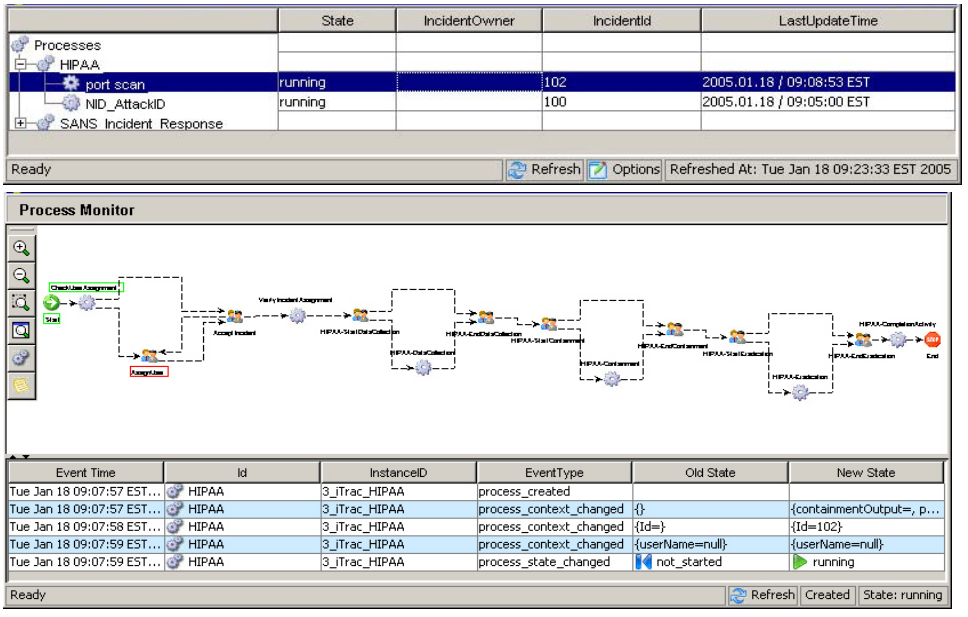


Les activités terminées sont signalées par un cadre vert et l'activité en cours par un cadre rouge.

### Accès à la fonction Traiter le moniteur

1. Cliquez sur l'onglet *iTRAC*.
2. Cliquez sur le bouton *Gestionnaire des options de vues*.

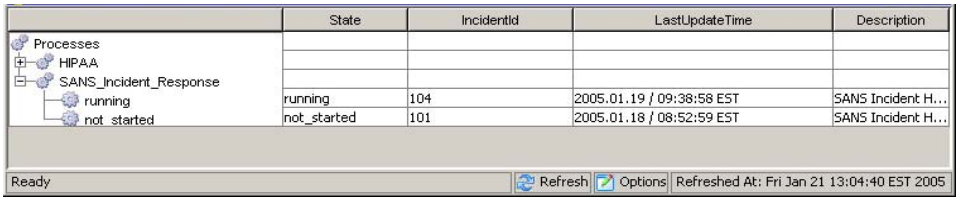
3. Double-cliquez sur l'une des options de vues par défaut ou créez une nouvelle vue. Les vues par défaut sont :
   - All Processes (Tous les processus)
   - Processes By Incident (Processus par incident)
   - Processes By Status (Processus par état)
4. Dans le Gestionnaire des processus actifs, sélectionnez un processus, puis double-cliquez sur celui-ci.




### Pour définir une option du Gestionnaire de processus

1. Cliquez sur l'onglet *iTRAC*.
2. Double-cliquez sur un processus.
3. Cliquez sur le bouton Options. Dans cette fenêtre, vous pouvez également définir les options suivantes :
   - Champs...
   - Regrouper par...
   - Trier...
   - Filtre...
   - Affichage sous forme d'arborescence
4. Cliquez sur *Appliquer* puis sur Enregistrer.

L'illustration ci-dessous montre une vue avec Affichage sous forme d'arborescence défini à Statut (en cours d'exécution ou non démarré).




## Démarrage ou arrêt d'un processus

Démarrage ou arrêt d'un processus

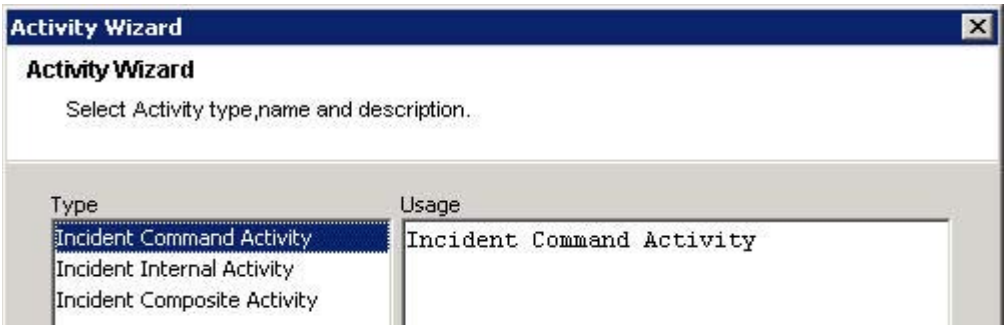
1. Cliquez sur l'onglet *iTRAC*.
2. Cliquez sur le bouton *Gestionnaire des options de vues*.

3. Double-cliquez sur l'une des options de vues par défaut ou créez une nouvelle vue. Les vues par défaut sont :
   - All Processes (Tous les processus)
   - Processes By Incident (Processus par incident)
   - Processes By Status (Processus par état)
4. Dans le Gestionnaire des processus actifs, sélectionnez un processus, cliquez avec le bouton droit sur celui-ci, puis cliquez sur *Début du processus* ou *Terminer le processus*.

# Création d'une activité à l'aide du framework d'activités

Création d'une activité

1. Cliquez sur l'onglet *iTRAC*.
2. Dans le navigateur, cliquez sur *Administration iTRAC > Gestionnaire d'activités*.
3. Cliquez avec le bouton droit, puis sélectionnez *Nouvelle activité*.
4. Sélectionnez l'une des options suivantes :



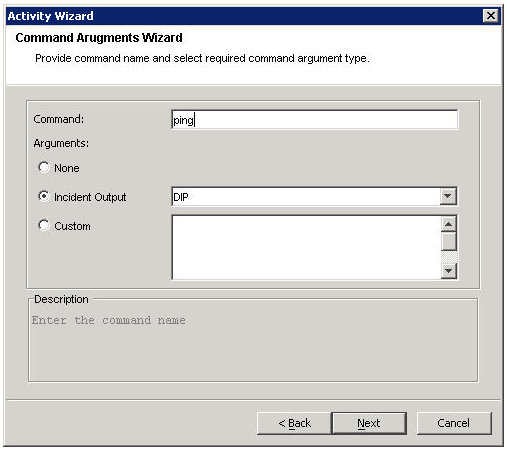
- Activité de commande d'incident : démarre une commande spécifique avec ou sans arguments.

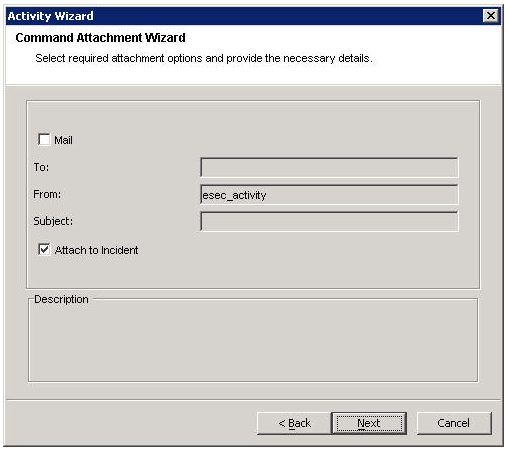
  L'option Sortie d'incident génère les arguments suivants :

  - DIP
  - DIP:Port
  - incident
  - RT1 (DeviceAttackName)
  - SIP
  - SIP:Port
  - Texte

  L'option Personnalisé vous permet d'entrer des arguments personnalisés.

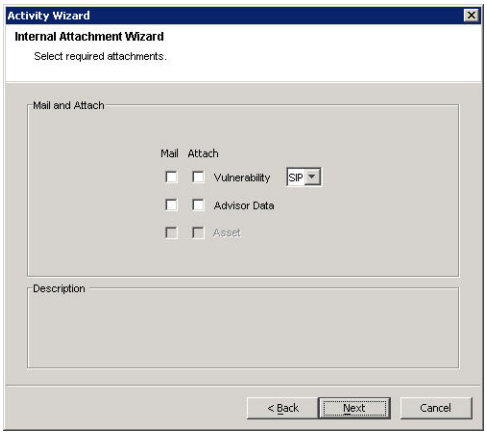
  Pour cette activité, vous pouvez également envoyer la sortie par courrier électronique et/ou la joindre à l'incident.



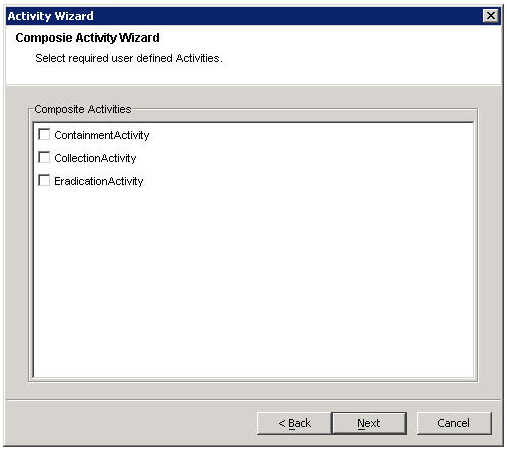



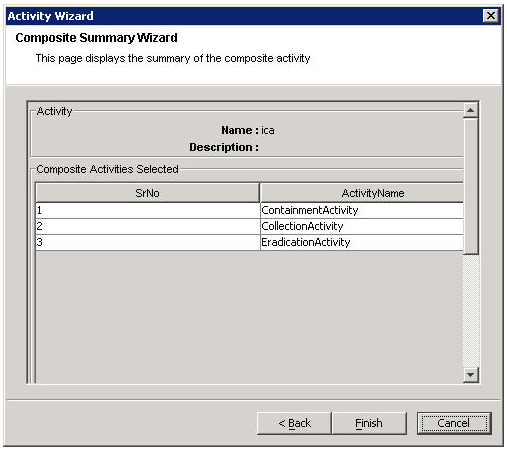

- Activité interne d'incident : permet d'envoyer par courrier électronique et/ou de joindre des informations relatives aux points suivants :

  - Vulnérabilité pour (SIP ou DIP)
  - Données de l'Advisor
  - Actif



- Activité composite d'incident : permet de créer une activité en fusionnant une ou plusieurs activités existantes.




## Modification d'une activité

### Modification d'une activité

1. Cliquez sur l'onglet *iTRAC*.
2. Dans le navigateur, cliquez sur *Administration iTRAC* > *Gestionnaire d'activité* > *Activités iTRAC*.
3. Double-cliquez sur une activité iTRAC. Effectuez vos modifications, puis cliquez sur OK.

## Importation/exportation d'une activité

Vous pouvez exporter des activités en tant que fichiers xml. Ces fichiers peuvent être importés d'un système à un autre.

### Exportation d'une activité

1. Cliquez sur l'onglet *iTRAC*.
2. Dans le navigateur, cliquez sur *Administration iTRAC* > *Gestionnaire d'activités*.
3. Cliquez avec le bouton droit, puis sélectionnez *Activités iTRAC* > *Activité d'importation/exportation*.
4. Sélectionnez Exporter l'activité, puis cliquez sur *Explorer*.
5. Accédez à l'emplacement auquel vous voulez enregistrer le fichier exporté.
6. Entrez le nom du fichier, puis cliquez sur *Exporter*.
7. Cliquez sur *Suivant*.
8. Sélectionnez une ou plusieurs activités à exporter.
9. Cliquez sur *Suivant*, puis sur *Terminer*.

### Importation d'une activité

1. Cliquez sur l'onglet *iTRAC*.
2. Dans le navigateur, cliquez sur *Administration iTRAC* > *Gestionnaire d'activités*.

3. Cliquez avec le bouton droit, puis sélectionnez *Activités iTRAC > Activité d'importation/exportation*.
4. Sélectionnez Importer l'activité, puis cliquez sur le bouton *Explorer*.
5. Accédez au fichier à importer. Cliquez sur *Importer*.
6. Cliquez sur *Suivant*.
7. Cliquez sur *Suivant*, puis sur *Terminer*.

# 6 Onglet Analyse

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

Vous devez disposer de l'autorisation appropriée pour pouvoir utiliser l'onglet Analyse. Si tel n'est pas le cas, aucune autre autorisation liée aux opérations effectuées à l'aide de cet onglet n'est disponible.

## Description

L'onglet Analyse est destiné à la génération de rapports d'historique. Les rapports d'historique et ceux relatifs aux vulnérabilités sont publiés sur un serveur Web et sont générés directement à partir de la base de données. Ils apparaissent sur les onglets Analyse et Advisor de la barre du navigateur.

> **REMARQUE** : Crystal Reports®, un outil qui permet de générer et d'afficher des rapports, est intégré à Sentinel. C'est l'administrateur qui est chargé de configurer l'emplacement du serveur Crystal Enterprise. Ce serveur permet de publier les rapports dans la fenêtre Options générales de l'onglet Admin. La fenêtre du navigateur comporte la liste des rapports disponibles.
>
> Pour pouvoir exécuter les modèles de rapport, Crystal Reports Enterprise Edition doit être installé et le Centre de contrôle Sentinel doit être configuré de façon à pouvoir accéder à ce serveur. Pour plus d'informations, reportez-vous au *guide d'installation de Sentinel™ 5*.

Des rapports types sont également fournis au format PDF.

### Les 10 rapports les plus utilisés

Pour générer l'un des 10 rapports les plus utilisés, le regroupement doit être activé et le service EventFileRedirectService doit être également activé dans le fichier DAS_Binary.xml. Pour plus d'informations sur l'activation du regroupement, reportez-vous à la section consacrée à *l'onglet Données de rapport du Chapitre 10 : Gestionnaire de données Sentinel du présent guide*.

#### Activation de EventFileRedirectService pour les 10 rapports Sentinel les plus utilisés

Activation de EventFileRedirectService

1. Depuis votre machine DAS, à l'aide d'un éditeur de texte, ouvrez :

   Pour UNIX :

   ```
   $ESEC_HOME/sentinel/config/das_binary.xml
   ```

   Pour Windows :

   ```
   %ESEC_HOME%\sentinel\config\das_binary.xml
   ```

2. Pour EventFileRedirectService, indiquez « on » comme statut.

```
<property name="status">on</property>
```

3. Pour Windows, redémarrez le service Sentinel. Pour UNIX, redémarrez la machine DAS.

## Exécution d'un rapport depuis Crystal Reports

Pour créer un rapport à partir d'un modèle Crystal Reports

1. Cliquez sur l'onglet *Analyse*.
2. Dans la *fenêtre de navigation*, cliquez sur un rapport de la liste.

**REMARQUE** : pour générer l'un des 10 rapports les plus utilisés, le regroupement doit être activé et le service EventFileRedirectService doit être également activé dans le fichier DAS_Binary.xml. Pour plus d'informations sur l'activation du regroupement, reportez-vous à la section consacrée à *l'onglet Données de rapport du Chapitre 10 : Gestionnaire de données Sentinel du présent guide*.

3. Cliquez sur *Analyse* > *Créer un rapport* ou sur *Créer un rapport*.

4. Renseignez les champs du modèle, puis cliquez sur *Afficher le rapport*. Le rapport s'affiche alors.

## Génération d'un rapport Requête d'événement

Pour créer un rapport Requête d'événement

1. Cliquez sur l'onglet *Analyse*.
2. Dans la fenêtre de navigation, ouvrez le dossier Historical Reports (Rapports d'historique).
3. Cliquez sur *Requête d'événement*.
4. Cliquez sur *Analyse* > *Créer un rapport* ou sur *Créer un rapport*.

Une fenêtre Requête d'événement s'ouvre.

5. Définissez ce qui suit :
   - le délai
   - le filtre
   - le niveau de gravité
   - la taille du lot (il s'agit du nombre d'événements à afficher. Les événements sont affichés du plus ancien au plus récent)
6. Cliquez sur le bouton *Rafraîchir la requête*.
7. Pour afficher le lot d'événements suivant, cliquez sur *Suite*.

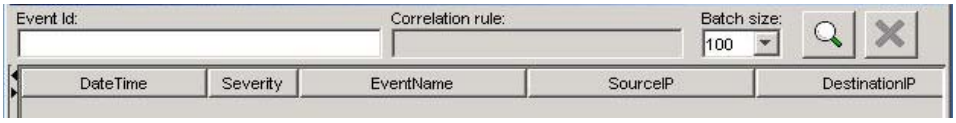
8. Vous pouvez réorganiser les colonnes par glisser-déplacer. Vous pouvez également changer l'ordre de tri d'une colonne en cliquant sur son en-tête.
9. Lorsque votre requête est terminée, elle est ajoutée à la liste de requêtes rapides dans le navigateur.

## Génération d'un rapport Événements corrélés

Pour créer un rapport Événements corrélés

1. Cliquez sur l'onglet Analyse.
2. Dans la fenêtre de navigation, ouvrez le dossier Historical Reports (Rapports d'historique).
3. Cliquez sur *Événements corrélés*.
4. Cliquez sur *Analyse* > *Créer un rapport* ou sur *Créer un rapport*.

Une fenêtre s'ouvre.




5. Dans le champ Correlation ID, entrez :
   - Le numéro d'ID d'événement, ou
   - CorrelatedEventUUID

**REMARQUE** : CorrelatedEventUUID n'est disponible que depuis une table d'événements en temps réel.

6. Pour afficher le lot d'événements suivant, cliquez sur *Suite*.

# 7 Onglet Advisor

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

Vous devez disposer de l'autorisation appropriée pour pouvoir utiliser l'onglet Advisor. Si tel n'est pas le cas, aucune autre autorisation liée aux opérations effectuées à l'aide de cet onglet n'est disponible.

Advisor est un module facultatif. Vous devez disposer d'une licence pour ce module. Si tel n'est pas le cas, lorsque vous cliquez sur l'onglet Advisor, un écran vous indique que vous ne disposez pas de licence.

Sentinel Advisor est activé par SecurityNexus. Advisor fournit des données en temps réel couvrant les vulnérabilités de l'entreprise ainsi que des conseils d'expert. Il indique également les mesures recommandées permettant de résoudre les problèmes. Advisor fait le lien entre les signatures d'attaques de système de détection d'intrusion en temps réel et sa base de connaissances de vulnérabilités. Pour plus d'informations, accédez à http://www.esecurity.net/Software/Products/Advisor.asp.

Le flux de données généré par Advisor comporte deux parties :

- Données d'alerte : informations d'alerte relatives aux vulnérabilités et aux menaces connues.
- Données d'attaque : normalisation des plug-ins d'analyse des signatures de détection d'intrusion et de vulnérabilité.

**REMARQUE** : au cours de l'installation et jusqu'au premier flux de données de SecurityNexus, vous ne pouvez pas cliquer avec le bouton droit sur les données Advisor d'un événement (dont le champ rt1 est rempli).

## Génération de rapports Advisor

Pour créer un rapport Advisor

1. Cliquez sur l'onglet Advisor.
2. Dans le navigateur, cliquez sur un modèle de rapport.
3. Cliquez sur Advisor > Créer un rapport.
4. Renseignez les champs du modèle, puis cliquez sur Afficher le rapport.

## Installation autonome : Mise à jour manuelle d'Advisor

Mise à jour du flux de données Advisor

1. Accédez à l'URL //advisor.esecurityinc.com/advisordata/.
2. Entrez votre nom d'utilisateur et votre mot de passe.

3. Accédez au mois le plus récent sous les dossiers d'attaques et d'alertes, puis téléchargez les fichiers zip.
4. Téléchargez les nouveaux fichiers de flux de données d'alerte et d'attaque (les fichiers sont au format zip) sur votre disque dur.

**REMARQUE** : ne placez pas les fichiers zip dans les répertoires attack et alert.

5. Dézippez les fichiers contenant les données d'attaque dans le répertoire suivant :

   Sous Windows :

   ```
   <emplacement spécifié lors de l'installation pour
      les fichiers de données Advisor>\attack
   ```

   ou

   Sous UNIX :

   ```
   <emplacement spécifié lors de l'installation pour
      les fichiers de données Advisor>/attack
   ```

6. Dézippez les fichiers contenant les données d'alerte dans le répertoire suivant :

   Sous Windows :

   ```
   <emplacement spécifié lors de l'installation pour
      les fichiers de données Advisor>\alert
   ```

   ou

   Sous UNIX :

   ```
   <emplacement spécifié lors de l'installation pour
      les fichiers de données Advisor>/alert
   ```

7. Accédez à :

   Sous Windows :

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   Sous UNIX :

   ```
   $ESEC_HOME/sentinel/bin
   ```

8. Exécutez la commande suivante :

   Sous Windows :

   ```
   advisor.bat
   ```

   Sous UNIX :

   ```
   ./advisor.sh
   ```

**REMARQUE :** advisor.sh et advisor.bat mettent à jour la base de données et suppriment les fichiers d'attaque et d'alerte dézippés dans les répertoires correspondants.

# Téléchargement direct depuis Internet : Mise à jour manuelle des données Advisor

Mise à jour manuelle des données Advisor

1. Accédez à :

   Sous Windows :

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   Sous UNIX :

   ```
   $ESEC_HOME/sentinel/bin
   ```

2. Exécutez la commande suivante :

   Sous Windows :

   ```
   advisor.bat
   ```

   Sous UNIX :

   ```
   ./advisor.sh
   ```

   **REMARQUE :** advisor.sh et advisor.bat mettent à jour la base de données et suppriment les fichiers d'attaque et d'alerte dézippés dans les répertoires correspondants.

# Changement de votre mot de passe Advisor Server et communication de votre nouvelle adresse de messagerie à Advisor Server

## Changement de votre mot de passe Advisor Server (configuration autonome)

Cette procédure ne s'applique pas aux configurations autonomes.

## Changement de votre mot de passe Advisor Server (téléchargement direct)

Pour changer votre mot de passe Advisor Server (téléchargement direct)

1. Envoyez une demande de changement de mot de passe au service d'assistance technique Novell.
2. Une fois que Novell vous aura communiqué votre nouveau mot de passe, sous UNIX, ouvrez une session en tant qu'utilisateur esecadm, sous Windows, ouvrez une session en tant qu'utilisateur doté des droits d'administrateur.
3. Avec la commande cd, accédez au répertoire :

3. Sous UNIX :

   ```
   $ESEC_HOME/sentinel/bin
   ```

   Sous Windows :

   ```
   %ESEC_HOME%\sentinel\bin
   ```

4. Entrez les commandes suivantes :

   Sous UNIX :

   ```
   ./adv_change_passwd.sh <ancien mot de passe> <nouveau
      mot de passe>
   ```

   Sous Windows :

   ```
   adv_change_passwd.bat <ancien mot de passe> <nouveau
      mot de passe>
   ```

## Communication de votre nouvelle adresse de messagerie à Advisor Server

Pour changer votre configuration de messagerie Advisor Server

1. Sous UNIX, ouvrez une session en tant qu'utilisateur esecadm ou sous Windows, ouvrez une session en tant qu'utilisateur doté des droits de l'administrateur.
2. Avec la commande cd, accédez au répertoire :

   Sous UNIX :

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

   Sous Windows :

   ```
   %ESEC_HOME%\sentinel\config
   ```

3. Ouvrez dans un éditeur de texte les fichiers alertcontainer.xml et alertcontainer.xml. Modifiez les informations apparaissant en gris ci-dessous.

   ```
   <property
      name="advisor.mail.from">fromNAME@domain.com</propr
      ty>
   <property
      name="advisor.mailto.list">toNAME@domain.com</propr
      ty>
   ```

**REMARQUE** : pour indiquer plusieurs adresses de messagerie, entrez les adresses en les séparant par une virgule (sans espace).

# Changement des heures de réception des flux de données

Par défaut, les flux de données sont transmis aux heures suivantes :

- Six heures : 01:00, 07:00, 13:00 et 19:00
- Douze heures : 02:00 et 14:00

Pour changer les heures de réception des flux de données

1. Ouvrez une session sur la machine Advisor (avec le nom d'utilisateur esecadm sous UNIX).
2. Pour changer les heures de réception des flux de données

   Sous UNIX : utilisez la commande crontab.

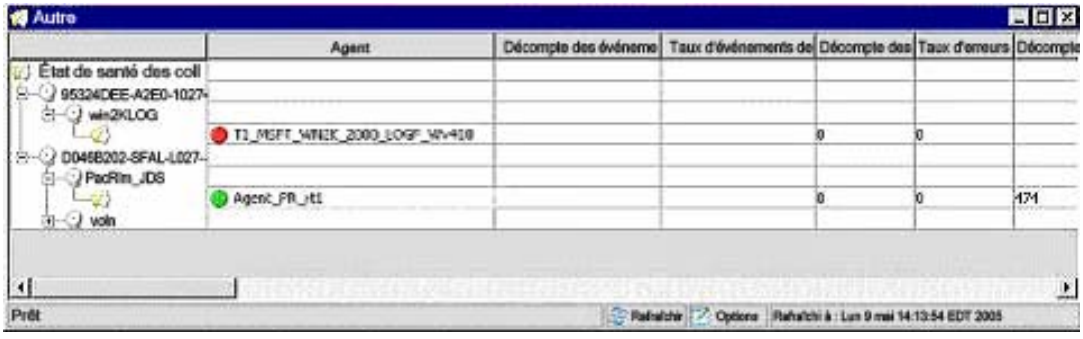
   Sous Windows : utilisez la commande at.

# 8 Onglet Collecteurs

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

Vous devez disposer de l'autorisation appropriée pour pouvoir utiliser l'onglet Collecteurs. L'onglet Collecteurs offre des fonctionnalités limitées d'assistant. Pour utiliser les fonctionnalités complètes de l'assistant, utilisez le Générateur de collecteurs. L'onglet Collecteurs vous permet d'effectuer les tâches suivantes :

- Surveillance d'un hôte Assistant
- Surveillance d'un collecteur
- Arrêt/démarrage des collecteurs (Gestionnaire des collecteurs) pour un hôte sélectionné




## Agencement

Le panneau gauche de l'onglet Collecteurs contient une arborescence de vues. Par défaut, la racine de l'arborescence comporte deux enfants : les vues du Gestionnaire des collecteurs et la vue du collecteur. Le panneau droit affiche les vues dans des tableaux. Chaque vue du panneau droit est associée à une entrée figurant dans la partie gauche de l'arborescence.

Quatre vues sont affichées dans le panneau droit :

- La vue du collecteur
  - Le Gestionnaire des vues du collecteur
- La vue du Gestionnaire des collecteurs
  - Le Gestionnaire des vues du Gestionnaire de collecteurs

La vue du collecteur affiche des informations sur les collecteurs et la vue du Gestionnaire des collecteurs des informations sur les gestionnaires de collecteurs. Chaque vue est affichée sous la forme d'une table d'arborescence : les objets sont regroupés par l'un ou plusieurs de leurs attributs. La configuration de la vue peut être définie. Les options d'une vue peuvent être changées et de nouveaux types de vues peuvent être ajoutés. La configuration de vue est affichée dans un gestionnaire de vues (Gestionnaire des vues du collecteur ou Gestionnaire des vues du Gestionnaire de collecteurs).

Au premier affichage de l'onglet, l'arborescence du panneau gauche reçoit les deux gestionnaires de vues et le Gestionnaire des vues du collecteur s'affiche dans le panneau gauche.

Le Gestionnaire des vues du collecteur comporte 3 options de vues préconfigurées par défaut. Vous pouvez en créer de nouvelles. Ces trois options sont : Tous les collecteurs, Collecteurs par gestionnaire et Collecteurs par état.

La vue Tous les collecteurs regroupe tous les collecteurs en fonction du gestionnaire sur lequel ils s'exécutent.

Le gestionnaire des vues du Gestionnaire des collecteurs regroupe tous les collecteurs en fonction de leur gestionnaire et de leur statut (activé ou désactivé) dans chaque gestionnaire.

La vue Collecteurs par état regroupe tous les collecteurs en fonction de leur statut (activé ou désactivé), puis, dans chaque état, en fonction de leur gestionnaire.

Il existe une vue par défaut pour afficher les gestionnaires de collecteurs : la vue Tous les gestionnaires. Elle affiche tous les gestionnaires de collecteurs actifs du système sans les regrouper.

# Surveillance d'un collecteur

Dans la fenêtre Hôtes de l'assistant, par défaut vous pouvez contrôler ce qui suit :

**Le Gestionnaire des vues du Gestionnaire de collecteurs**

- StartTime — Heure à laquelle le Gestionnaire des collecteurs a démarré, spécifiée en mm/jj/aa hh:mm:ss et selon le fuseau horaire.
- UpTime — Durée d'exécution du Gestionnaire des collecteurs, spécifiée en jours, heures, minutes et secondes.
- EventReceivedCount — Nombre d'événements reçus de tous les collecteurs par le Gestionnaire des collecteurs depuis qu'il a démarré.
- EventReceivedRate — Taux d'événements moyen par seconde que le Gestionnaire des collecteurs a reçus dans la dernière minute.

**Gestionnaire des vues du collecteur**

- Statut — activé ou désactivé
- EventsReceivedRate — Taux d'événements moyen par seconde que le port du collecteur a reçus dans la dernière minute.
- EventsReceivedCount — Nombre d'événements reçus par le port du collecteur depuis qu'il a démarré.
- UpTime — Durée d'exécution du port du collecteur, spécifiée en heures, minutes et secondes.

Vous pouvez créer vos propres vues dotées de plus ou moins de champs.

## Surveillance d'un hôte Assistant

Surveillance d'un hôte Assistant

1. Cliquez sur l'onglet Collecteurs.
2. Cliquez sur *Gestionnaire des vues du Gestionnaire des collecteurs*.

3. Sélectionnez une option de vue en double-cliquant sur une vue ou créez une nouvelle vue. Une fenêtre d'hôte Assistant s'affiche.

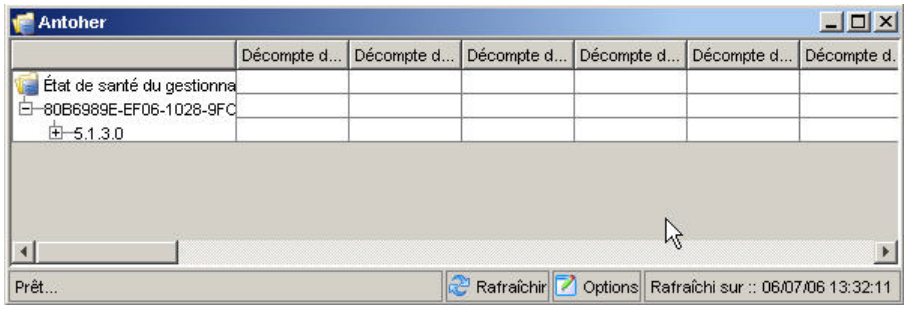

## Création d'une vue de collecteur

Création d'une vue de collecteur

1. Cliquez sur l'onglet *Collecteurs*.
2. Cliquez sur Gestionnaire des vues du Gestionnaire des collecteurs.

3. Pour créer une nouvelle vue, cliquez sur *Ajouter une vue*.
   - Entrez votre nom d'option.
   - Pour sélectionner les champs à afficher, cliquez sur *Champs*.
   - Pour regrouper des titres, cliquez sur *Groupe*.
   - Pour appliquer un tri en fonction des titres, cliquez sur *Trier*.
   - Pour appliquer un filtre, cliquez sur *Filtre*.

   Voici une vue avec l'option Groupe définie sur UUID du gestionnaire et par version.

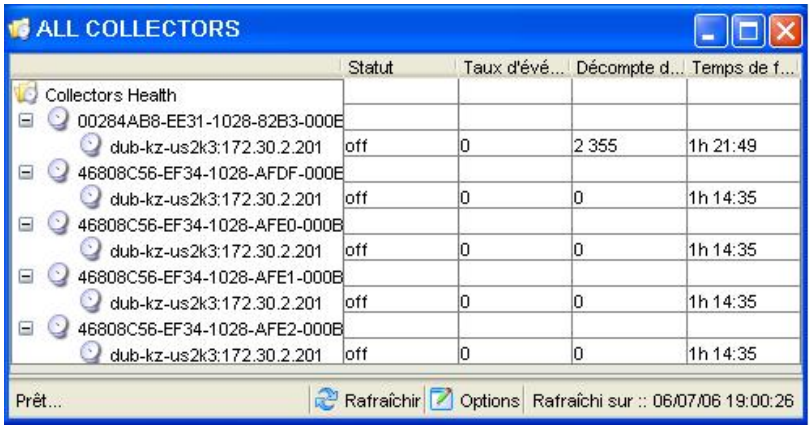


## Modification d'une vue de collecteur

Modification d'une vue de collecteur

1. Ouvrez le Gestionnaire des vues du collecteur.
2. Double-cliquez sur un nom.
3. Cliquez sur *Options*. Dans cette fenêtre, vous pouvez également définir les options suivantes :
   - Champs...
   - Regrouper par...
   - Trier...
   - Filtre...
   - Affichage sous forme d'arborescence
4. Cliquez sur *Appliquer* puis sur Enregistrer.

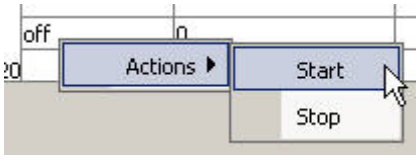
   L'illustration suivante présente une vue avec l'option Tree Display (Affichage de l'arborescence) défini sur UUID du gestionnaire.




## Arrêt/démarrage/détails des collecteurs

Arrêt/démarrage des collecteurs

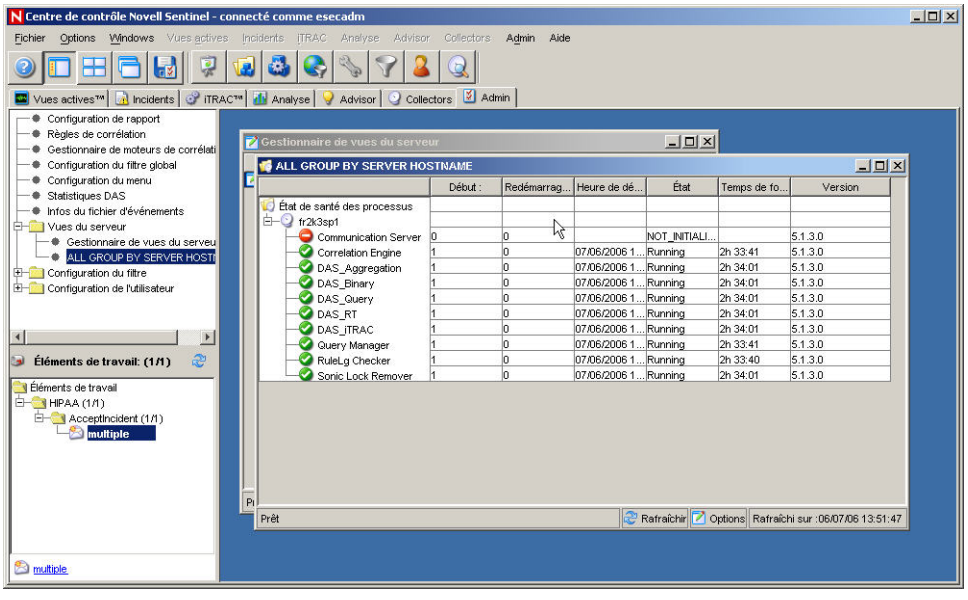
1. Cliquez sur l'onglet *Collecteurs*.
2. Ouvrez un Gestionnaire des vues du collecteur.
3. Pour arrêter/démarrer un collecteur spécifique ou en afficher les détails, cliquez avec le bouton droit sur un *collecteur* > *Opérations* > *Démarrer ou Arrêter*.



# 9 Onglet Admin

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

Vous devez disposer de l'autorisation appropriée pour pouvoir utiliser l'onglet Admin. Si tel n'est pas le cas, aucune autre autorisation liée aux opérations effectuées à l'aide de cet onglet n'est disponible.




## Onglet Admin : Description

L'onglet Admin vous permet d'accéder aux fonctionnalités suivantes :

- Option de configuration des rapports disponibles depuis les onglets Analyse et Advisor
- Filtres
- Règles de corrélation Sentinel
- Configuration des menus
- Statistiques DAS
- Informations du fichier d'événements
- Vues du serveur
- Configuration d'un compte d'utilisateur

# Option de configuration des rapports disponibles depuis les onglets Analyse et Advisor

Pour configurer l'URL des rapports Analyse et Advisor

1. Cliquez sur l'onglet *Admin*.
2. Dans le *navigateur*, cliquez sur *Configuration de rapport*.
3. Dans la fenêtre *Configuration de rapport*, cliquez sur *Modifier*.
   - Dans la zone URL d'analyse, entrez l'URL de Crystal Enterprise Server, puis cliquez sur *Rafraîchir*.

     ```
     http://<IP>/GetReports.asp?APS=<IP>&user=Guest&passwor
        d=&tab=Analysis
     ```

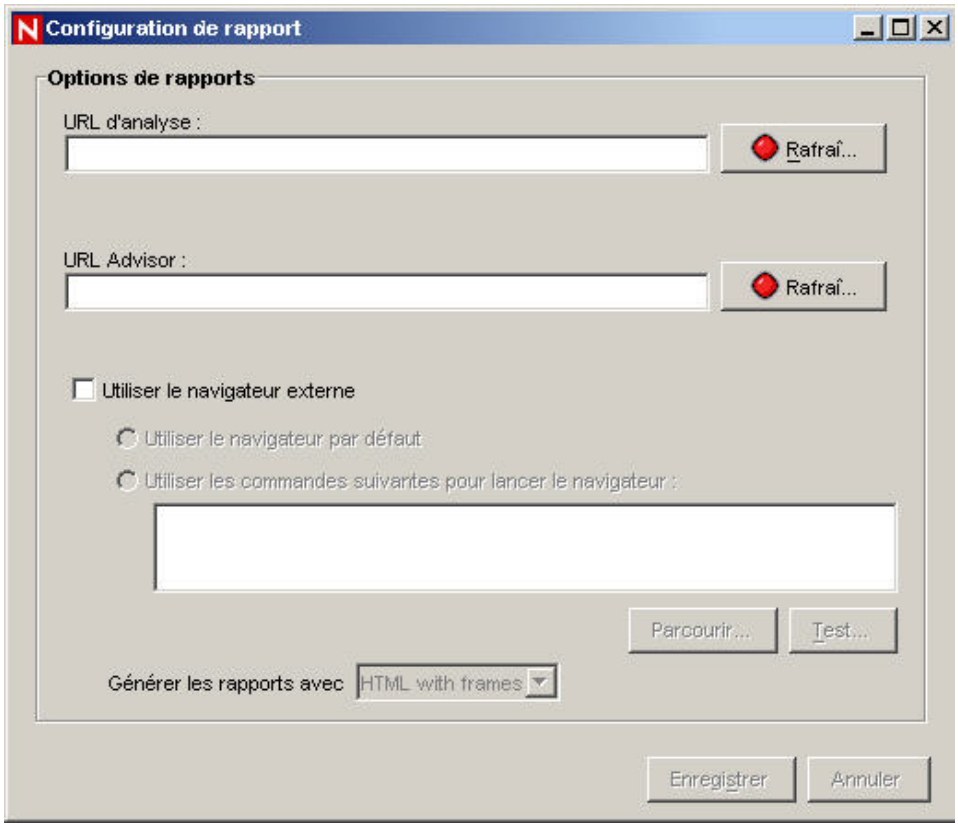
**REMARQUE** : <IP> correspond à l'adresse IP du serveur Crystal Enterprise Server.

   - Dans la zone URL d'Advisor, entrez l'URL de Crystal Enterprise Server, puis cliquez sur *Rafraîchir*.

     ```
     http://<IP>/GetReports.asp?ASP=<IP>&user=Guest&passwor
        d=&tab=Advisor
     ```

**REMARQUE** : <IP> correspond à l'adresse IP de Crystal Enterprise Server.

Pour plus d'informations, reportez-vous au *guide d'installation*.



L'option Utiliser le navigateur externe vous permet de choisir entre votre navigateur par défaut ou un autre navigateur. Si vous utilisez un autre navigateur, la ligne de commande doit se terminer par le paramètre %URL%. Par exemple :

```
C:\Program Files\Internet Explorer\IEXPLORE.EXE %URL%
```

4. Attendez que le bouton Rafraîchir devienne vert, puis cliquez sur Enregistrer. Vous devrez vous déconnecter du Centre de contrôle Sentinel, puis vous y reconnecter.

# Règles de corrélation Sentinel

La fonction de corrélation améliore la gestion des événements de sécurité en vous permettant d'automatiser l'analyse des flux d'événements entrants en vue de rechercher des modèles pertinents. Cette fonction vous permet de définir des règles qui identifient les menaces critiques et les modèles d'attaque complexes de sorte que vous puissiez classer les événements par priorité ainsi que gérer les incidents et y répondre avec efficacité.

Les dossiers de règles regroupent de façon logique les règles de corrélation. Ce regroupement permet aussi de disposer d'un ensemble de règles qui s'exécute pendant les heures de travail et d'un ensemble qui s'exécute la nuit ou le week-end. En d'autres termes, cela vous permet de surveiller des activités différentes en fonction de l'heure de la journée.

Par exemple, vous pouvez activer des règles de corrélation de jour qui s'exécutent à 8h00 du lundi au vendredi et, au même moment, désactiver les règles de corrélation de nuit. En outre, si le regroupement de règles de corrélation ne vous est pas utile, vous pouvez ne créer qu'un dossier de règles destiné à accueillir toutes les règles de corrélation que vous créez.

Le nombre d'utilisateurs pouvant accéder aux règles de corrélation n'est pas limité. Lorsque plusieurs utilisateurs modifient la même règle, les modifications enregistrées en dernier supplantent les précédentes.

Cette section aborde les sujets suivants :



**REMARQUE** : vous ne pouvez pas établir de corrélation à partir d'une valeur null (vide).

## Dossiers de règles et règles

La relation entre les dossiers de règles et les règles est définie comme suit. Les dossiers de règles et les règles s'affichent en ordre hiérarchique dans la fenêtre Règles de corrélation.

- Un dossier de règles peut contenir plusieurs règles ou aucune.
- Le nombre de dossiers de règles et de règles n'est limité que par l'espace disque disponible (stockage).
- Le fait de double-cliquer sur un dossier de règles affiche l'éditeur de règles correspondant au type de règle de corrélation que le dossier contient.

- Le chemin d'accès d'un dossier de règles est limité à 255 caractères tout comme le nom d'une règle est limité à 255 caractères.
- Les descriptions des dossiers de règles et des règles sont limitées à 1 024 caractères.

## Types des règles de corrélation

Lorsque vous définissez une règle de corrélation, vous pouvez choisir parmi les quatre types de règles de corrélation disponibles. Ces types sont les suivants :

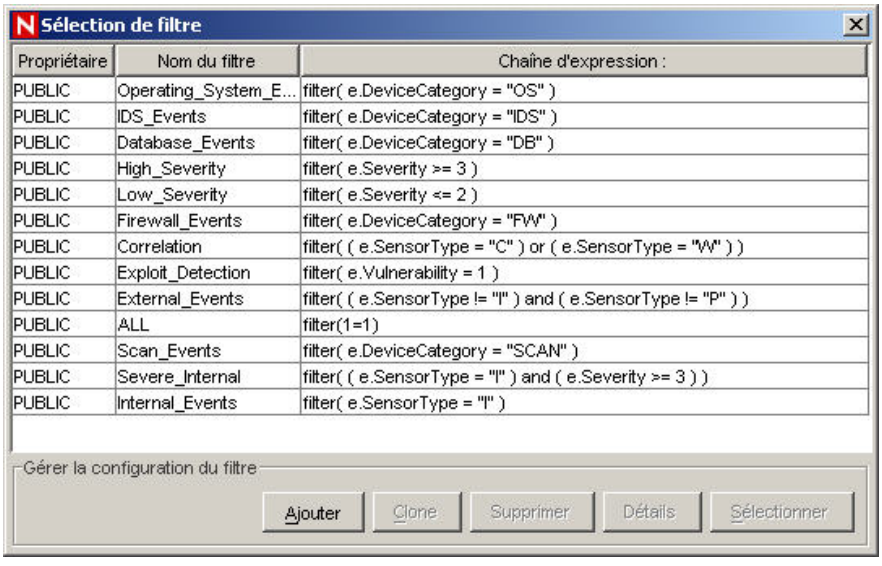
- Liste de surveillance
- Corrélation de base
- Corrélation avancée
- RuleLg libre

**ATTENTION :** l'utilisation de ce type de règle de corrélation exige la connaissance préalable du langage RuleLg. En outre, si vous avez renommé une balise, n'utilisez pas le nom d'origine pour créer une règle de corrélation avec le langage RuleLg.

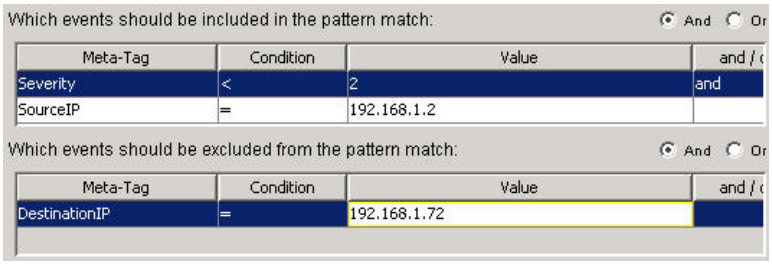
### Liste de surveillance

Quatre types de filtres sont disponibles. Ces types sont les suivants :

- Allow All (autoriser tout) : laisse passer tous les événements.
- Pattern (modèle) : toute expression générique dont la syntaxe est similaire à celle d'une commande Grep.
- Filter Manager (gestionnaire de filtres) : liste déroulante qui permet de sélectionner ou de créer un filtre.




- Builder (générateur) : permet de créer des critères d'inclusion ou d'exclusion d'événements en fonction d'opérateurs booléens. Deux volets (d'inclusion et d'exclusion) sont disponibles. Entrez-y vos valeurs, par exemple :




### Corrélation de base

Quatre types de filtres sont disponibles. Ces types sont les suivants :

- Allow All (autoriser tout) : laisse passer tous les événements.
- Pattern (modèle) : toute expression générique dont la syntaxe est similaire à celle d'une commande Grep.
- Filter Manager (gestionnaire de filtres) : liste déroulante qui permet de sélectionner ou de créer un filtre.
- Builder (générateur) : permet de créer des critères d'inclusion ou d'exclusion d'événements en fonction d'opérateurs booléens.

Cette règle permet de compter le nombre de fois que des conditions sont remplies sur une durée déterminée.

Par exemple, une règle de corrélation de base peut rechercher la même adresse IP source signalée cinq fois en cinq minutes, même si les événements sont signalés par des dispositifs différents, par exemple un système de détection d'intrusion et un pare-feu.

### Corrélation avancée

Quatre types de filtres sont disponibles. Ces types sont les suivants :

- Allow All (autoriser tout) : laisse passer tous les événements.
- Pattern (modèle) : toute expression générique dont la syntaxe est similaire à celle d'une commande Grep.
- Filter Manager (gestionnaire de filtres) : liste déroulante qui permet de sélectionner ou de créer un filtre.
- Builder (générateur) : permet de créer des critères d'inclusion ou d'exclusion d'événements en fonction d'opérateurs booléens.

Cette règle vous permet :

- de compter combien de fois des conditions sont remplies pendant une durée déterminée.
- d'incorporer toutes les fonctions d'une règle de corrélation simple ainsi que de comparer tous les événements aux événements passés.

Par exemple, une règle de corrélation avancée peut rechercher des événements portant le même nom, émanant de la même adresse IP et destinés à la même adresse IP, qu'ils se soient produits à l'intérieur ou à l'extérieur du pare-feu (ce qui signifie que l'attaque a peut-être réussi à traverser le pare-feu).

### Règle de corrélation RuleLg libre

Le langage de définition de règle de corrélation RuleLg vous permet de définir entièrement les règles de corrélation. L'utilisation de ce type de règle de corrélation exige un minimum de connaissances en matière de langage de définition de règle de corrélation RuleLg.

## Déploiement du moteur de règles de corrélation

Pour utiliser cette fonctionnalité, vous devez disposer de l'autorisation Start/Stop Correlation Engine (Démarrage/Arrêt du moteur de corrélation). Le moteur de corrélation peut avoir l'état activé ou désactivé. L'icône indique son état actuel.

- Activé - 
- Désactivé - 

Lorsque le moteur de corrélation est activé, cela signifie qu'il est en train de traiter les dossiers de règles de corrélation.

Lorsqu'il est désactivé, toutes ses données en mémoire sont conservées et aucun nouvel événement de corrélation n'est généré. Cet état équivaut à la désactivation de tous les dossiers de règles. La désactivation du moteur de corrélation n'a aucune incidence sur les autres parties du système. Les événements entrants transitent toujours et remplissent la base de données Sentinel.

## Importation et exportation des règles de corrélation

La fonction d'exportation permet à Sentinel de créer et d'exporter des règles de corrélation prêtes à l'emploi que vous pouvez importer dans votre système. Il s'agit de documents XML formatés spécifiquement pour le moteur de corrélation. Ces règles prêtes à l'emploi sont conçues par Sentinel et sont disponibles depuis le portail client à l'adresse http://www.esecurityinc.com.

Le fait de pouvoir exporter ces règles en tant que documents XML vous permet de vous appuyer sur l'aide de Novell pour la mise au point de vos règles de corrélation. L'exportation est également utile lorsque vous exécutez Sentinel dans un environnement de production et un environnement de développement. Ainsi, vous pouvez développer et tester des règles de corrélation dans l'environnement de développement, puis les exporter vers l'environnement de production. Un fichier de règles de corrélation exporté porte l'extension .crf.

## Rôle de la base de données lors du stockage des règles de corrélation

Lorsque vous activez le moteur de corrélation, qui est un processus serveur Sentinel, au sein du Centre de contrôle Sentinel, celui-ci demande les informations sur le déploiement et les règles auprès de la base de données. Lorsque vous modifiez et enregistrez une règle de corrélation et l'enregistrez, elle est envoyée à la base de données en vue d'être stockée. Les modifications apportées à la règle ne seront répercutées dans le moteur de corrélation que si l'une des conditions suivantes est remplie :

- la règle déployée est désactivée, puis activée ;
- la règle vient tout juste d'être déployée.

Lorsque vous modifiez des règles de déploiement, puis les enregistrez, elles sont transmises à la base de données pour y être stockées ainsi que vers le moteur de corrélation qui les utilisera.

## Conditions logiques des règles de corrélation

Lors de la création de règles de corrélation, les conditions logiques suivantes sont utilisées. Pour plus d'informations sur les balises META, reportez-vous au *Guide des références utilisateur de Sentinel*.

| Condition | Champ Type | Description |
|---|---|---|
| = | numérique<br>chaîne | Le contenu de la balise META sélectionné est égal à la valeur entrée. |
| != | numérique<br>chaîne | Le contenu de la balise META sélectionné est différent de la valeur entrée. |
| < | numérique | Le contenu de la propriété sélectionnée est inférieur à la valeur entrée. |
| > | numérique | Le contenu de la balise META sélectionnée est supérieur de la valeur entrée. |
| <= | numérique | Le contenu de la balise META sélectionnée est inférieur ou égal à la valeur entrée. |
| >= | numérique | Le contenu de la balise META sélectionnée est supérieur ou égal à la valeur entrée. |
| =Balise META | numérique<br>chaîne | Le contenu de la balise META sélectionnée dans la liste déroulante à gauche est égal au contenu de la balise META sélectionnée à droite de l'expression. |
| !=Balise META | numérique<br>chaîne | Le contenu de la balise META sélectionnée dans la liste déroulante à gauche est différent du contenu de la balise META sélectionnée à droite de l'expression. |
| <Balise META | numérique | Le contenu de la balise META sélectionnée dans la liste déroulante à gauche est inférieur au contenu de la balise META sélectionnée à droite de l'expression. |
| >Balise META | numérique | Le contenu de la balise META sélectionnée dans la liste déroulante à gauche est supérieur au contenu de la balise META sélectionnée à droite de l'expression. |
| <=Balise META | numérique | Le contenu de la balise META sélectionnée dans la liste déroulante à gauche est inférieur ou égal au contenu de la balise META sélectionnée à droite de l'expression. |
| >=Balise META | numérique | Le contenu de la balise META sélectionnée dans la liste déroulante à gauche est supérieur ou égal au contenu de la balise META sélectionnée à droite de l'expression. |
| =Regex | numérique<br>chaîne | Utilisez, pour la valeur, un point (.) et un astérisque (*) dans la chaîne. |
| Subnet | numérique<br>chaîne | Une opération de correspondance de sous-réseau aboutira si l'adresse IP en cours de comparaison fait partie du même sous-réseau que celui spécifié dans l'opération de correspondance de sous-réseau. |

## Ouverture de la fenêtre Règles de corrélation

La fenêtre Règles de corrélation propose les options suivantes :

- Nouveau dossier : permet de créer un nouveau dossier de règles.
- Nouvelle règle : permet de créer une règle pour un dossier de règles.
- Copier un dossier de règles : permet de modifier un dossier de règles ou des règles tout en préservant le dossier ou la règle d'origine.
- Supprimer un dossier de règles ou une règle : vous ne pouvez pas récupérer un dossier de règles ou une règle après avoir confirmé sa suppression.
- Renommer : permet de renommer une règle ou un dossier de règles.
- Importer un dossier de règles : ouvre une fenêtre de navigateur.
- Exporter un dossier de règles : une fenêtre de navigateur s'ouvre pour l'exportation du dossier de règles dans un fichier XML.
- Modifier : permet de modifier des propriétés de règles et de dossiers et d'afficher l'aperçu de vos modifications.

### Ouverture de la fenêtre Règles de corrélation

1. Cliquez sur l'onglet *Admin*.
2. Dans le *navigateur*, cliquez sur *Règles de corrélation*.

## Copie et création d'un dossier de règles ou d'une règle

### Création d'un dossier de règles

1. Ouvrez la fenêtre Règles de corrélation
2. Sélectionnez le dossier parent qui contiendra le nouveau dossier.
3. Cliquez avec le bouton droit sur le dossier parent, puis cliquez sur *Nouveau dossier*.
4. Tapez le nom du dossier de règles. Ce nom, qui respecte la casse, ne doit pas dépasser 255 caractères ni comporter de point (.).
5. (Facultatif) Tapez une description, dans la limite de 1 024 caractères.
6. Cliquez sur OK.

### Création d'une règle

1. Sélectionnez le dossier parent qui contiendra la nouvelle règle.
2. Cliquez avec le bouton droit sur le dossier parent, puis cliquez sur Nouvelle règle.
3. L'Assistant de règle de corrélation s'ouvre. Sélectionnez l'un des types de règles suivant :
   - Liste de surveillance
   - Corrélation de base
   - Corrélation avancée
   - RuleLg libre

   **REMARQUE :** pour obtenir une description de chaque type de règle, reportez-vous à la section Types des règles de corrélation.
4. Cliquez sur *Terminer*.

## Suppression d'un dossier de règles de corrélation ou d'une règle

Suppression d'un dossier de règles de corrélation ou d'une règle

1. Ouvrez la fenêtre Règles de corrélation.
2. Sélectionnez le dossier de règles ou la règle à supprimer.
3. Cliquez avec le bouton droit sur le dossier ou la règle, puis cliquez sur *Supprimer*.
4. Un message de confirmation apparaît :
   - Oui : si vous supprimez un dossier de règles, toutes les règles qu'il contient seront également supprimées. Vous ne pouvez pas récupérer une règle supprimée après avoir cliqué sur *OK*.
   - Non : permet de revenir à la fenêtre Règles de corrélation.

## Importation ou exportation d'un dossier de règles de corrélation

Importation ou exportation d'un dossier de règles de corrélation

1. Ouvrez la fenêtre Règles de corrélation.
2. Sélectionnez un dossier de règles.
3. Cliquez avec le bouton droit sur le dossier, puis cliquez sur [*Dossier de règles d'importation ou Dossier de règles d'exportation*]
   - Importer : un navigateur de fichiers s'ouvre. Accédez au dossier de règles à importer, puis cliquez sur *OK*.
   - Exporter : un navigateur de fichiers s'ouvre. Accédez au périphérique cible dans lequel écrire le dossier de règles, puis cliquez sur *OK*. Le dossier de règles est exporté dans un fichier doté de l'extension crf.

## Modification au sein de la fenêtre Corrélation

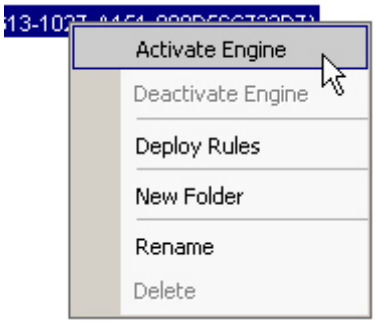
Modification d'une règle dans la fenêtre Corrélation

1. Ouvrez la fenêtre Règles de corrélation.
2. Cliquez avec le bouton droit, puis cliquez sur *Éditer*.
3. Modifiez la règle, puis cliquez sur *Terminer*.

## Activation ou désactivation d'un moteur de corrélation

Activation ou désactivation d'un moteur de corrélation

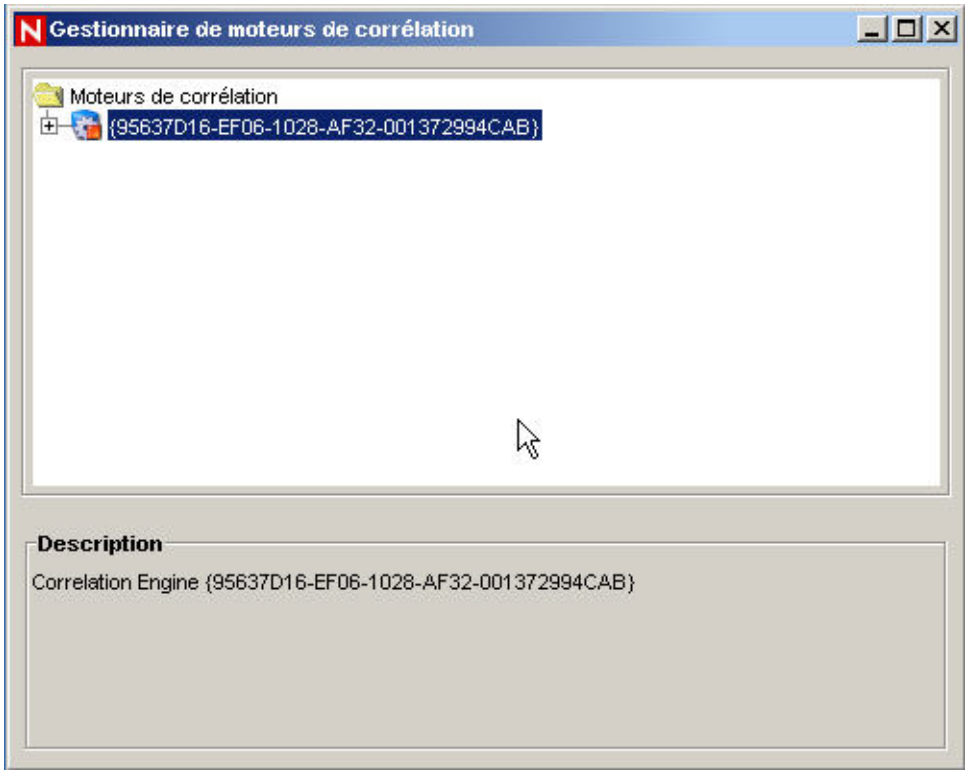
1. Ouvrez la fenêtre Gestionnaire de moteurs de corrélation.
2. Sélectionnez un *moteur de corrélation*, cliquez sur celui-ci avec le bouton droit, puis cliquez sur *Activer le moteur ou Désactiver le moteur*.



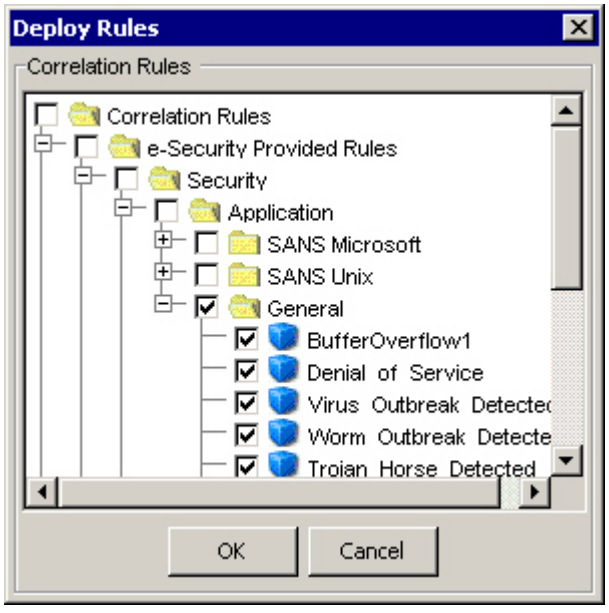

## Déploiement de règles de corrélation

Déploiement de règles de corrélation

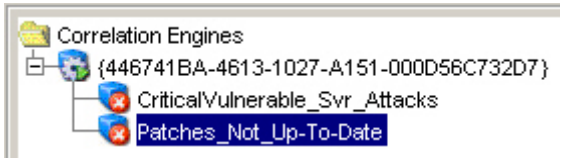
1. Ouvrez la fenêtre Gestionnaire de moteurs de corrélation.




2. Cliquez avec le bouton droit (sur un dossier de la fenêtre ou sélectionnez le moteur vers lequel déployer la règle), puis cliquez sur *Déployer les règles*.
3. Cochez les règles à déployer. Cliquez sur *OK*.

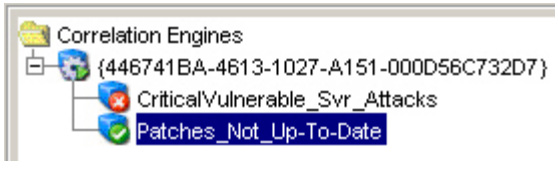



4. Pour démarrer la règle, vous devez la placer sous un moteur de corrélation.




**REMARQUE** : les règles sont prêtes au déploiement.

5. Sous le moteur de corrélation, sélectionnez la règle, cliquez avec le bouton droit sur celle-ci, puis cliquez sur *Activer la règle*.



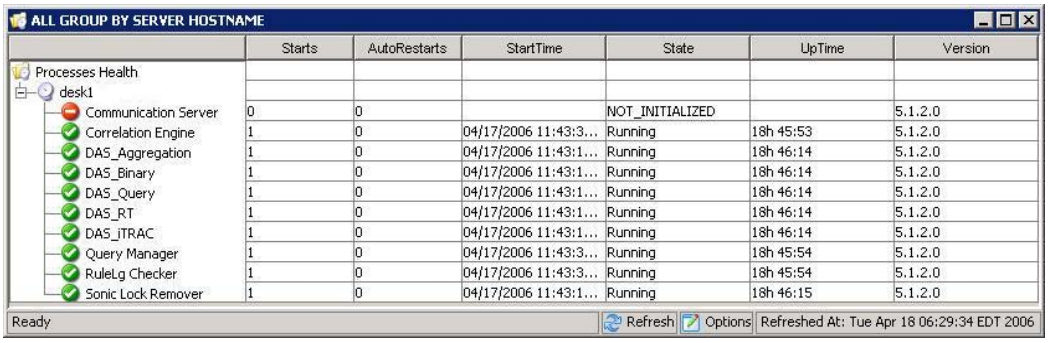

# Vues du serveur

Les vues du serveur vous permettent d'effectuer les opérations suivantes :

- Surveiller le statut de tous les processus du serveur Sentinel sur l'intégralité du système :
  - Serveur de communication
  - Moteur de corrélation
  - DAS_Binary
  - DAS_iTrac
  - DAS_Query
  - DAS (RT)
  - Query Manager
  - RuleLg Checker
  - Sonic Lock Remover

**REMARQUE** : sous Windows, le serveur de communication est exécuté en tant que Service Windows et, par conséquent, ne peut pas être contrôlé par le biais de la fonctionnalité de vue du serveur. Pour contrôler le serveur de communication sous Windows, utilisez le Gestionnaire de services Windows.

Le processus Sonic Lock Remover est uniquement activé sous Windows. Lorsqu'un processus n'est pas activé sur un serveur donné, sa colonne Activé est définie à « 0 » et sa colonne État apparaît comme NON_INITIALISEE.




- Démarrer, arrêter ou redémarrer les processus : ces actions peuvent être entreprises en cliquant via le bouton droit sur l'entrée de processus correspondante.

**REMARQUE** : les actions effectuées en cliquant avec le bouton droit ne sont pas activées pour le serveur de communication car l'arrêt de ce dernier entraînerait un perte de contact avec tous les processus.

Dans le contexte d'une vue serveur, les termes Démarrages et Redémarrages automatiques sont définis comme ceci :

- Démarrages : nombre de fois qu'un processus a été démarré, quelle qu'en soit la raison. Il peut s'agir de démarrages initiés par l'utilisateur par l'intermédiaire de l'interface ou de démarrages automatiques.
- Redémarrages automatiques : nombre de fois qu'un processus a été démarré automatiquement. Ceci ne s'applique qu'aux scénarios de redémarrage automatique et non aux redémarrages initiés par l'utilisateur. Ce champ est utile pour déterminer si le processus a été suspendu (par exemple, en raison d'une erreur) et s'il a été redémarré par Sentinel Watchdog.

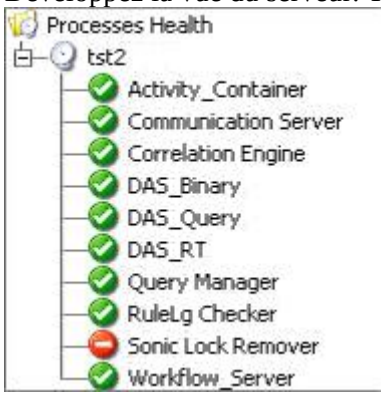
## Surveillance d'un processus

Surveillance d'un processus

1. Cliquez sur l'onglet *Admin*.
2. Cliquez sur *Vues du serveur*.

3. Double-cliquez sur le nom d'une vue. Une vue apparaît.

4. Développez la vue du serveur. Tous les processus sont répertoriés.




## Création d'une vue du serveur

Création d'une vue du serveur

1. Cliquez sur l'onglet *Admin*.
2. Cliquez sur *Vues du serveur*.

3. Pour créer une nouvelle vue, cliquez sur *Ajouter une vue*.
   - Entrez votre nom d'option.
   - Pour sélectionner les champs à afficher, cliquez sur *Champs*.
   - Pour regrouper des titres, cliquez sur *Groupe*.
   - Pour appliquer un tri en fonction des titres, cliquez sur *Trier*.
   - Pour appliquer un filtre, cliquez sur *Filtre*.
4. Cliquez sur *OK*, puis sur *Enregistrer*.

## Démarrage, arrêt et redémarrage de processus

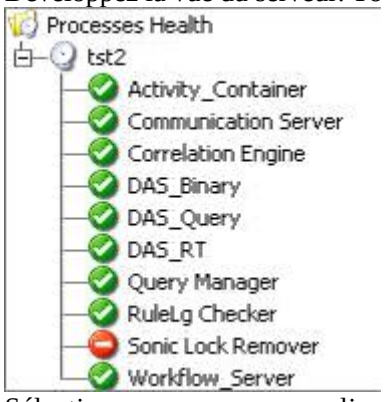
Vous ne pouvez pas arrêter le serveur avec cette fonctionnalité.

Démarrage, arrêt et redémarrage de processus

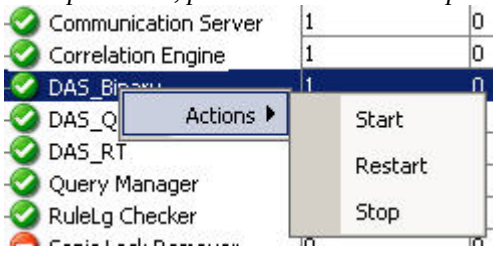
1. Cliquez sur l'onglet *Admin*.
2. Cliquez sur *Vues du serveur*.

3. Double-cliquez sur le nom d'une vue. Une vue apparaît.

4. Développez la vue du serveur. Tous les processus sont répertoriés.




5. Sélectionnez un processus, cliquez avec le bouton droit sur *celui-ci, cliquez sur Opérations, puis sélectionnez une option (Démarrer, Redémarrer ou Arrêter).*




# Filtres

Les filtres permettent de traiter des données en fonction de critères spécifiques relatifs à des événements en temps réel ou des utilisateurs du système. Ils permettent également de gérer les données affichées dans le Centre de contrôle Sentinel. Le moteur de filtres gère la structure des données de chaque filtre de sécurité des fenêtres en temps réel d'événements. Les filtres empêchent les utilisateurs d'afficher des événements non autorisés et permettent d'ignorer les événements que les utilisateurs ne souhaitent pas afficher. Les filtres sont créés depuis l'onglet Admin du Centre de contrôle Sentinel.

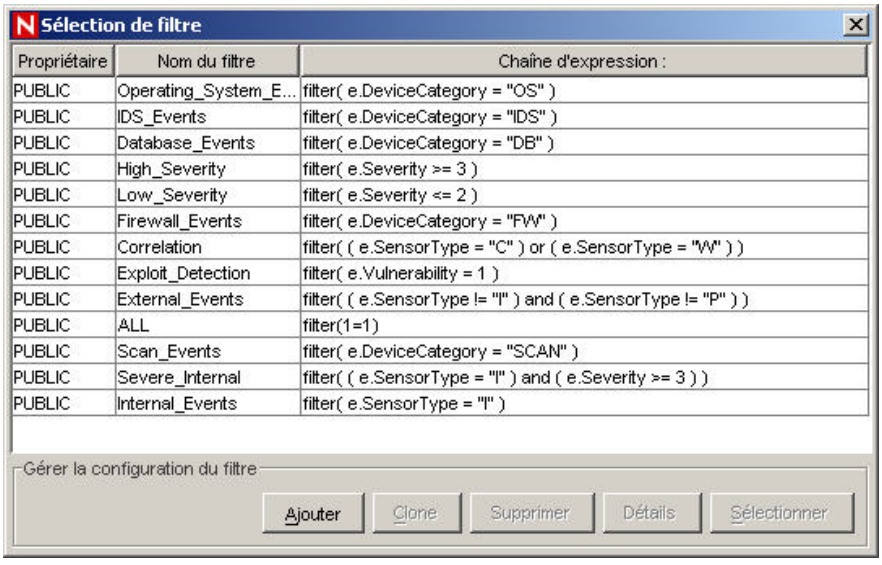
**REMARQUE** : les noms de filtres ne peuvent pas comporter les caractères suivants : $ # . * & : < >.

Il existe trois types de filtres :

- Filtres publics
- Filtres privés
- Filtres globaux

## Filtres publics

Les filtres publics appartiennent au système. Ils peuvent être utilisés en tant que filtres de sécurité ou d'affichage. Les filtres de sécurité sont basés sur les autorisations utilisateur, alors que les filtres d'affichage déterminent les événements devant apparaître dans les tables d'événements en temps réel et les graphiques.




## Filtres privés

Les filtres privés appartiennent à l'utilisateur. Il s'agit de filtres d'affichage. Ils sont partageables à condition que vous disposiez de l'autorisation View Private Filters (Affichage des filtres privés).

## Filtres globaux

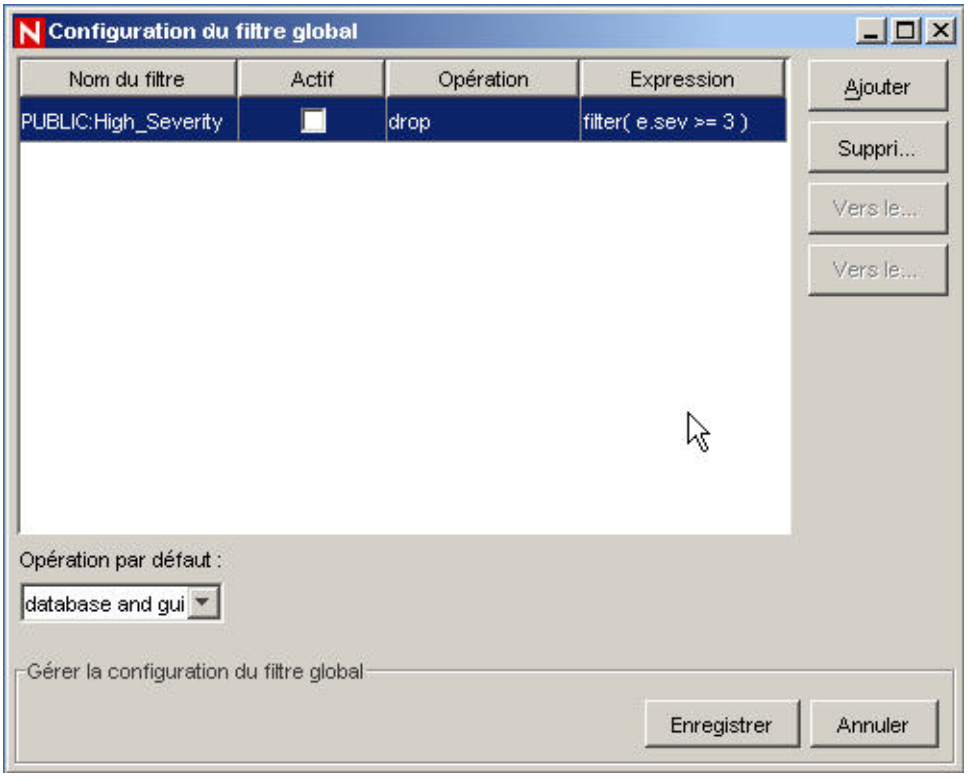
Les filtres globaux font partie de la catégorie des filtres publics. Ils sont traités séquentiellement au niveau du Gestionnaire des collecteurs pour chaque événement jusqu'à ce qu'une correspondance soit établie. L'évaluation du filtre global s'arrête à l'événement et l'action qui est associée au filtre est prise. L'ordre d'analyse des filtres globaux s'effectue de haut en bas, comme l'indique la console. Les filtres peuvent être activés ou désactivés selon les besoins.

Les filtres globaux effectuent les actions suivantes :

- Activent une action globale sur des événements, comme ignorer des événements ainsi qu'acheminer des événements vers la base de données uniquement ou vers la base de données et le Centre de contrôle Sentinel.
- Sont traités par le Gestionnaire de collecteurs de l'assistant.
- Sont configurés à partir de l'onglet Admin sous l'option Configuration du filtre global où ils peuvent être activés et désactivés.
- Peuvent ignorer des événements.
- Peuvent acheminer des événements vers la base de données uniquement.
- Peuvent acheminer des événements vers la base de données et le Centre de contrôle Sentinel.

À partir de la fenêtre Configuration du filtre global, vous pouvez effectuer les opérations suivantes :

- Création d'un filtre global
- Réorganisation d'un filtre global
- Suppression d'un filtre global




## Création d'un filtre global

Création d'un filtre global

1. Cliquez sur l'onglet *Admin*.
2. Cliquez sur *Admin > Configuration du filtre global ou sélectionnez Configuration du filtre global* dans l'arborescence.
3. Dans la fenêtre Configuration du filtre global, cliquez sur *Modifier*, puis sur *Ajouter*.
4. Dans la ligne vide, cliquez sur la *colonne Nom du filtre*.
5. Sélectionnez un filtre, cliquez sur *Sélectionner* ou *Ajouter* (si vous devez créer un filtre).
6. Dans la colonne Actif, cochez la case *Actif*.
7. Dans la colonne Action, sélectionnez l'action que le filtre doit effectuer sur les événements qu'il analyse. Si un événement ne correspond à aucun des filtres globaux actifs, c'est l'action par défaut qui détermine comment cet événement doit être traité.

   La liste déroulante Opération par défaut propose les options suivantes :

   - drop (abandonner) : les événements ne sont pas envoyés au Centre de contrôle Sentinel
     ni à la base de données Sentinel Server.
   - database (base de données) : les événements sont envoyés directement à la base de données sans passer par le Centre de contrôle Sentinel.
   - database and GUI (base de données et interface utilisateur) : les événements sont envoyés à la base de données Sentinel Server et au Centre de contrôle Sentinel.
8. Ajoutez autant de filtres que nécessaire.
9. Cliquez sur *Enregistrer*.

### Réorganisation des filtres globaux

Réorganisation des filtres globaux

1. Dans la fenêtre Configuration de filtre global, cliquez sur *Modifier*.
2. Sélectionnez un filtre, puis cliquez sur *Vers le haut* ou *Vers le bas* pour le déplacer.
3. Cliquez sur *Enregistrer*.

### Suppression d'un filtre global

**REMARQUE :** lorsque vous supprimez un filtre global, vous ne recevez pas de message de confirmation.

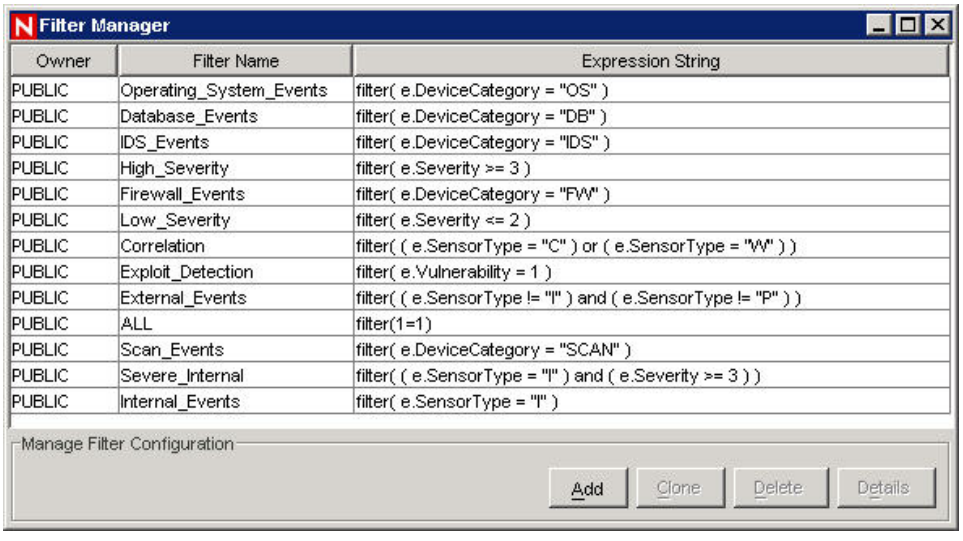
Pour supprimer un filtre global

1. Dans la fenêtre *Configuration de filtre global*, cliquez sur *Modifier*.
2. Sélectionnez un filtre dans la liste, puis cliquez sur *Supprimer*.
3. Cliquez sur *Enregistrer*.

## Configuration des filtres publics et privés

Vous pouvez effectuer les opérations suivantes sur les filtres publics et privés :

- Ajout d'un filtre
- Pour cloner un filtre
- Modification d'un filtre
- Affichage des détails d'un filtre
- Suppression d'un filtre

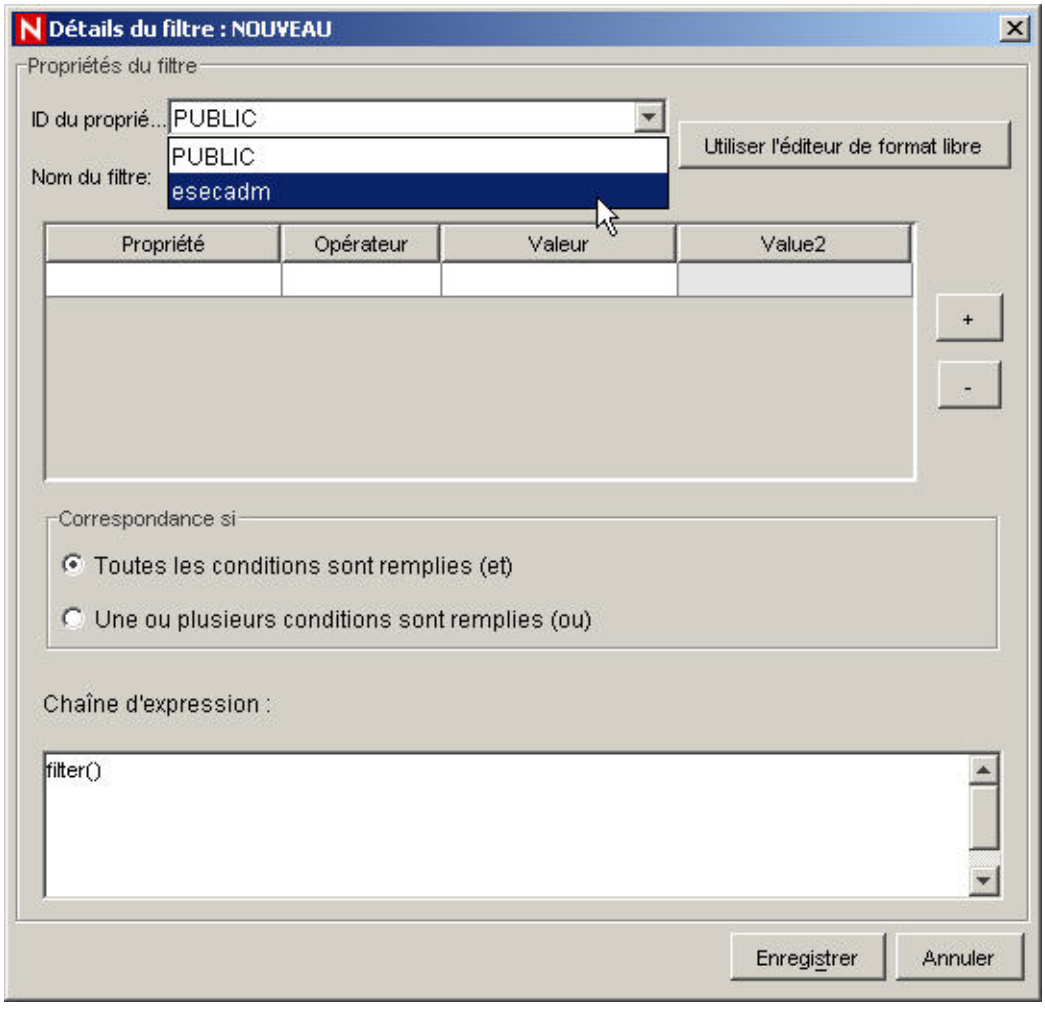



### Ajout d'un filtre

Pour ajouter un filtre public ou privé

1. Cliquez sur l'onglet *Admin*.
2. Cliquez sur *Admin > Gestionnaire de filtres ou sélectionnez Gestionnaire de filtres sous le dossier Configuration du filtre* dans l'arborescence.
3. Cliquez sur *Ajouter*.

4. Sélectionnez une valeur dans la liste déroulante ID du propriétaire (public ou privé [nom d'utilisateur]).




5. Entrez un nom de filtre.
6. L'éditeur de tables est sélectionné par défaut comme éditeur de contenu.

**REMARQUE** : vous pouvez également cliquer sur le bouton Utiliser l'éditeur libre pour afficher l'éditeur correspondant. Cet éditeur vous permet de créer des expressions complexes, ce qui n'est pas le cas de l'éditeur de tables. Sachez cependant que lorsqu'une expression a été modifiée dans l'éditeur libre, elle ne peut plus être exploitée dans l'éditeur de tables.

7. Sélectionnez les critères des colonnes suivantes :
   - Propriété
   - Opérateur
   - Valeur des colonnes

   Vos sélections apparaissent dans la zone Expression.

8. Dans la zone Correspondance si, cliquez sur l'une des options suivantes :
   - Toutes les conditions sont remplies (et)
   - Une ou plusieurs conditions sont remplies (ou)
9. Pour créer une autre expression de filtre, cliquez sur *Créer une expression de filtre* (+) pour ajouter une ligne supplémentaire à la table d'expressions de filtre.
10. Pour supprimer une expression de filtre, sélectionnez-en une dans la table, puis cliquez sur *Supprimer l'expression sélectionnée* (-).
11. Cliquez sur *Enregistrer*.

### Pour cloner un filtre public ou privé

Le clonage constitue un moyen pratique de dupliquer un filtre et de garantir la cohérence des critères au sein d'un groupe de filtres ou d'utilisateurs.

Pour cloner un filtre public ou privé

1. Ouvrez la fenêtre Gestionnaire de filtres.
2. Cliquez sur *Cloner*.
3. Entrez un nouveau nom de filtre.
4. Modifiez les critères du filtre d'origine.
5. Cliquez sur *Enregistrer*.

### Modification d'un filtre public ou privé

Pour modifier un filtre public ou privé

1. Ouvrez le Gestionnaire de filtres.
2. Sélectionnez un filtre, puis cliquez sur *Détails*.
3. Modifiez les critères du filtre d'origine. Vous ne pouvez pas modifier l'ID du propriétaire ni le *nom du filtre*.
4. Cliquez sur *Enregistrer*.

### Affichage des détails d'un filtre public ou privé

Pour afficher les détails d'un filtre public ou privé

1. Ouvrez la fenêtre *Gestionnaire de filtres*.
2. Sélectionnez un filtre, puis cliquez sur *Détails*.

### Suppression d'un filtre public ou privé

Pour supprimer un filtre public ou privé

1. Ouvrez la fenêtre *Gestionnaire de filtres*.
2. Sélectionnez un filtre, puis cliquez sur *Supprimer*.
3. Une fenêtre de confirmation s'ouvre.

# Configuration du menu

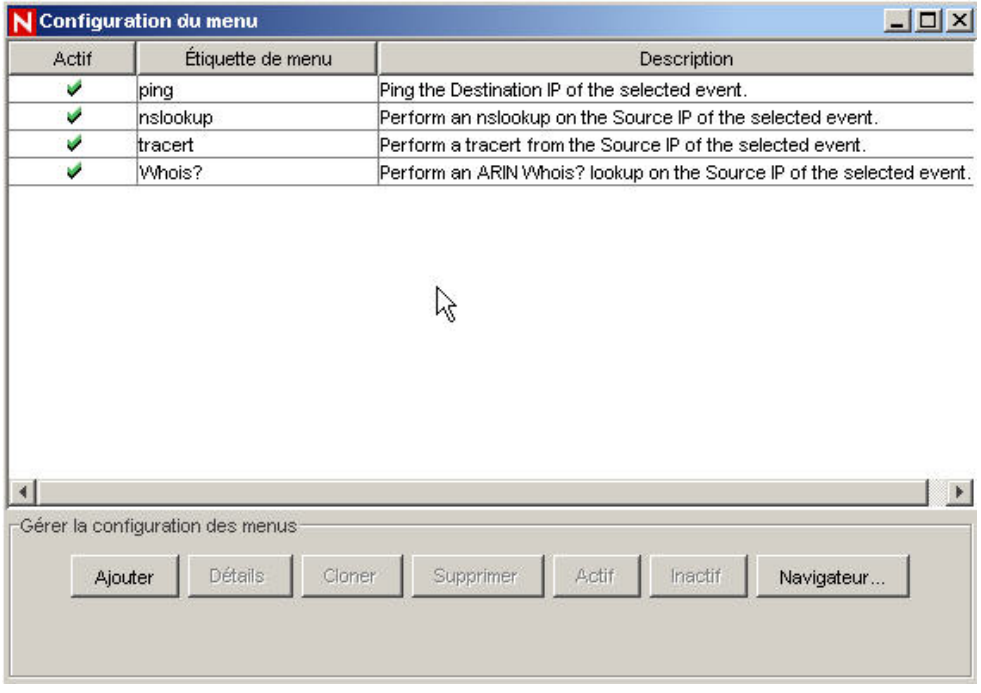
Vous devez disposer de l'autorisation Configuration du menu pour pouvoir utiliser cette fonctionnalité.

La fenêtre Configuration du menu permet de créer les éléments de menu devant apparaître dans e menu Événement, qui s'affiche sur toutes les tables comportant des événements (par exemple, les fenêtres Événement en temps réel, Instantané, Incidents, etc.). Le menu Événement est accessible lorsque vous sélectionnez un ou plusieurs événements, puis cliquez avec le bouton droit. La configuration de menu par défaut de Sentinel comporte les éléments suivants. Vous pouvez les cloner, activer ou désactiver :

- ping : interrogation ping de l'IP de destination pour l'événement sélectionné.
- nslookup : commande nslookup à exécuter sur l'IP source de l'événement sélectionné.
- traceroute (tracert sur MS SQL) : commande traceroute à exécuter de l'IP source de l'événement sélectionné vers Sentinel Server.
- Whois? : commande de recherche ARIN Whois? à exécuter sur l'IP source de l'événement sélectionné.

La fenêtre Configuration du menu vous permet d'effectuer les opérations suivantes :

- Ajout d'une option au menu Configuration des menus
- Clonage d'une option du menu Configuration des menus
- Modification d'une option du menu Configuration des menus
- Affichage des paramètres d'une option du menu Configuration des menus
- Activation ou désactivation d'une option du menu Configuration des menus
- Réorganisation des options du menu Événements
- Suppression d'une option de menu Configuration des menus
- Modification des paramètres de navigateur de la fenêtre Configuration des menus



## Ajout d'une option au menu Configuration du menu

**REMARQUE** : si vous avez renommé une balise, par exemple CustomerVar24 en PolicyName, vous devez utiliser le nouveau nom lors de la définition des paramètres.

Pour ajouter une option au menu Configuration du menu

1. Cliquez sur l'onglet *Admin*.
2. Dans le navigateur, cliquez sur *Admin* > *Configuration des menus*.
3. Dans la boîte de dialogue Configuration du menu, entrez ce qui suit :
   - Nom
   - Description
   - Opération : exécuter une commande ou lancer un navigateur.
   - Utiliser le navigateur : si vous avez choisi l'opération Exécuter une commande et si les paramètres du navigateur sont définis à Utiliser le navigateur externe (reportez-vous à la section Modification des paramètres de navigateur de la fenêtre Configuration des menus pour plus d'informations sur ces paramètres), vous pouvez sélectionner Utiliser
     le navigateur. Si vous sélectionnez cette option, la sortie générée par la commande est affichée à l'aide des paramètres définis dans cette boîte de dialogue pour le Centre de contrôle Sentinel.
   - Type de fichier : si vous avez choisi l'opération « Exécuter une commande ». les paramètres du navigateur sont définis à « Utiliser le navigateur externe ». Si vous avez sélectionné l'opération « Utiliser le navigateur », vous pouvez indiquer le type de fichier
     de la sortie générée par cette commande.
   - Commande / URL

**REMARQUE** : sous UNIX, le script/l'application ou le lien symbolique vers le script/l'application doit se trouver dans le répertoire $ESEC_HOME\sentinel\exec. Pour tout script, application ou lien symbolique, veillez à n'entrer que la commande. Tout chemin entré sera ignoré.

**REMARQUE** : sous Windows (corrélation), le script/l'application doit se trouver dans l'un des répertoires listés dans vos variables d'environnement Windows. Tout nom de chemin entré sera ignoré.

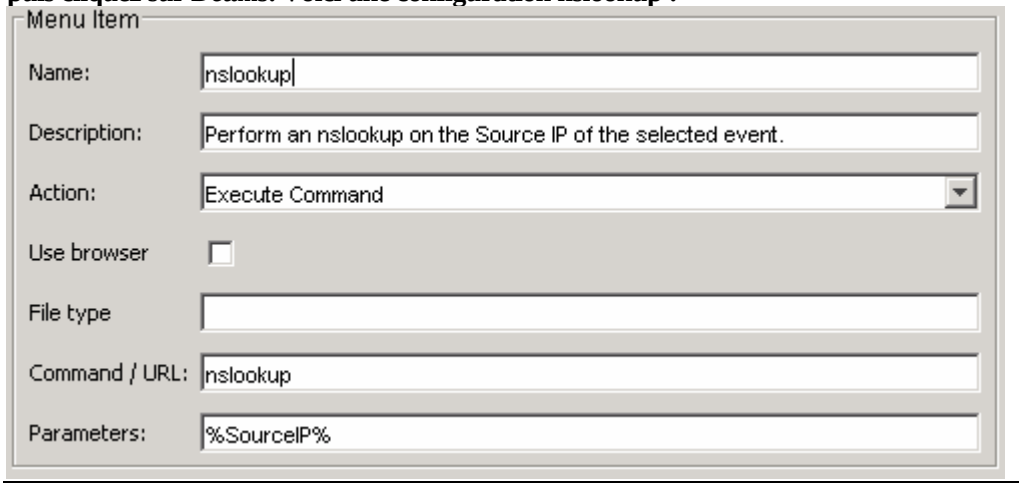
**REMARQUE** : sous Windows (non-corrélation), la saisie d'un nom de chemin est facultative. Si vous entrez une commande sans chemin, la valeur par défaut sera %ESEC_HOME%\sentinel\bin ainsi que tous les autres chemins spécifiés dans les variables d'environnement.

   - Paramètres : la valeur que vous entrez dans ce champ doit figurer entre des signes de pourcentage (par exemple, %NomÉvénement%).

**REMARQUE :** pour obtenir une liste des balises que vous pouvez utiliser lors de la spécification de paramètres, cliquez sur *Aide* dans la boîte de dialogue Configuration des menus ou reportez-vous au chapitre consacré aux balises META du *Guide des références utilisateur de Sentinel*.

4. Cliquez sur OK. L'option est ajoutée à la liste des éléments de menu de la fenêtre Configuration du menu.

REMARQUE : **à titre d'exemple, sélectionnez un des éléments de menu par défaut, puis cliquez sur *Détails*. Voici une configuration nslookup :**




## Clonage d'une option de menu Configuration du menu

Pour cloner une option du menu Configuration du menu

1. Ouvrez la fenêtre Configuration du menu.
2. Sélectionnez un élément de menu dans la table, puis cliquez sur Cloner.
3. Dans la boîte de dialogue Configuration du menu, modifiez ce qui suit :
   - Nom
   - Description
   - Opération
   - Utilisation ou non d'un navigateur. Pour plus d'informations, reportez-vous à Modification des paramètres de navigateur de la fenêtre Configuration des menus.
   - Commande / URL
   - Paramètres
   - Sélectionnez une action :
     - Exécuter une commande
     - Lancer le navigateur Web

**REMARQUE :** pour obtenir une liste des balises que vous pouvez utiliser lors de la spécification de paramètres, cliquez sur *Aide* dans la boîte de dialogue Configuration des menus ou reportez-vous au chapitre consacré aux balises META du *Guide des références utilisateur de Sentinel*.

4. Cliquez sur OK. L'option est ajoutée à la liste des éléments de menu de la fenêtre Configuration du menu.

## Modification d'une option du menu Configuration des menus

Pour modifier une option de menu Configuration des menus

1. Ouvrez la fenêtre Configuration des menus.
2. Double-cliquez sur une option de menu.
3. Tapez vos modifications, puis cliquez sur *OK*.

## Affichage des paramètres d'option du menu Configuration des menus

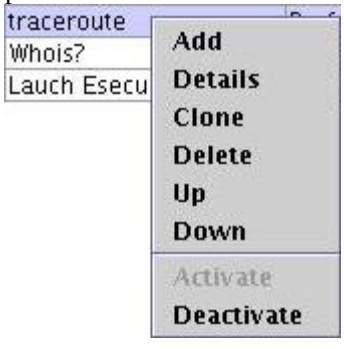
Pour afficher les paramètres d'une option du menu Configuration du menu

1. Ouvrez la fenêtre Configuration du menu.
2. Sélectionnez un élément de menu, puis cliquez sur *Détails*.

## Activation ou désactivation d'une option de menu Configuration du menu

Pour activer ou désactiver une option de menu Configuration des menus

1. Ouvrez la fenêtre Configuration des menus.
2. Sélectionnez une option de menu, cliquez avec le bouton droit sur celle-ci, puis sélectionnez Activer ou Désactiver.




## Réorganisation des options du menu Événements

Pour déplacer une option de menu Événements vers le haut ou vers le bas

1. Ouvrez la fenêtre Configuration des menus.
2. Sélectionnez une option de menu, puis cliquez sur *Vers le haut* ou *Vers le bas*.

## Suppression d'une option du menu Configuration du menu

Pour supprimer une option de menu Configuration des menus

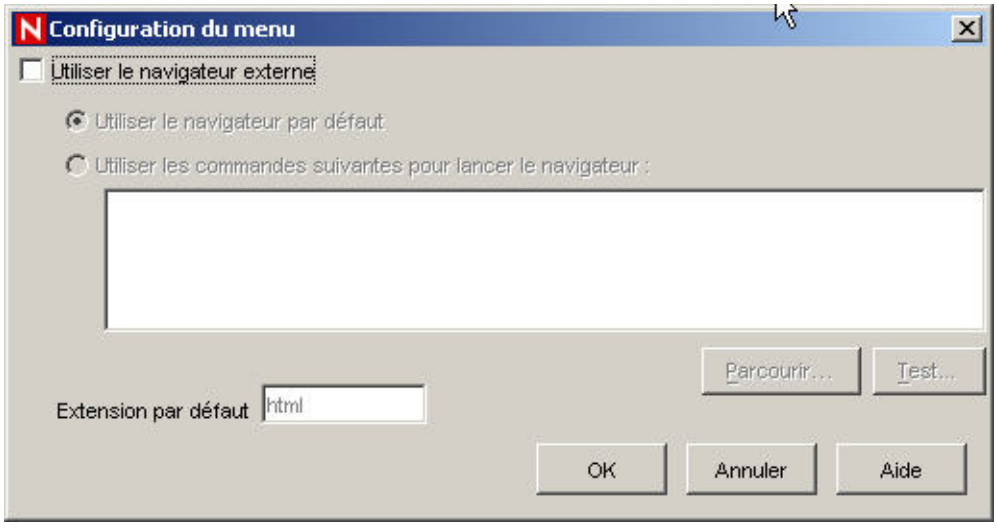
1. Ouvrez la fenêtre Configuration des menus.
2. Sélectionnez une option de menu, puis cliquez sur *Supprimer*.
   - Cliquez sur *Oui* pour confirmer la suppression.
   - Cliquez sur *Non* pour conserver l'option de menu.

## Modification des paramètres de navigateur de la fenêtre Configuration des menus

Cette option vous permet d'envoyer la sortie générée à partir de la fenêtre Configuration des menus vers un navigateur externe, quel qu'il soit. Il ne s'agit pas nécessairement d'un navigateur Internet. En changeant l'extension, vous pouvez lancer l'application associée à cette extension. Par exemple, l'extension txt est généralement associée au Bloc-notes. Vous pouvez également choisir de lancer un programme spécifique afin d'ouvrir un fichier txt dans WordPad ou un autre éditeur.

### Modification des paramètres de navigateur dans la fenêtre Configuration du menu

1. Ouvrez la fenêtre Configuration du menu.
2. Cliquez sur Navigateur.



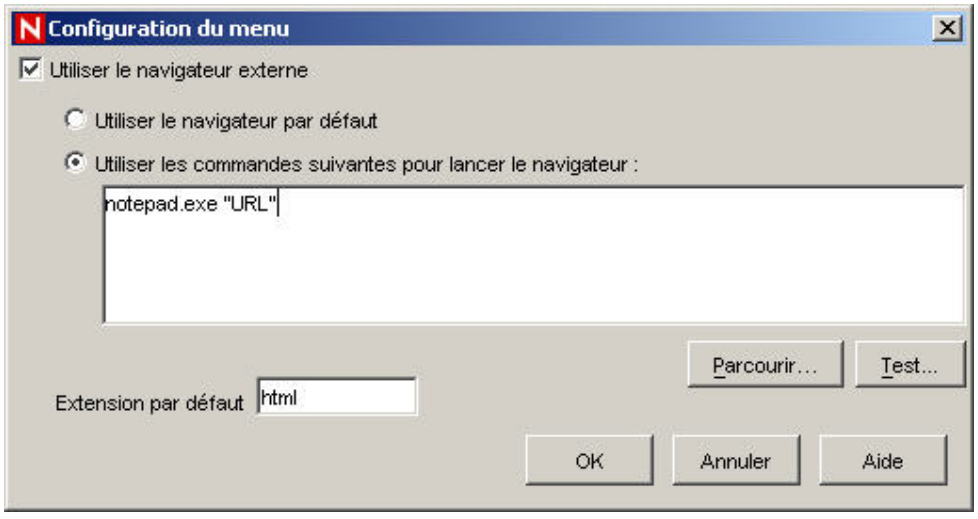

Si vous sélectionnez Utiliser le navigateur lors de la configuration du menu et activez l'option Utiliser le navigateur par défaut (comme dans l'exemple ci-dessus), l'option Configuration
du menu agit comme si la case à cocher Utiliser le navigateur n'avait pas été cochée.

Si vous avez coché l'option Utiliser le navigateur externe, vous avez le choix entre les options suivantes :

- Utiliser le navigateur par défaut : cette option permet d'utiliser le navigateur par défaut (ou l'application) associé à l'extension de fichier définie dans le champ correspondant.
- Utiliser les commandes suivantes pour lancer le navigateur : cette option vous permet d'indiquer l'application à lancer. Si vous utilisez un navigateur autre que le navigateur par défaut, la ligne de commande doit se terminer par le paramètre %URL%. Par exemple :

  ```
  C:\Program Files\Internet Explorer\IEXPLORE.EXE %URL%
  ```

Dans l'exemple suivant, le navigateur est le Bloc-notes.




3. Lorsque vous avez terminé la configuration, cliquez sur OK.

## Statistiques DAS

Cette fonctionnalité sert à la surveillance interne de votre système. Elle est destinée aux utilisateurs expérimentés. Elle permet de surveiller :

- DAS_Binary
- DAS_Query
- DAS_rt

Les statistiques sont réparties comme ceci :

- Service : nom du service, tel que DAS_Query.
- Heure : heure de la dernière mise à jour.
- Num : nombre de requêtes traitées pour cette entrée.
- Attente (sec) : temps d'attente en secondes avant que le traitement d'une requête démarre.
- Exécution (sec) : temps d'attente moyen en secondes de traitement d'une requête.
- #En attente : taille moyenne de la file d'attente.
- #En cours d'exécution : taille moyenne de la file d'exécution.

Les informations sont réparties en 3 sections :

- Requêtes
- Services
- ThreadPools (pools de threads)

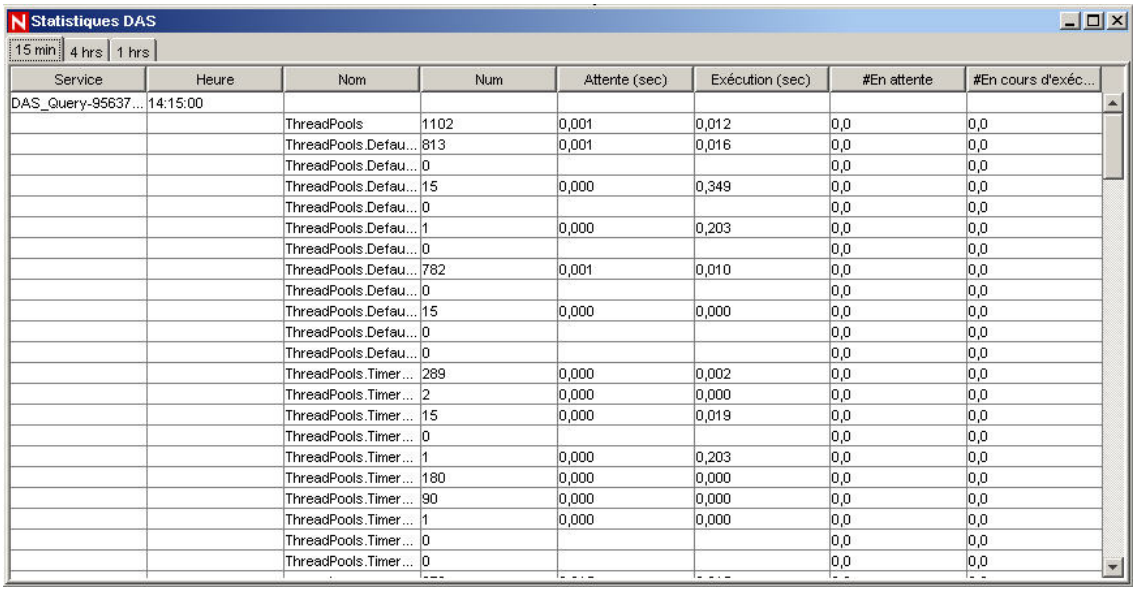
La section Requêtes regroupe les requêtes par canal (tel que services.CorrelationService).
La section Services regroupe les services. Parfois, la mention <catégorie> est ajoutée au nom, par exemple Services.CorrelationService ou Services.RemoteObjectService.EMap.getMapPK.

Dans la section Services, tous les appels de méthode distants émanant des services définis par l'utilisateur (vos services XML) sont regroupés sous services.RemoteObjectService. Le nom du service apparaît au-dessous (EMap, dans l'exemple ci-dessous), de même que le nom de la méthode (getMapPK, dans l'exemple), s'il a été requis.

Lorsqu'une requête est reçue par un serveur, DAS Query, par exemple, une tâche est créée, puis planifiée. La tâche est ensuite assignée à un pool de threads à exécuter. Plusieurs pool

de threads peuvent coexister et un pool de threads peut servir plusieurs services. C'est pour cette raison qu'une requête doit attendre qu'un thread se libère même si le service ne fait pas l'objet d'une utilisation intensive. Si les statistiques indiquent que le temps d'attente d'une requête est important et que le nombre de requêtes pour ce service est faible, vérifiez les informations relatives aux pools de threads.

Les nombres affichés en regard d'une entrée sont la somme de tous ses enfants. Ainsi, si la colonne Num indique 15 pour « requêtes », cela signifie que 15 requêtes existent pour tous les appels de méthode de requêtes. Sous « requêtes », figurent « requests.configurations 1 », qui signifie que 1 des 15 requêtes est associée aux configurations et « requests.esecurity.correlation.config 2 », qui signifie que 2 des 15 requêtes sont associées à « esecurity. correlation.config », etc.



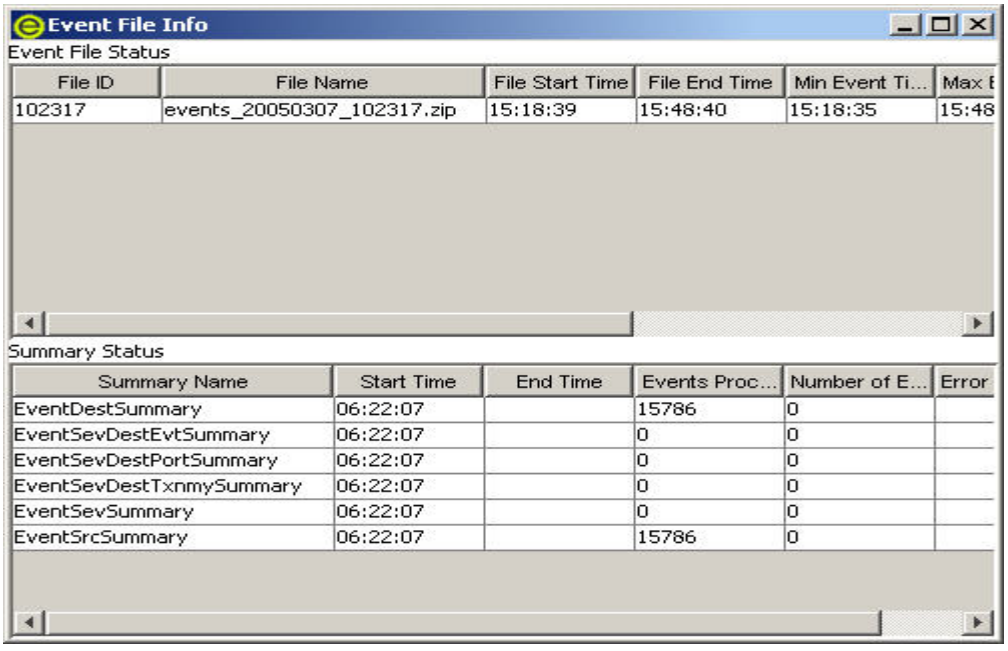

| Service | Heure | Nom | Num | Attente (sec) | Exécution (sec) | #En attente | #En cours d'exéc... |
|---|---|---|---|---|---|---|---|
| DAS_Query-95637... | 14:15:00 | | | | | | |
| | | ThreadPools | 1102 | 0,001 | 0,012 | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 813 | 0,001 | 0,016 | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 15 | 0,000 | 0,349 | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 1 | 0,000 | 0,203 | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 782 | 0,001 | 0,010 | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 15 | 0,000 | 0,000 | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defau... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 289 | 0,000 | 0,002 | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 2 | 0,000 | 0,000 | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 15 | 0,000 | 0,019 | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 1 | 0,000 | 0,203 | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 180 | 0,000 | 0,000 | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 90 | 0,000 | 0,000 | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 1 | 0,000 | 0,000 | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Timer... | 0 | | | 0,0 | 0,0 |

Ces informations peuvent être utiles, car elles montrent ce qui se passe. Le nombre de requêtes, en particulier, vous permet de visualiser où elles vont et où elles sont concentrées. La colonne #En attente est pratique, car elle indique le niveau d'activité du serveur. Ce nombre devrait être petit. S'il est élevé, les nouvelles requêtes (même celles concernant des tâches simples) devront attendre que les tâches potentiellement lentes se terminent. Cette situation n'est pas satisfaisante. Le temps d'exécution moyen est très important, car il montre les requêtes lentes par opposition à celles qui attendent les autres.

# Informations du fichier d'événements

Le volet supérieur indique les informations de statut de chaque fichier d'événements. Le statut des fichiers d'événements est tel qu'il était au moment de l'ouverture de la fenêtre. Le volet n'indique pas le statut des fichiers d'événements passés. Il indique l'ID de fichier (qui correspond à arch_id dans la table d'événements), le nom et les statistiques relatives au fichier (si ce dernier est terminé, l'heure de début et de fin de l'écriture du fichier, les heures minimale et maximale des événements contenus dans le fichier, etc.).

Lorsque vous sélectionnez un fichier d'événements dans le volet supérieur, le volet inférieur affiche un résumé du statut de ce fichier. Le volet inférieur affiche le nom du récapitulatif, les heures de début et de fin du traitement, le nombre d'événements traités et la présence ou non de messages d'erreur.




# Configuration de l'utilisateur

Pour utiliser cette fonctionnalité, vous devez disposer de l'autorisation Configuration de l'utilisateur.

La fenêtre Configuration de l'utilisateur permet d'effectuer les opérations suivantes :

- Création d'un compte d'utilisateur
- Modification d'un compte d'utilisateur
- Affichage des détails d'un compte d'utilisateur
- Clonage d'un compte d'utilisateur
- Suppression d'un compte d'utilisateur
- Arrêt d'une session active
- Ajout d'un rôle iTRAC
- Suppression d'un rôle iTRAC
- Affichage des détails d'un rôle

Le programme d'installation crée les utilisateurs par défaut suivants sur le serveur Sentinel :

### Authentification Oracle et MS SQL:

- esecdba : propriétaire du schéma (configurable lors de l'installation).
- esecadm : utilisateur administrateur de Sentinel (configurable lors de l'installation).

**REMARQUE** : sous UNIX, le programme d'installation crée un utilisateur du système d'exploitation doté du même nom d'utilisateur et du même mot de passe.

- esecrpt : utilisateur des rapports, même mot de passe que l'utilisateur admin.
- ESEC_CORR : utilisateurs des moteurs de corrélation, chargés de créer les incidents.
- esecapp : nom de l'utilisateur de l'application Sentinel pour la connexion à la base de données.

## Authentification Windows :

- Administrateur de la base de données Sentinel : propriétaire du schéma (configurable lors de l'installation).
- Administrateur Sentinel : utilisateur administrateur de Sentinel (configurable lors de l'installation).
- Utilisateur des rapports Sentinel : utilisateur des rapports, même mot de passe que l'utilisateur admin.
- Utilisateur de la base de données de l'application Sentinel : nom d'utilisateur de l'application Sentinel pour la connexion à la base de données.

## Ouverture de la fenêtre Gestionnaire d'utilisateurs

Pour ouvrir la fenêtre Gestionnaire d'utilisateurs

1. Cliquez sur l'onglet *Admin*.
2. Cliquez sur *Admin > Configuration de l'utilisateur*.

## Création d'un compte d'utilisateur

**REMARQUE** : pour satisfaire les exigences strictes en matière de configuration de la sécurité de la certification CC (Common Criteria), Sentinel requiert 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 facile à mémoriser et complexe à la fois. Par exemple, Mf1l$a5!A (mon fils a 5 ans) OU J!hb1tE75 (j'habite à Paris).

Vous devez disposer de l'autorisation Create User Account (Création d'un compte d'utilisateur) pour pouvoir utiliser cette fonction. Les autorisations utilisateur sont assez bien documentées. Reportez-vous à la section consacrée aux *autorisations utilisateur du Guide des références utilisateur de Sentinel*.

**REMARQUE** : le mot de passe de l'utilisateur esecrpt doit être changé directement dans la base de donnée. Vous pouvez utiliser Enterprise Manager pour cela.

Pour créer un compte d'utilisateur

1. Ouvrez la fenêtre Gestionnaire d'utilisateurs.
2. Cliquez sur *Ajouter un nouvel utilisateur*,


ou sélectionnez un utilisateur, cliquez avec le bouton droit sur celui-ci, puis cliquez sur *Ajouter un utilisateur*.


3. Sous Autorisation, remplissez les champs suivants :
   - Nom d'utilisateur
   - Mot de passe
   - Confirmer le mot de passe
   - Filtre de sécurité : pour sélectionner un filtre de sécurité, cliquez sur la flèche vers le bas. La fenêtre Sélection de filtre s'ouvre. Sélectionnez un filtre ou cliquez sur *Ajouter* pour créer un filtre pour ce compte d'utilisateur.

---

**REMARQUE** : une fois qu'un filtre de sécurité a été assigné à un utilisateur, vous ne pouvez plus le supprimer.

---

   - Cliquez sur Sélectionner.

---

**REMARQUE** : il est vivement recommandé d'utiliser des mots de passe comportant au moins 8 caractères, dont des caractères alphanumériques.

---

   (Facultatif) Sous Détails, renseignez les champs suivants :
   - Prénom
   - Nom
   - Service
   - Téléphone
   - Adresse électronique
4. Cliquez sur l'onglet Autorisations pour assigner des autorisations à l'utilisateur.
5. Cliquez sur l'onglet Rôles et sélectionnez le rôle de l'utilisateur.
6. Cliquez sur OK.

---

**REMARQUE :** Oracle n'autorise pas la création de noms d'utilisateur identiques aux mots réservés Oracle. En outre, Sentinel ne vous autorise pas à utiliser ces noms non plus.

---

## Modification d'un compte d'utilisateur

Vous devez disposer de l'autorisation Modify Existing User Account (Modification d'un compte d'utilisateur existant) pour pouvoir utiliser cette fonctionnalité.

**REMARQUE** : le mot de passe de l'utilisateur esecrpt doit être changé directement dans la base de données. Vous pouvez utiliser Enterprise Manager pour cela.

Pour modifier un compte d'utilisateur

1. Ouvrez la fenêtre Gestionnaire d'utilisateurs.
2. Double-cliquez sur un compte d'utilisateur ou cliquez avec le bouton droit sur celui-ci, puis cliquez sur *Détails de l'utilisateur*.
3. Modifiez le compte.
4. Cliquez sur *OK*.

## Affichage des détails d'un compte d'utilisateur

Vous devez disposer de l'autorisation Use/View User Account (Utilisation/affichage des comptes d'utilisateur) pour pouvoir utiliser cette fonctionnalité.

Pour afficher les détails d'un compte d'utilisateur

1. Ouvrez la fenêtre Gestionnaire d'utilisateurs.
2. Double-cliquez sur un compte d'utilisateur ou cliquez avec le bouton droit sur celui-ci, puis cliquez sur Détails de l'utilisateur.
3. Consultez les détails, puis fermez la fenêtre.

## Clonage d'un compte d'utilisateur

Pour cloner un compte d'utilisateur

1. Ouvrez la fenêtre Gestionnaire d'utilisateurs.
2. Sélectionnez un ID de compte d'utilisateur, cliquez avec le bouton droit sur celui-ci, puis cliquez sur *Cloner l'utilisateur*.
3. Modifiez les informations et les autorisations.
4. Cliquez sur Enregistrer.

## Suppression d'un compte d'utilisateur

Vous devez disposer de l'autorisation Delete User Account (Suppression d'un compte d'utilisateur) pour pouvoir utiliser cette fonctionnalité.

**REMARQUE** : si vous supprimez un compte utilisateur, vous ne pouvez pas recréer un compte avec le même nom. Par exemple, si vous avez créé un compte pour l'utilisateur Jean, puis supprimez ce compte, vous ne pouvez pas recréer de compte appelé Jean.

Pour supprimer un compte d'utilisateur

1. Ouvrez la fenêtre Gestionnaire d'utilisateurs.
2. Sélectionnez un ID de compte d'utilisateur, cliquez avec le bouton droit sur celui-ci, puis cliquez sur *Supprimer l'utilisateur*.

## Terminer une session active

Arrêt d'une session active

1. Ouvrez la fenêtre Sessions utilisateur actives.
2. Sélectionnez la session active que vous souhaiter terminer.
3. Cliquez avec le bouton droit sur la session, puis cliquez sur *Arrêter la session*.
4. Vous êtes invité à entrer un message. Ce message est destiné à informer l'utilisateur que vous arrêtez sa session.

## Ajout d'un rôle iTRAC

Pour ajouter un rôle iTRAC

1. Ouvrez la fenêtre Gestionnaire de rôles.
2. Cliquez sur Ajouter un nouveau rôle,


ou cliquez avec le bouton droit, puis cliquez sur *Ajouter un nouveau rôle*.

## Suppression d'un rôle iTRAC

Pour supprimer un rôle iTRAC

1. Ouvrez la fenêtre Gestionnaire de rôles.
2. Sélectionnez un rôle, cliquez avec le bouton droit sur celui-ci, puis cliquez sur Supprimer le rôle.

## Affichage des détails d'un rôle

Pour afficher les détails d'un rôle

1. Ouvrez la fenêtre Gestionnaire de rôles.
2. Sélectionnez un rôle, cliquez avec le bouton droit sur celui-ci, puis cliquez sur Détails du rôle.

# 10 Gestionnaire de données Sentinel

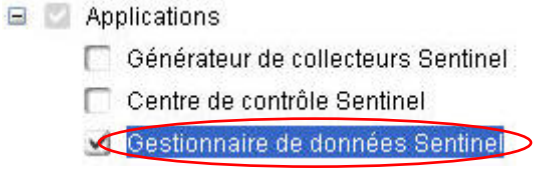
**REMARQUE** : les termes Agent et Collecteur sont interchangeables. Le terme Collecteur sera utilisé dans la suite de cette documentation.

Le Gestionnaire des données Sentinel est un outil qui permet aux utilisateurs de gérer la base de données Sentinel. et d'effectuer les opérations suivantes :

- Surveiller l'utilisation de l'espace de la base de données
- Afficher et gérer les partitions de la base de données
- Gérer les archives de la base de données
- Importer des données dans la base de données
- Configurer les assignations de données
- Configurer les noms des balises d'événements
- Configurer les paramètres de rapport de récapitulatifs

## Installation du Gestionnaire de données

Le Gestionnaire de données peut-être installé directement à l'aide de l'Assistant InstallShield de Sentinel 5 en sélectionnant le composant *Gestionnaire de données Sentinel* dans l'écran Sélection des composants de Sentinel 5.




- (Oracle seulement) Notez que pour que le Gestionnaire de données puisse communiquer avec des bases de données Oracle, vous devez aussi télécharger manuellement le pilote JDBC Oracle 9.2.0.4 ou 9.2.0.5 et copier le fichier .jar téléchargé dans le répertoire $ESEC_HOME/lib sur la machine où vous avez installé le Gestionnaire de données ou dans %ESEC_HOME%\lib si vous installez le Gestionnaire de données sur Windows. Vous pouvez télécharger le pilote JDBC à partir de l'URL suivante :

**REMARQUE :** sur une machine UNIX équipée du composant DAS, le pilote JDBC est automatiquement placé à l'endroit adéquat par le programme d'installation. Par conséquent, ce cas de figure ne requiert pas de téléchargement manuel.

http://otn.oracle.com/software/tech/java/sqlj_jdbc/index.html

Le nom habituel de ce fichier .jar est ojdbc14.jar.

**REMARQUE :** au moment de la publication de ce guide, le site Web mentionné ci-dessus était actuel.

**REMARQUE** : le Gestionnaire de données Sentinel pour Oracle nécessite l'installation d'Oracle Enterprise avec partitionnement.

# Démarrage de l'interface du Gestionnaire de données Sentinel

**REMARQUE** : pour utiliser l'interface du Gestionnaire de données, votre fichier configuration.xml doit pointer vers un serveur de communication auquel AS_Binary et DAS_Query sont connectés. Ceci est normalement le cas, par défaut, si les processus Serveur de communication et DAS s'exécutent.

Sous UNIX : démarrage de l'interface utilisateur du Gestionnaire de données Sentinel

1. Connectez-vous à l'ordinateur UNIX en tant que membre du groupe esec (par exemple : esecadm).
2. Avec la commande cd, accédez au répertoire $ESEC_HOME/sdm.
3. Entrez la ligne de commande suivante :

```
./sdm
```

Sous Windows : démarrage de l'interface utilisateur du Gestionnaire de données Sentinel

1. Cliquez sur Démarrer > Tous les programmes > Sentinel > Gestionnaire de données Sentinel.

**REMARQUE** : pour exécuter le Gestionnaire de données à partir de la ligne de commande, reportez-vous à la section Ligne de commande du Gestionnaire des données Sentinel de ce document.

## Connexion à la base de données

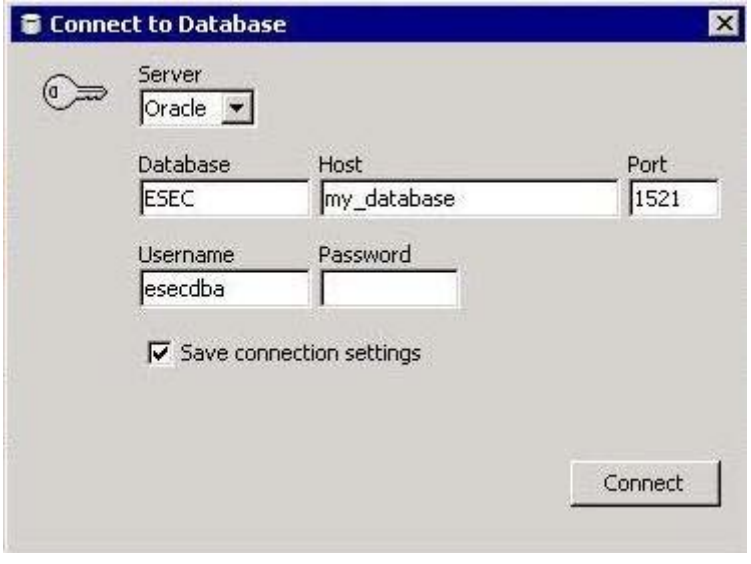
Lorsque le Gestionnaire de données démarre, vous devez établir une connexion à la base de données. Dans la boîte de dialogue *Connexion à la base de données*, entrez les valeurs appropriées dans chaque champ.

Connexion à la base de données

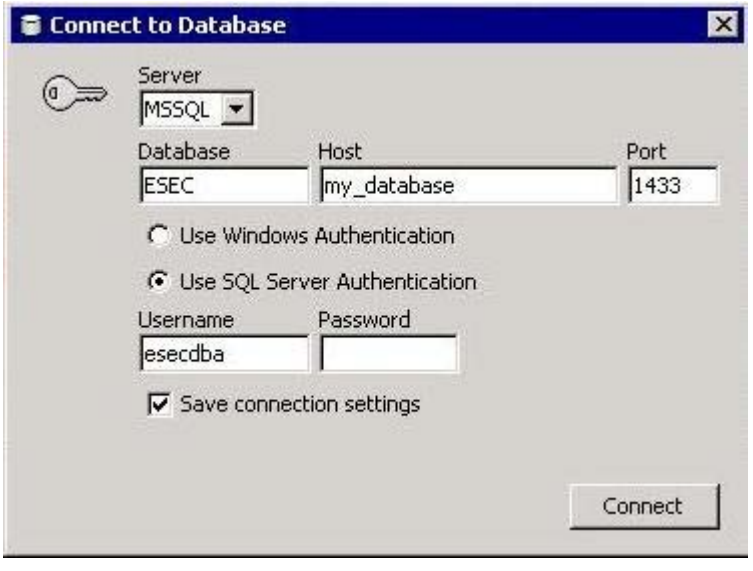
1. Démarrez l'interface du Gestionnaire de données Sentinel.
2. Sélectionnez le type de la base de données : Oracle ou MSSQL
3. Spécifiez le nom d'instance de la base de données (par exemple, ESEC).
4. Spécifiez l'hôte de la base de données (utilisez le nom de l'hôte ou son adresse IP).
5. Pour le port, utilisez le port par défaut 1521 pour Oracle ou le port par défaut 1433 pour MSSQL.
6. Pour le nom d'utilisateur et le mot de passe, utilisez votre nom d'utilisateur et votre mot de passe d'administrateur de la base de données Sentinel (par exemple, esecdba).

**REMARQUE** : sous Windows et MS SQL, si vous avez installé MS SQL en mode mixte, vous pouvez vous connecter à l'aide de l'Authentification Windows OU de l'Authentification SQL Server. Si vous avez installé MS SQL en mode Authentification Windows, vous devez vous connecter à l'aide de l'Authentification Windows. Si vous choisissez d'utiliser l'Authentification Windows, la base de données MS SQL reconnaîtra votre type de connexion à Windows et vous identifiera sur cette base (par exemple, authentification unique).

Dans le cas d'un serveur Oracle :




Sous Windows :



**REMARQUE :** si vous choisissez d'enregistrer vos paramètres de connexion, ceux-ci sont enregistrés dans le fichier sdm.connect local. La prochaine fois que vous démarrez l'interface, le fichier sdm.connect fournira les paramètres de connexion. Vous pouvez utiliser ce fichier lorsque vous exécutez le Gestionnaire de données Sentinel à partir de la ligne de commande.

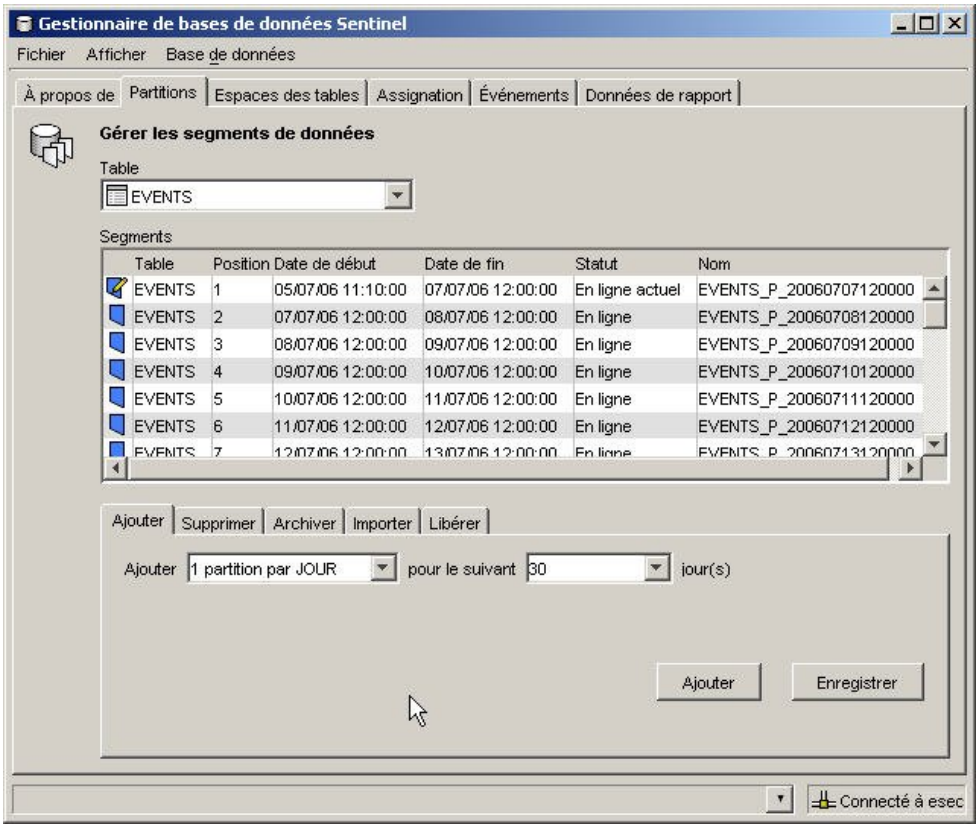
7. Cliquez sur Connecter.

## Partitions

L'onglet Partitions du Gestionnaire de données Sentinel permet aux utilisateurs d'afficher et de gérer les partitions de la base de données.

Pour afficher les partitions sur l'interface

1. Cliquez sur l'onglet Partitions.
2. Sélectionnez la table que vous voulez voir dans la liste déroulante.




La table Segments affiche les partitions de la table de base de données sélectionnée.

Chaque ligne de la table Segments indique les heures de début et de fin, le statut et le nom de la partition, ainsi que la table de base de données dans laquelle cette partition est créée.

Les partitions répertoriées dans la table Segments peuvent présenter l'un des états suivants :

| | |
|---|---|
| En ligne | Les données de la partition en ligne sont disponibles |
| En ligne actuel | Partition en ligne dans laquelle des lignes sont en cours d'insertion |
| En ligne archivé | Partition dont les données sont archivées mais toujours disponibles |

| | |
|---|---|
| | pour l'une des raisons suivantes :<br>▪ la partition existe toujours ;<br>▪ la partition est réimportée |
| Hors ligne | Les données dans une partition hors ligne ne sont pas disponibles car la partition est supprimée et n'est pas importée |
| Hors ligne archivé | Partition archivée et supprimée |

### Pour gérer les partitions

1. Cliquez sur l'onglet *Partitions*.
2. Sélectionnez la table dans la liste déroulante.
3. Sélectionnez l'onglet au bas de la fenêtre qui correspond à l'opération que vous voulez effectuer : Ajouter, Supprimer, Archiver, Importer ou Libérer.

### Pour ajouter des partitions

1. Sélectionnez l'onglet *Ajouter*.
2. Spécifiez le nombre de partitions à ajouter et le nombre de jours pour lesquels vous voulez ajouter des partitions.
3. Appuyez sur *Ajouter*.

### Pour supprimer des partitions

1. Sélectionnez l'onglet *Supprimer*.
2. Spécifiez le nombre de jours pour lesquels vous voulez supprimer des anciennes partitions.
3. Appuyez sur *Supprimer*.

### Pour archiver des partitions

**REMARQUE** : les tables Regroupement ne sont pas archivées.

1. Sélectionnez l'onglet *Archiver*.
2. Spécifiez le nombre de jours pour lesquels vous voulez archiver les anciennes partitions et le répertoire dans lequel stocker l'archive.

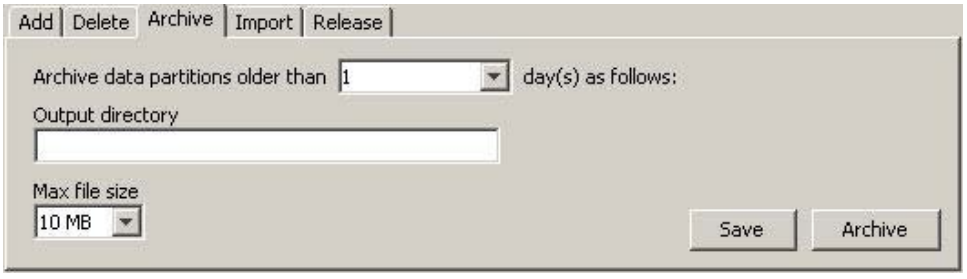
**REMARQUE** : sous UNIX, il n'est pas possible d'archiver les partitions dans /racine.

3. Cliquez sur *Archiver*.

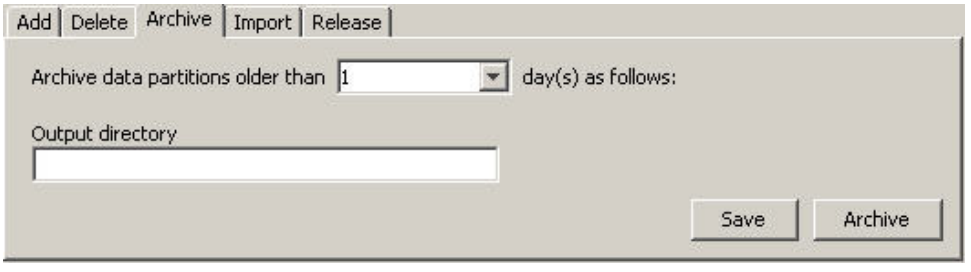
**REMARQUE** : lorsque vous archivez des partitions, veillez à entrer un chemin d'accès valide sur le serveur de la base de données avec les autorisations correctes.

**REMARQUE** : l'onglet Archiver diffère pour MSSQL et Oracle. Dans le cas d'Oracle, vous pouvez spécifier la taille maximale du fichier d'archive.

Onglet Archiver pour Oracle :




Onglet Archiver pour MSSQL :




### Pour importer des partitions

1. Sélectionnez l'onglet *Importer*.
2. Sélectionnez la partition de la table Segments dans laquelle vous voulez importer les données.
3. Spécifiez le répertoire d'entrée dans lequel les données archivées seront lues.
4. Cliquez sur *Importer*.

### Pour libérer des partitions importées

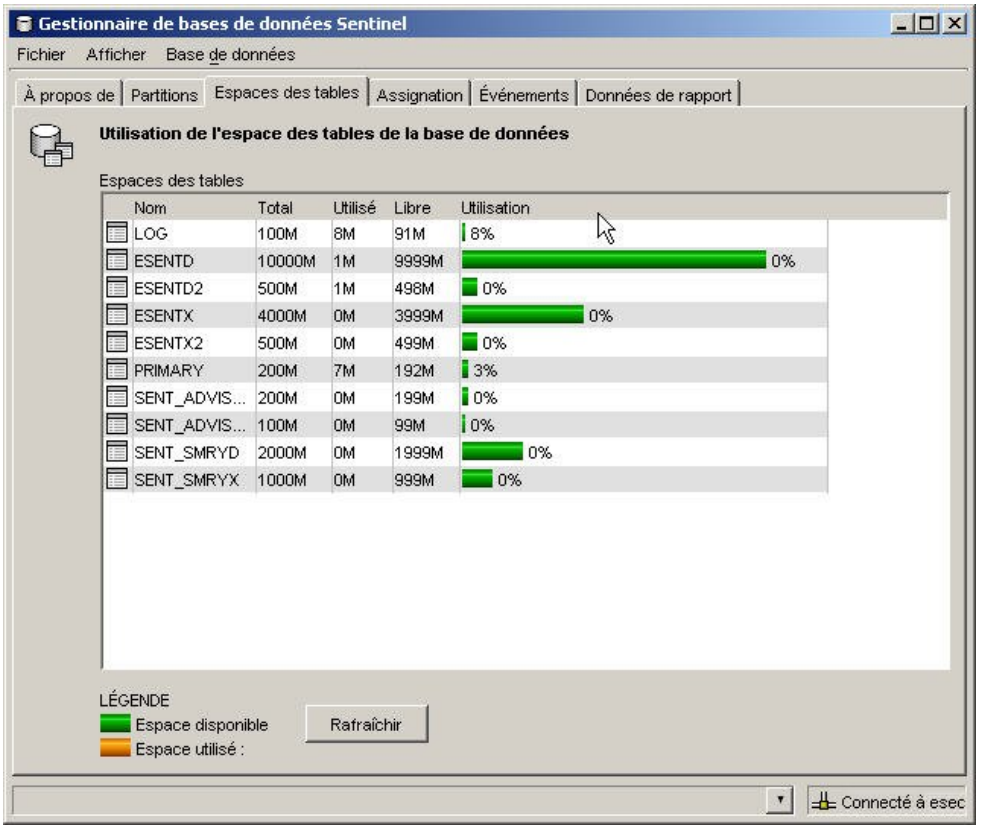
1. Sélectionnez l'onglet *Libérer*.
2. Sélectionnez la partition de la table Segments à libérer.
3. Cliquez sur *Libérer*.

## Espaces des tables

L'onglet Espaces des tables du Gestionnaire de données Sentinel permet aux utilisateurs d'afficher l'utilisation de l'espace des tables de la base de données actuelle.

Pour afficher les espaces des tables sur l'interface

1. Cliquez sur l'onglet *Espaces des tables.*




La table Utilisation de l'espace des tables de la base de données indique l'espace alloué à chaque espace de table ainsi que la quantité de mémoire utilisée et la quantité de mémoire encore disponible pour chaque espace de table. Les barres de couleur permettent de visualiser l'espace total alloué pour chaque espace de table et le pourcentage utilisé.

**REMARQUE** : sous MS SQL, les espaces de tables n'existent pas, des groupes de fichiers sont utilisés.

## Onglet Assignation

**REMARQUE** : pour utiliser l'onglet Assignation, votre fichier configuration.xml doit pointer vers un serveur de communication auquel DAS_Binary et DAS_Query sont connectés. Ceci est normalement le cas, par défaut, si les processus Serveur de communication et DAS s'exécutent.

L'onglet Assignation permet d'effectuer les opérations suivantes :

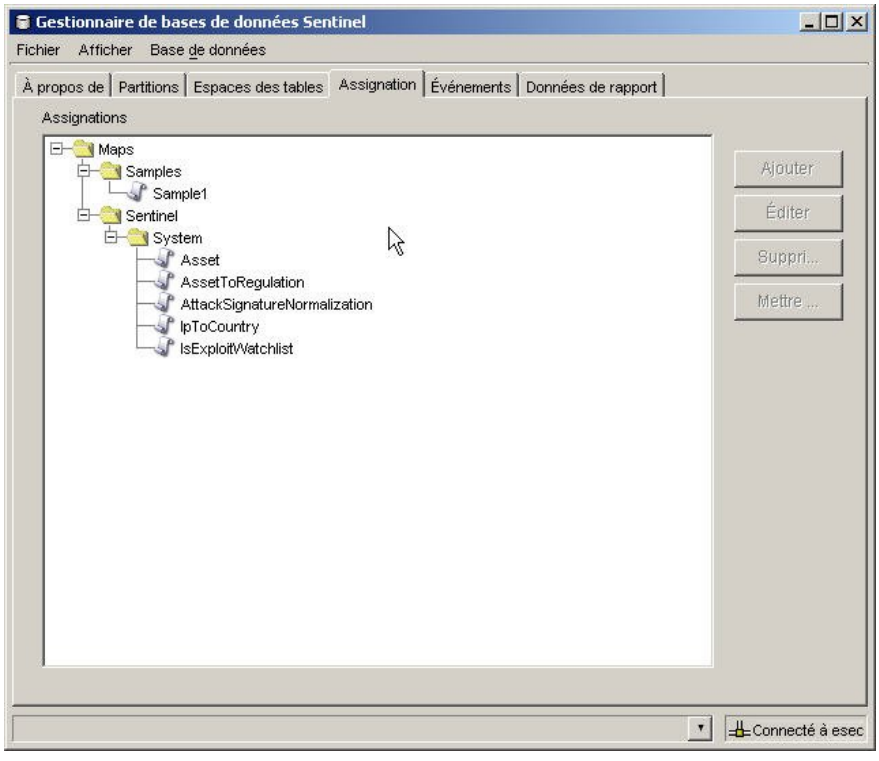
- ajouter de nouvelles définitions d'assignation ;

- modifier des définitions d'assignation ;
- supprimer des définitions d'assignation ;
- mettre à jour les données d'assignation.

L'onglet Assignation fonctionne conjointement avec l'option de source de données *Référencé par l'assignation* sous l'onglet Événements. Vous pouvez effectuer l'assignation à l'aide d'une chaîne ou d'une plage de nombres.

Pour afficher les assignations sur l'interface

1. Cliquez sur l'onglet *Assignation*.




L'onglet Assignation affiche une liste de toutes les assignations définies pour le système.

**REMARQUE** : les assignations figurant dans le dossier System ne peuvent être ni modifiées, ni supprimées.

## Ajout de définitions d'assignation

Pour ajouter une définition d'assignation :

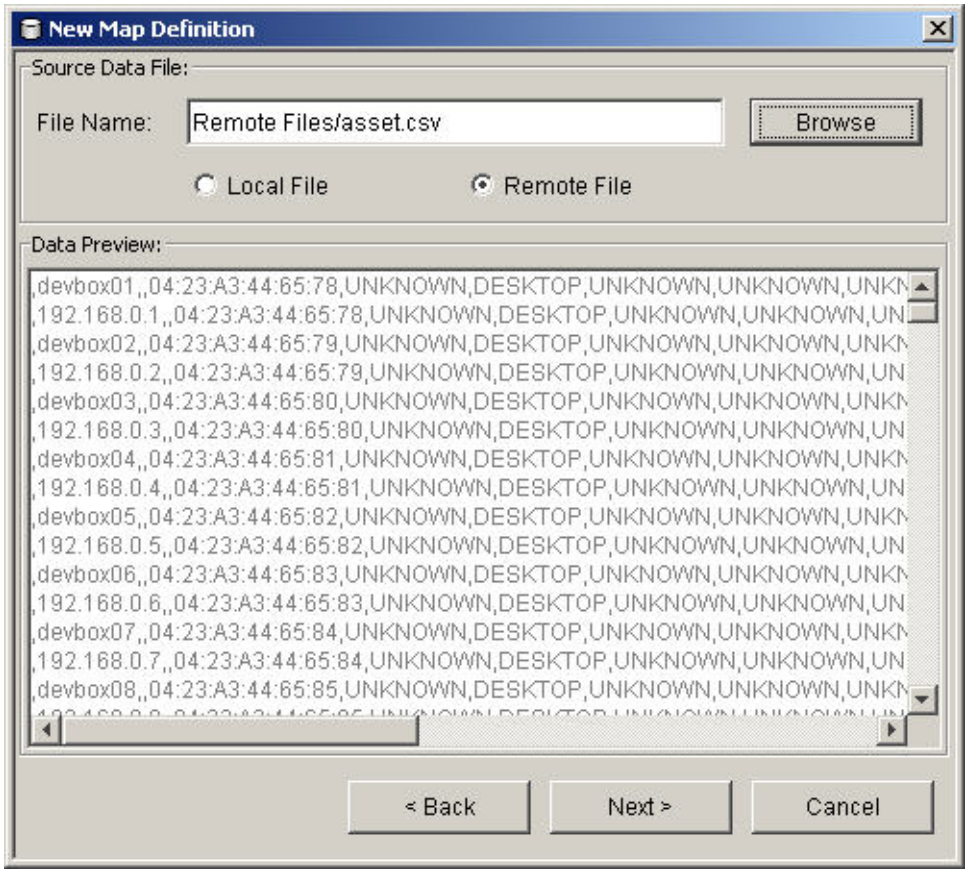
1. Cliquez sur l'onglet *Assignation*.
2. Cliquez sur *Ajouter*.
3. Si vous créez un nouveau dossier d'assignation, cliquez sur Nouveau. Entrez le nom du dossier.

**REMARQUE** : s'il s'agit d'une première définition d'assignation, il est conseillé de créer un nouveau dossier de définition d'assignation. Vous ne pourrez pas modifier ou supprimer la définition d'assignation si vous la créez dans le dossier System.

4. Assurez-vous que le dossier dans lequel vous voulez enregistrer la définition d'assignation est sélectionné (en d'autres termes, que le dossier indique qu'il est ouvert).
5. Entrez le nom de l'assignation.
6. Cliquez sur *Suivant*.

**REMARQUE** : la case du champ Type d'assignation est cochée.

7. Sélectionnez Fichier local ou Fichier distant.
   - Fichier local : permet de rechercher le fichier sur votre système de fichiers local (sur la machine sur laquelle le Gestionnaire de données Sentinel a été lancé).
   - Fichier distant : permet de choisir un fichier contenant les données source de l'assignation sur le serveur où DAS s'exécute. Deux fichiers pouvant déjà exister sur le serveur (si Advisor est installé et que les données de vulnérabilité ont été téléchargées) sont en général attackNormalization.csv et exploitDetection.csv. Le fichier distant pointe vers %ESEC_HOME%\sentinel\bin\map_data (Windows) ou $ESEC_HOME/sentinel/bin/map_data (UNIX).



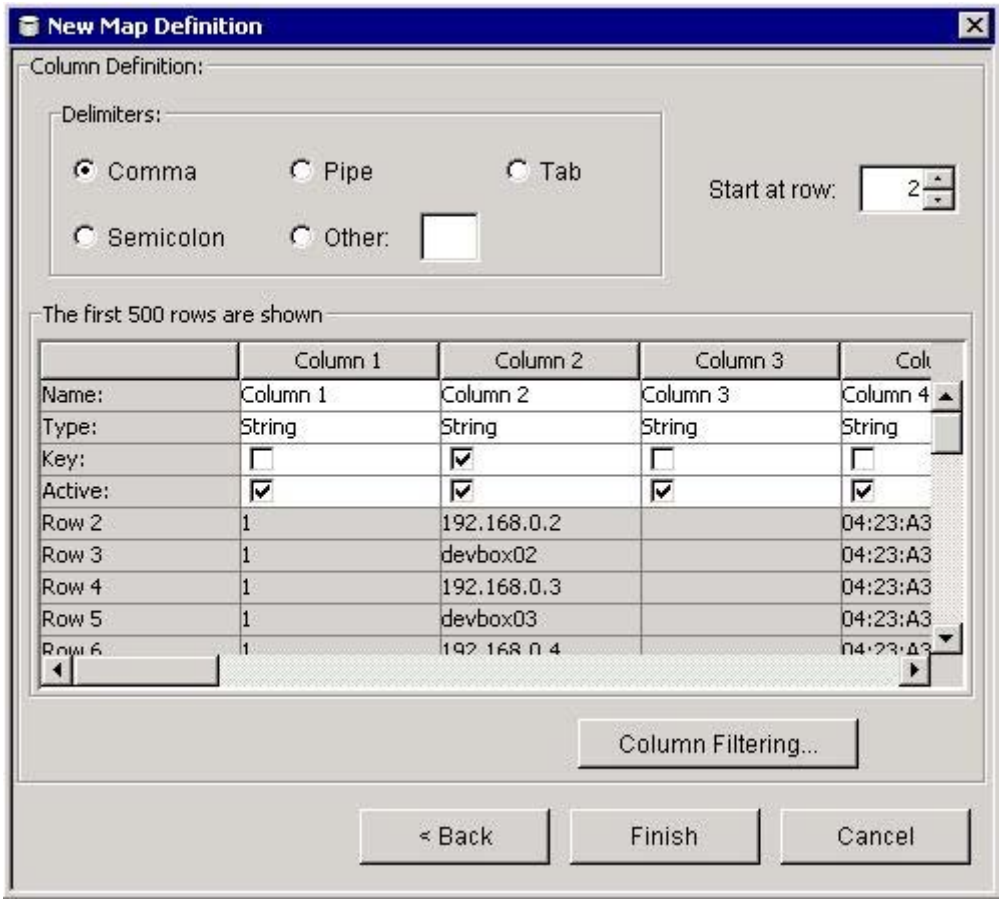

Sélectionnez le fichier de définition d'assignation. Cliquez sur *Suivant*.

**REMARQUE** : vous ne verrez pas toutes les lignes des fichiers d'assignation contenant plus de 500 lignes dans le Gestionnaire de données Sentinel.

8. Dans la fenêtre Définition de la nouvelle assignation, définissez les paramètres suivants :
   - Le séparateur (barre verticale, virgule, point-virgule, etc.) des données dans les lignes du fichier source des données de l'assignation.
   - Commencer à la ligne : le nombre de lignes à ignorer à partir du début du fichier source des données de l'assignation.
   - Le nom des colonnes.
   - Types de colonne : les types de colonne actuellement pris en charge sont les suivants :

  - *Chaîne :* une chaîne est un groupe de caractères utilisés en tant qu'objet unique par un ordinateur. Une chaîne peut être constituée d'une seule lettre comme d'un seul mot ou nombre. Le mot FINANCE ou l'adresse IP 192.168.2.40 peuvent être des chaînes. Une chaîne peut également être constituée d'une combinaison de mots, d'espaces et de nombres. L'adresse postale 1515 AVENUE DE MARIGNAN peut être une chaîne.
  - *Plage de nombres* : une plage de nombres (NumberRange - PlageNombres) est une fourchette de nombres. Par exemple, la plage allant de 10 à 200 serait représentée ainsi : 10-200. Pour utiliser la fonctionnalité d'assignation de plage, une définition d'assignation ne doit comporter qu'une colonne clé de type NumberRange (PlageNombres). S'il existe plusieurs colonnes clés ou si le type de la colonne clé est différent, le service d'assignation ne reconnaîtra pas l'assignation comme étant une assignation de plage.
- Les colonnes actives : lorsqu'une colonne est marquée comme active, ses données sont distribuées aux processus à l'aide des assignations. Toutes les colonnes clés doivent être actives. Seules les colonnes non-clés actives peuvent être sélectionnées en tant que *Colonne de l'assignation* dans l'onglet Événements.
- Les colonnes clés : une clé est l'identificateur unique de chaque ligne de données dans les données de l'assignation. Si plusieurs colonnes sont sélectionnées comme clés, la clé globale de l'assignation comprendra toutes les colonnes sélectionnées en tant que clés.
- Le filtrage des colonnes : une ligne peut être explicitement incluse ou exclue en fonction des critères de correspondance pour une colonne particulière. Le filtrage peut être utilisé pour exclure des lignes des données source de l'assignation, si ces lignes sont inutiles ou interfèrent avec l'assignation.

Au fur et à mesure que vous configurez les paramètres et les filtres, la table de données est automatiquement mise à jour pour vous permettre d'examiner vos données et de vérifier qu'elles sont analysées comme prévu.




9. Une fois que vous avez fini de configurer tous les paramètres et les filtres de la définition, cliquez sur Terminer.
10. Si vous avez choisi Fichier local à l'étape 7 ci-dessus, vous serez invité à télécharger le fichier dans le dossier virtuel des fichiers distants situé dans : %ESEC_HOME%\sentinel\bin\map_data. Entrez le nom du fichier, puis cliquez sur OK.

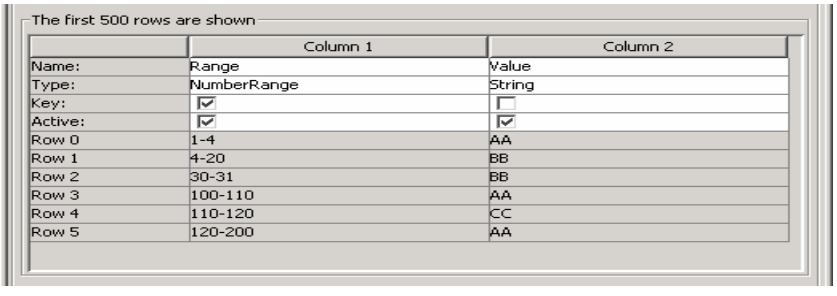
## Ajout d'une définition d'assignation de plage de nombres

Pour utiliser la fonctionnalité d'assignation de plage, une définition d'assignation ne doit comporter qu'une colonne clé de type NumberRange. S'il existe plusieurs colonnes clés ou si le type de la colonne clé est différent, le service d'assignation ne reconnaîtra pas l'assignation comme étant une assignation de plage.

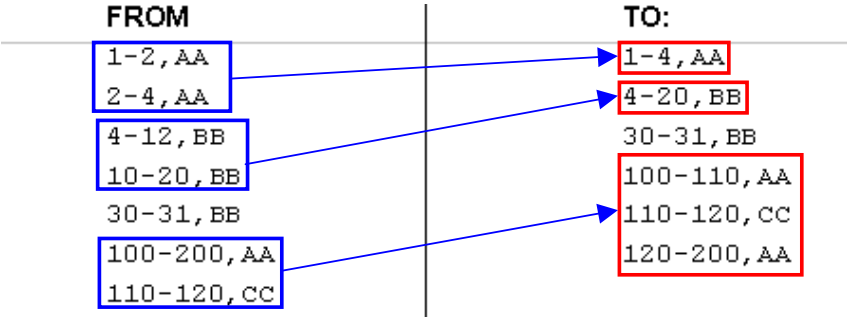
Pour créer une assignation de plage, sélectionnez la colonne devant être la clé de l'assignation, puis sélectionnez *NumberRange (PlageNombres)* comme type de la colonne. Le format des données dans une colonne de type *NumberRange (PlageNombres)* doit être « m-n », m étant le nombre minimal de la plage et n le nombre maximal (par exemple, 10-200 pour une plage de 10 à 200).

Le nombre maximal de la plage n'est pas inclus dans la plage (par exemple, [m,n)). Cela signifie qu'une plage de 10 à 200 ne pourra avoir pour clé que des nombres allant de 10 à 199. Dans l'exemple de données suivant, la première colonne est la clé :

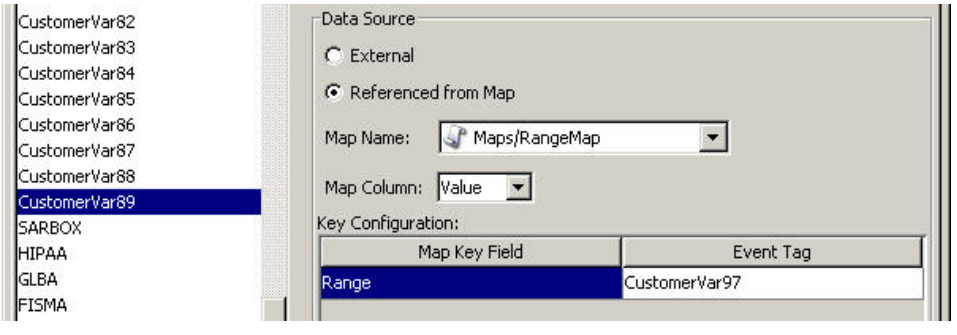
```
1-2,AA
2-4,AA
4-12,BB
10-20,BB
30-31,BB
100-200,AA
110-120,CC
```




Notez les changements de la table ci-dessous.




La configuration d'un événement sur l'assignation ci-dessus peut, par exemple, être la suivante :




CustomerVar97 devrait contenir une valeur numérique (ou est d'un type de valeur qui peut être convertie en valeur numérique, telle qu'une adresse IP ou une date).

Lorsque vous effectuez des recherches dans l'exemple d'assignation de plage, la valeur dans CustomerVar97 prend en compte l'assignation de plage indiquée et recherche la plage à laquelle la valeur appartient (si elle existe). Voici quelques exemples et leurs résultats :

```
CustomerVar97 = 1 ; CustomerVar89 aura pour valeur AA.
CustomerVar97 = 4 ; CustomerVar89 aura pour valeur BB.
CustomerVar97 = 300 ; CustomerVar89 ne sera pas
   défini.
```

Sentinel convertit en interne les adresses IP et les dates en nombres entiers pour les balises de type IPv4 et de type Date.

Les balises IPv4 sont :

- DestinationIP (dip)
- SourceIP (sip)

Les balises de date sont :

- CustomerVar11 à CustomerVar20 (cv11 à cv20)
- DateTime (dt)
- ReservedVar11 à ReservedVar20 (rv11 à rv20)

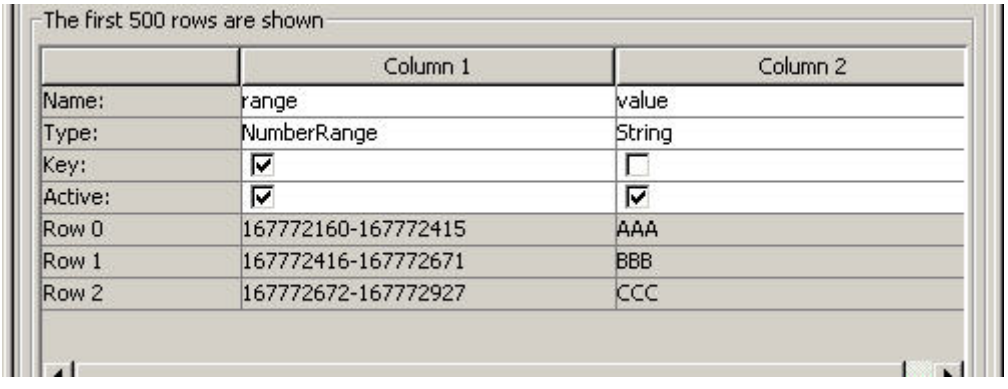
Pour plus d'informations sur les balises META, reportez-vous au Chapitre 5 : Balises META d'Assistant et de Sentinel du Guide des références de l'utilisateur Sentinel.

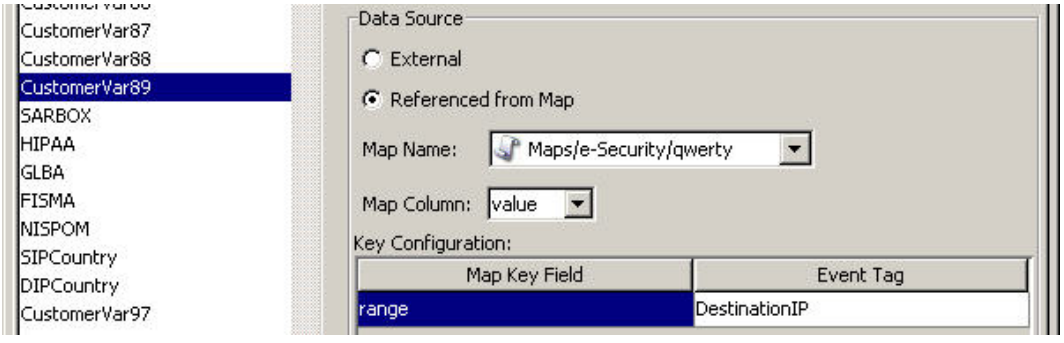
Par exemple, pour la table ci-dessous, la colonne 1 indique une plage numérique équivalente à une plage IP allant de 10.0.0.0 à 10.0.2.255.

```
167772160-167772415,AAA
167772416-167772671,BBB
167772672-167772927,CCC
```

La même configuration que l'exemple précédent est utilisée, si :

- la balise d'événement est définie sur DestinationIP et la colonne clé est la colonne 1 (plage) ;
- la colonne de l'assignation est la colonne 2 (valeur). Les valeurs générées pour CustomerVar89.






Si un événement contient l'adresse IP de destination 10.0.1.14 (équivalente à la valeur numérique 167772430), le résultat pour la colonne CustomerVar89 dans l'événement sera BBB.

Sentinel prend en charge les plages de nombres suivantes :

- nombre négatif à nombre négatif (par exemple, -234 à -34) ;
- nombre négatif à nombre positif (par exemple, -234 à 34) ;
- nombre positif à nombre positif (par exemple, 234 à 236) ;
- un nombre négatif unique (par exemple, -234), dans ce cas, le nombre minimal et le nombre maximal seront tous deux -234 ;
- un nombre positif unique (par exemple, 234), dans ce cas, le nombre minimal et le nombre maximal seront tous deux 234 ;
- nombre négatif à nombre maximal (par exemple, -234 à ...), dans ce cas, le nombre minimal sera -234 et le nombre maximal sera (2^63 - 1) ;
- nombre positif à nombre maximal (par exemple, 234 à ...), dans ce cas, le nombre minimal sera 234 et le nombre maximal sera (2^63 - 1).

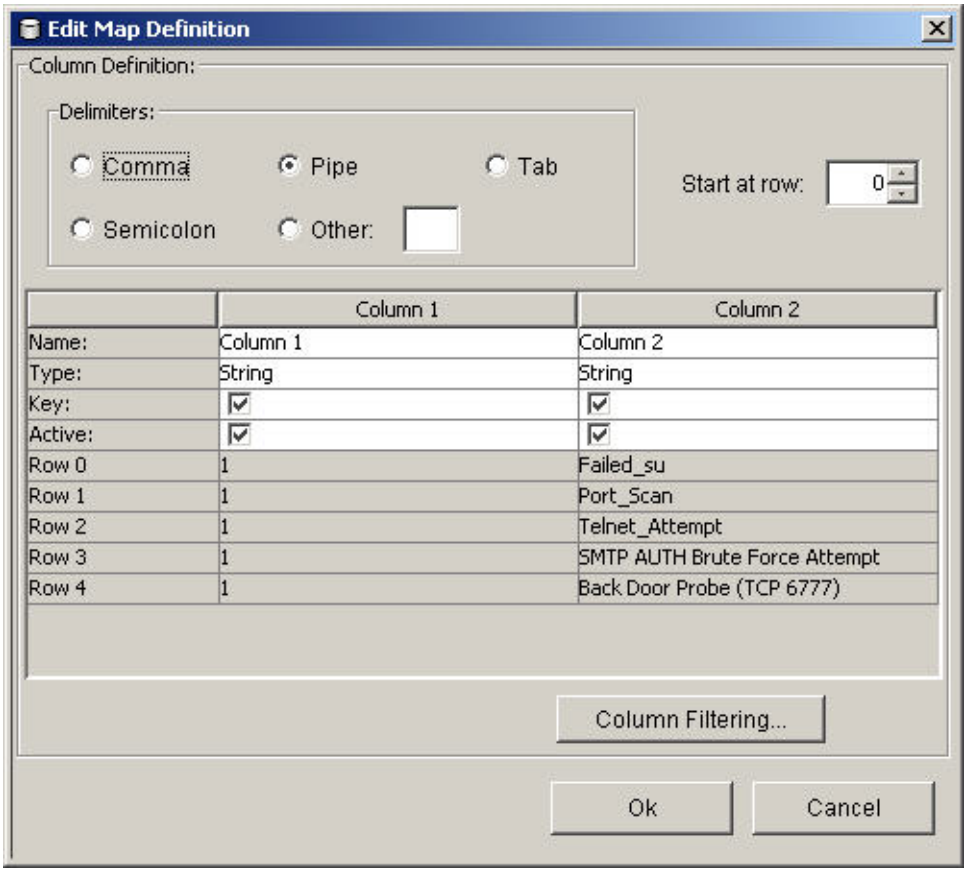
**REMARQUE** : dans tous les cas, le nombre minimal doit être inférieur ou égal au nombre maximal (par exemple, -234 à -235 n'est PAS valide).

## Modification de définitions d'assignation

Pour modifier une définition d'assignation :

1. Cliquez sur l'onglet Assignation.
2. Développez le dossier qui vous intéresse.
3. Sélectionnez une définition d'assignation et cliquez sur Éditer.

**REMARQUE** : la fonction de modification est désactivée pour les définitions d'assignation figurant dans le dossier System.




La fonction de modification permet d'effectuer les opérations suivantes :

- définir les séparateurs ;
- définir la ligne de début de l'assignation ;
- renommer les colonnes ;
- activer ou désactiver une colonne ;
- définir les colonnes clés ;
- filtrer les colonnes.

4. Une fois que vous avez effectué vos modifications, cliquez sur Ok.

## Suppression de définitions d'assignation

Pour supprimer une définition d'assignation

1. Cliquez sur l'onglet Assignation.
2. Développez le dossier qui vous intéresse.
3. Sélectionnez la définition d'assignation à supprimer.
4. Cliquez sur Supprimer.

**REMARQUE** : les assignations figurant dans le dossier Sentinel ne peuvent pas être modifiées.

## Mise à jour des données d'assignation

La mise à jour d'une assignation consiste à remplacer son fichier de données source sur le serveur exécutant DAS par un autre fichier. Le nouveau fichier de données source de l'assignation doit comporter le même séparateur, le même nombre de colonnes et la même structure que le fichier existant pour que l'assignation fonctionne correctement après la mise

à jour. En revanche, les valeurs figurant dans les colonnes du nouveau fichier de données source de l'assignation peuvent différer de celles du fichier existant. Si la structure du nouveau fichier de données source de l'assignation est différente de celle du fichier existant, utilisez la fonctionnalité Éditer de l'interface utilisateur du Gestionnaire de données Sentinel pour mettre à jour la définition de l'assignation.

### Pour mettre à jour les données d'une assignation

1. Si vous ne l'avez pas déjà fait, créez un fichier contenant les données source de la nouvelle assignation sur la machine exécutant le Gestionnaire de données Sentinel. Ce fichier peut être généré (par exemple, à partir d'un script de vidage des données) ou créé manuellement. Il peut également s'agir d'une version modifiée du fichier source des données de l'assignation existant. Si nécessaire, vous pouvez rechercher le fichier source des données de l'assignation existant à l'emplacement suivant :

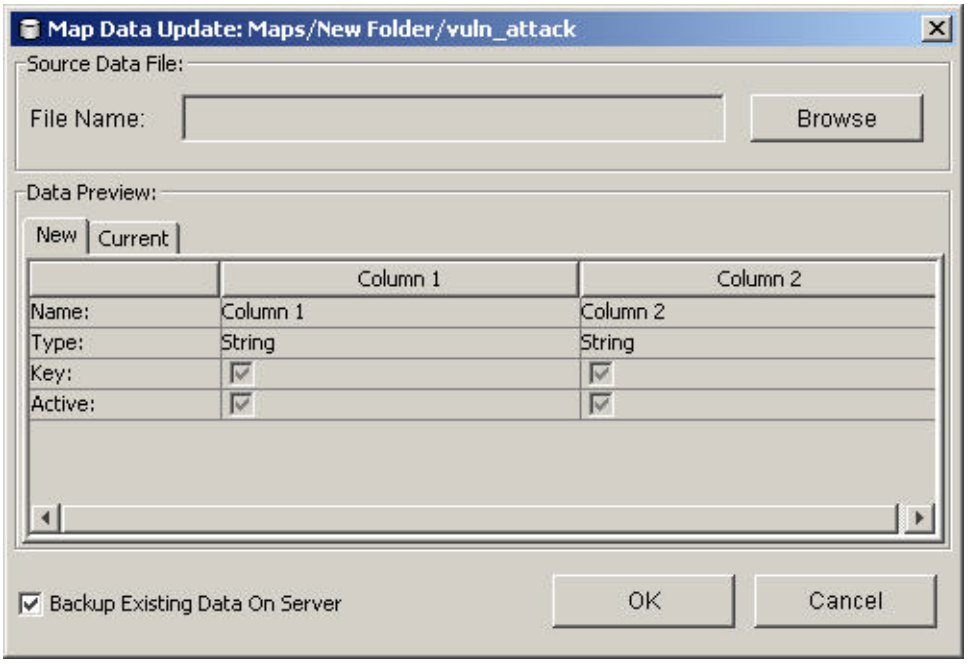
   Sous Windows :

   ```
   %ESEC_HOME%\sentinel\bin\map_data.
   ```

   Sous UNIX :

   ```
   $ESEC_HOME/sentinel/bin/map_data
   ```

2. Cliquez sur l'onglet Assignation.
3. Développez le dossier qui vous intéresse. Sélectionnez l'assignation à mettre à jour. Cliquez sur Mettre à jour.




4. Cliquez sur le bouton Parcourir pour rechercher le nouveau fichier source des données de l'assignation, puis sélectionnez-le. Lorsque le fichier est sélectionné, ses données apparaissent dans l'onglet Nouveau. Les données de l'assignation que vous remplacez se trouvent, quant à elles, dans l'onglet Actuel.
5. Désactivez ou conservez le paramètre par défaut Sauvegarder les données existantes sur le serveur. Si vous activez cette option, une sauvegarde du fichier source des données de l'assignation existant est effectuée et placée dans le dossier

%ESEC_HOME%\sentinel\bin\map_data (Windows) ou $ESEC_HOME/sentinel/bin/map_data (UNIX). Le préfixe du nom du fichier sauvegardé est le même que celui du fichier existant. La fin du nom du fichier contient des nombres aléatoires suivis du suffixe .bak. Par exemple : attaques_vuln10197.bak.

6. Cliquez sur OK.
7. Les données du nouveau fichier source de l'assignation sont téléchargées vers le serveur et remplacent le contenu du fichier source existant. Au terme du téléchargement, les données de l'assignation sont régénérées et distribuées aux clients de l'assignation (par exemple, le Gestionnaire des collecteurs).

## Onglet Événements

**REMARQUE** : pour utiliser l'onglet Événements, votre fichier configuration.xml doit pointer vers un serveur de communication auquel DAS_Binary et DAS_Query sont connectés. Ceci est normalement le cas, par défaut, si les processus Serveur de communication et DAS s'exécutent.

### Assignation de données aux événements

L'assignation de données aux événements est un mécanisme qui permet d'ajouter des données à un événement à l'aide des données qu'il contient pour faire référence aux données d'une source externe et les importer. La source de données externe est une assignation définie à l'aide de l'onglet Assignation. Utilisez l'onglet Événements pour spécifier les données figurant dans l'événement et devant faire référence aux données de l'assignation et les données à importer de l'assignation dans l'événement.

N'importe quelles données pouvant être assignées à un événement, l'assignation de données aux événements s'avère utile pour incorporer dans le flux d'événements des données figurant à tous les niveaux de votre entreprise. Certains des avantages liés à l'assignation de données aux événements sont les suivants :

- Contrôle de la conformité aux réglementations
- Conformité à la stratégie
- Attribution d'une priorité aux réponses
- Analyse des données de sécurité en fonction des activités de l'entreprise
- Renforcement des responsabilités

Lorsqu'une assignation de données aux événements est définie, elle est appliquée sur l'ensemble du système à tous les événements de tous les collecteurs. En outre, Sentinel distribue auto-matiquement les données d'assignation à tous les processus qui effectuent des assignations de données aux événements et maintiennent ces données à jour. Pour ces raisons, l'assignation de données aux événements contribue de manière significative aux déploiements de solutions dans les entreprises.

L'assignation de données aux événements comprend quatre composants :

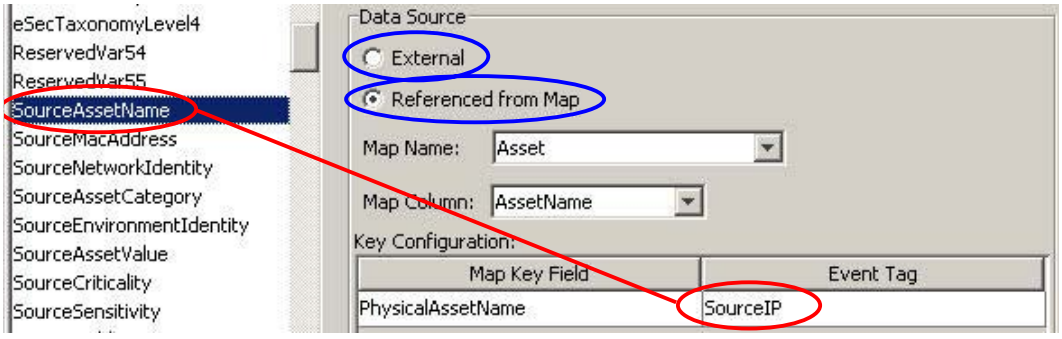
- Contrôleur : stocke toutes les informations d'assignation.
- Distributeur : redistribue automatiquement les assignations modifiées aux processus associés aux assignations.
- Moniteur : permet de détecter les changements dans les données source des assignations.
- Générateur : génère des assignations à partir de données source.

Une application de l'assignation de données aux événements peut être illustrée par la fonction Données de l'actif de Sentinel. Par exemple, les informations d'actif sont recueillies et stockées

dans le schéma des actifs de la base de données Sentinel et sont représentées par une entrée d'actif physique. Les actifs non physiques, tels que les services et les applications, sont représentés par une entrée liée à un actif physique. Le mécanisme de mise à jour automatisé principal des données d'actif a recours à un collecteur d'actifs qui lit les données dans un scanner tel que Nmap. Le collecteur d'actifs automatise l'extraction des informations d'actif en lisant celles-ci dans le scanner, puis en les fournissant aux tables de schéma d'actif. Pour l'assignation de données aux événements, les informations d'actif sont assignées depuis l'IP de destination et l'IP source.

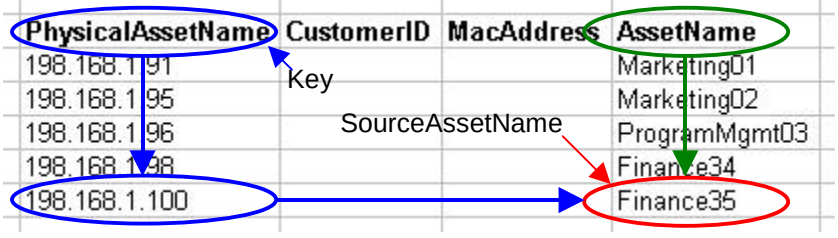
Il existe deux types de sources de données :

- Externe : un collecteur renseigne la balise d'événement avec cette valeur.
- Référencé par l'assignation : les données sont extraites d'une assignation pour renseigner la balise.



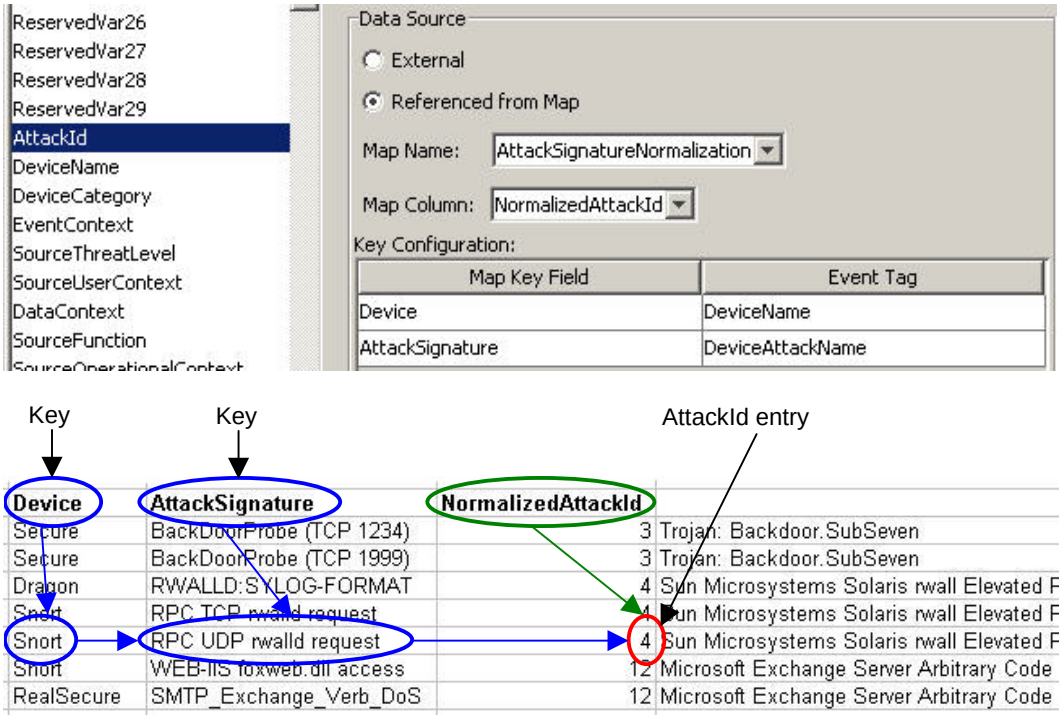

Dans l'illustration ci-dessus, la balise SourceAssetName est renseignée par l'assignation Asset (dont le fichier source de données est asset.csv). La valeur spécifique de SourceAssetName est extraite de la colonne AssetName de l'assignation Asset. La colonne PhysicalAsssetName est définie comme clé. Lorsque la balise SourceIP de l'événement correspond à l'une des valeurs de l'IP source dans la colonne PhysicalAsssetName de l'assignation, la ligne comportant la clé corres-pondante fournit une valeur à la colonne AssetName. Par exemple, dans l'exemple ci-dessous, IP 198.168.1.100 correspond à Finance35 de la colonne AssetName.

**REMARQUE** : lorsqu'une colonne est définie comme clé, elle n'apparaît pas dans le champ déroulant Colonne.




Il peut arriver que plusieurs colonnes soient définies comme clé pour éviter que l'assignation soit une assignation de plage (ce type d'assignation ne peut comporter qu'une colonne clé, si le type défini de la colonne est NumberRange). Par exemple (si le type défini de la colonne est String), les colonnes DeviceName (nom du périphérique de sécurité) et DeviceAttackName sont définies comme clés pour la balise AttackId qui est renseignée par la valeur correspondante de la colonne NormalizedAttackID de l'assignation AttackNormalization. Dans une ligne où la balise d'événement DeviceName correspond à la valeur de la colonne Device de l'assignation et où DeviceAttackName correspond à la valeur de la colonne AttackSignature de l'assignation, la valeur de AttackId est la valeur de la colonne NormalizedAttackID.

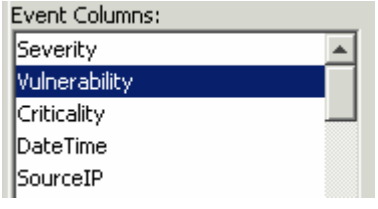
La configuration de l'assignation de données aux événements est la suivante :



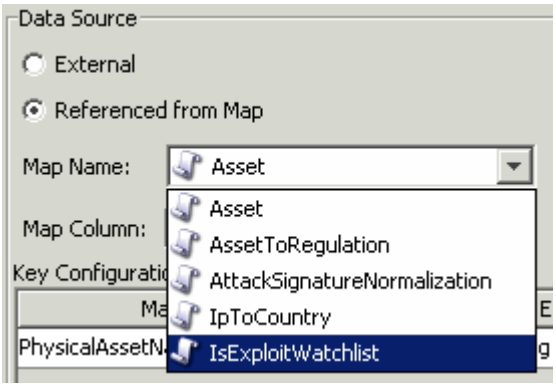

## Configuration des balises d'événements (colonnes) pour utiliser Assignation

1. Cliquez sur l'onglet Événements.
2. Sélectionnez une balise d'événement dans la liste Colonnes des événements.

   **REMARQUE** : le nom d'origine de la balise d'événement apparaît au-dessus du champ Étiquette. La description de la colonne d'événements est également fournie.



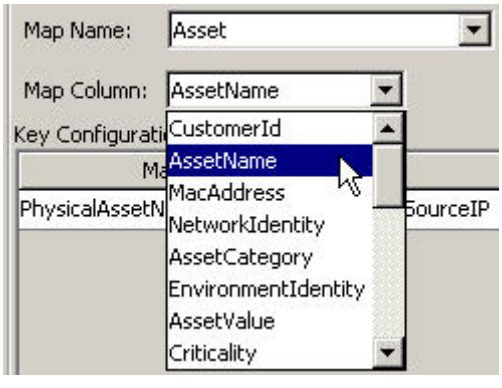

3. Cliquez sur Référencé par l'assignation pour configurer la balise d'événement à renseigner avec les données d'une assignation. Cliquez sur Externe pour conserver la valeur que le collecteur place dans la balise d'événement (s'il y en a une).
4. Cliquez sur la flèche du champ déroulant Nom de l'assignation.



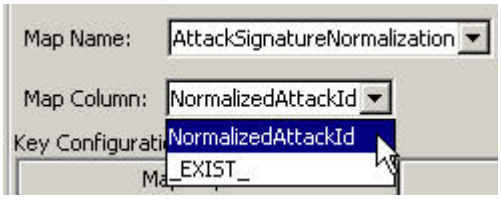

Sélectionnez l'une des assignations par défaut suivantes ou une assignation que vous avez créée :

- Asset : contient les données du fichier source de l'assignation asset.csv. Le fichier asset.csv est automatiquement généré à partir des données d'actif de la base de données Sentinel lorsqu'un collecteur d'actifs est exécuté. Ce fichier peut être renseigné manuellement, si besoin.
- AssetToRegulation : contient les données du fichier source de l'assignation AssetToRegulation.csv. Ce fichier doit être renseigné manuellement.
- AttackSignatureNormalization : contient les données du fichier source de l'assignation attackNormalization.csv (signatures IDS). Le fichier attackNormalization.csv est automatiquement généré à partir des données Advisor de la base de données Sentinel lorsqu'Advisor est alimenté.
- IpToCountry : contient les données du fichier source de l'assignation IpToCountry.csv. Ce fichier doit être renseigné manuellement.
- IsExploitWatchlist : contient les données du fichier source de l'assignation exploitDetection.csv (vulnérabilités et menaces). Le fichier exploitDetection.csv est automatiquement généré à partir des données Advisor et des données de vulnérabilité de la base de données Sentinel lorsqu'Advisor est alimenté ou lorsqu'un collecteur de vulnérabilités est exécuté.

5. Cliquez sur la flèche du menu déroulant Colonne de l'assignation et sélectionnez un nom de colonne d'assignation. Selon l'assignation que vous avez choisie à l'étape précédente, ces valeurs varient.



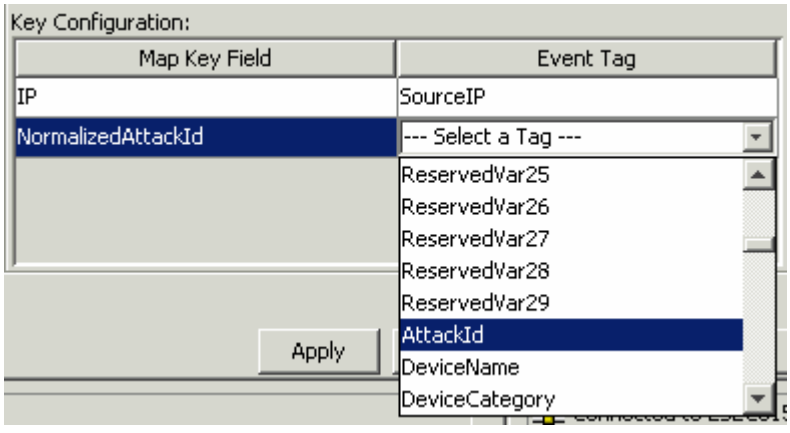




- _EXIST_ : colonne d'assignation spéciale qui existe dans chaque assignation. Si cette colonne d'assignation est sélectionnée, un « 1 » sera placé dans la balise d'événement à condition que la clé figure dans les données de l'assignation. Dans le cas contraire, un « 0 » sera placé dans la balise d'événement.
- Tous les autres choix : noms des colonnes actives dans la définition de l'assignation qui ne sont pas définies comme clés (par exemple, la colonne CustomerId dans Asset ou la colonne NormalizedAttackId dans AttackNormalization).

6. Pour chacune des lignes de la table Configuration clé, sélectionnez la balise d'événement dans la colonne Balise d'événement qui correspondra à la colonne clé de l'assignation spécifiée dans la colonne Champ de clé d'assignation. Les lignes de la table Configuration clé dépendent de l'assignation sélectionnée.

**REMARQUE** : une clé est un identificateur unique pour chaque ligne de données dans les données de l'assignation.




7. Cliquez sur Appliquer.

**REMARQUE :** cliquez sur *Appliquer* pour enregistrer les modifications que vous avez apportées à la colonne d'événements sélectionnée dans une mémoire tampon temporaire. Si vous ne cliquez pas sur *Appliquer* lorsque vous sélectionnez une autre colonne d'événements, les modifications que vous avez apportées à la colonne d'événements précédente seront perdues. Les modifications ne sont enregistrées sur le serveur que lorsque vous cliquez sur *Enregistrer*.

8. Si vous voulez modifier l'assignation de données aux événements d'une autre colonne d'événements, répétez la procédure ci-dessus. Pensez à cliquer sur Appliquer après avoir modifié l'assignation de données aux événements de chaque colonne d'événements.
9. Cliquez sur Enregistrer.

**REMARQUE** : cliquez sur *Enregistrer* pour enregistrer vos modifications sur le serveur. Cette fonction enregistre toutes les modifications stockées dans la mémoire tampon temporaire (lorsque vous avez cliqué sur *Appliquer*).

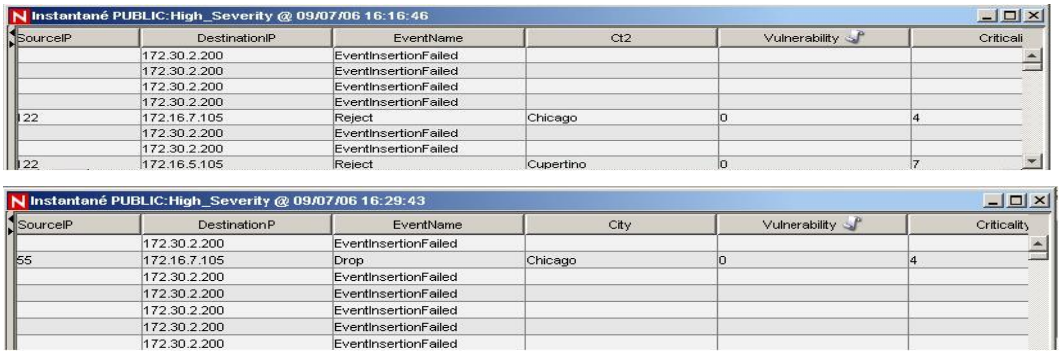
## Renommer des balises

L'onglet Événements permet également d'assigner des noms aux étiquettes de balises d'événements existantes. Par exemple, vous pouvez renommer City la balise d'événement Ct2. Ainsi, la balise d'événement qui apparaissait auparavant sous le nom « Ct2 » dans le Centre de contrôle Sentinel apparaît désormais sous le nom « City ». Les balises d'événements

apparaissent à plusieurs emplacements dans le Centre de contrôle Sentinel, notamment dans les filtres, les règles de corrélation et les vues actives.

Renommer des balises ne change pas le nom de la variable dans les scripts des collecteurs. Therefore, even if the event tag labeled Ct2 is renamed to City, the variable that must be used in a Collector script to reference this meta-tag will still be s_CT2.

Voici une illustration de l'utilisation avant et après de cette fonctionnalité dans une vue active.




## Renommer une colonne d'événements

1. Cliquez sur l'onglet Événements.

   **REMARQUE** : le nom d'origine de la colonne d'événements apparaît au-dessus du champ Étiquette. La description de la colonne d'événements est également fournie.

2. Sélectionnez une colonne d'événements.
3. Entrez une valeur pour votre colonne d'événements dans le champ Étiquette.


4. Cliquez sur Appliquer.

   **REMARQUE** : le fait de cliquer sur *Appliquer* enregistre les modifications que vous avez apportées à la balise d'événement sélectionnée dans une mémoire tampon temporaire. Si vous ne cliquez pas sur *Appliquer*, lorsque vous sélectionnez une autre balise d'événement, les modifications apportées à la balise d'événement précédente seront perdues. Les modifications ne sont enregistrées sur le serveur que lorsque vous cliquez sur *Enregistrer*.

5. Cliquez sur Enregistrer.

**REMARQUE** : cliquez sur *Enregistrer* pour enregistrer vos modifications sur le serveur. Cette fonction enregistre toutes les modifications stockées dans la mémoire tampon temporaire (lorsque vous avez cliqué sur *Appliquer*).

6. Pour que les modifications soient visibles dans le Centre de contrôle Sentinel, fermez et rouvrez celui-ci.

## Onglet Données de rapport

**REMARQUE** : pour utiliser l'onglet Données de rapport, votre fichier configuration.xml doit pointer vers un serveur de communication auquel DAS_Binary et DAS_Query sont connectés. Ceci est normalement le cas, par défaut, si les processus Serveur de communication et DAS s'exécutent.

L'onglet *Données de rapport* est l'*interface de gestion des récapitulatifs* de Sentinel. Cet onglet permet d'activer et de désactiver les **récapitulatifs**. Activer un récapitulatif permet à la fonction de regroupement de calculer le nombre d'événements pour ce récapitulatif.

Un récapitulatif est un ensemble défini d'attributs qui constituent la clé pour laquelle le nombre d'occurrences (nombre d'événements) doit être calculé pour chaque tranche horaire (heure d'événement). Le récapitulatif *EventSevDestPortSummary*, lorsqu'il est *actif*, enregistre le décompte des événements pour chaque combinaison port de destination-gravité pour une tranche horaire. Ces calculs de données d'événement enregistrés permettent de créer des rapports de récapitulatif et de lancer des requêtes sur la base de ces récapitulatifs plus rapidement. Les rapports sont utilisés par Crystal Reports. Reportez-vous aux chapitres consacrés à l'installation de Crystal Reports dans le Guide d'installation de Sentinel pour plus d'informations. Certains récapitulatifs doivent être *actifs* pour que les rapports établis à partir de ceux-ci soient précis.

Le regroupement désigne le processus de calcul de tous les récapitulatifs actifs au fur et à mesure que les événements se produisent dans le système. Ces calculs sont enregistrés dans les tables de récapitulatifs appropriées de la base de données.

Avantages des récapitulatifs :

- Volume de données considérablement réduit
- Dimensions conformes qui permettent d'effectuer sur les données d'événement des analyses à tous les niveaux
- Les rapports sur les récapitulatifs s'exécutent beaucoup plus rapidement avec des récapitulatifs précalculés.

Avantages du regroupement :

- Ne traite que les récapitulatifs actifs.
- N'affecte pas l'insertion des événements dans la base de données en temps réel.

L'onglet Données de rapport permet d'effectuer les opérations suivantes :

- activer et désactiver les récapitulatifs prédéfinis ;
- afficher les attributs de chaque récapitulatif ;

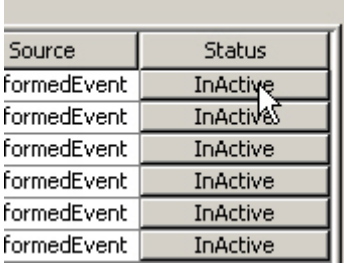
- afficher la validité d'un récapitulatif pour une tranche horaire ;
- demander quels *fichiers d'événements* doivent être exécutés pour que le récapitulatif soit généré.

Le tableau suivant répertorie tous les récapitulatifs déjà définis dans le système. Il indique le nom de chaque récapitulatif, le nom de la table de la base de données à laquelle il appartient et ses attributs en fournissant une brève description de chaque récapitulatif.

| **Nom du récapitulatif** | **Table/Description** |
|---|---|
| EventSrcSummary | EVT_SRC_SMRY_1<br>Ce récapitulatif établit le compte des événements par : ip source, actif source, port source, utilisateur source, taxinomie, nom, ressource, collecteur, protocole, gravité et heure. |
| EventSevDestTxnmySummary | EVT_DEST_TXNMY_SMRY_1<br>Ce récapitulatif établit le compte des événements par ip de destination, actif de destination, taxinomie, gravité et heure. |
| EventSevDestPortSummary | EVT_PORT_SMRY_1<br>Ce récapitulatif établit le compte des événements par port de destination, gravité et heure. |
| EventSevSummary | EVT_SEV_SMRY_1<br>Ce récapitulatif établit le compte des événements par gravité et heure. |

## Désactiver et activer un récapitulatif

1. Cliquez sur l'onglet *Données de rapport*.
2. Pour désactiver un récapitulatif, cliquez sur *Actif* dans la colonne Statut pour qu'il indique *Inactif*.
3. Pour activer un récapitulatif, cliquez sur *inactif* dans la colonne Statut pour qu'il indique *Actif*.




Pour activer le regroupement pour les 10 premiers rapports pour Crystal Reports :

- Activez les trois récapitulatifs suivants :
  - EventDestSummary
  - EventSevSummary
  - EventSrcSummary
- Activez EventFileRedirectService dans le fichier das_binary.xml situé dans :

Sous UNIX :

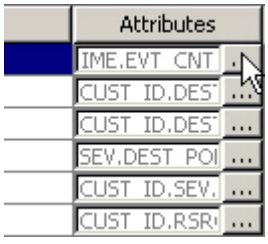
```
$ESEC_HOME/sentinel/config/das_binary.xml
```

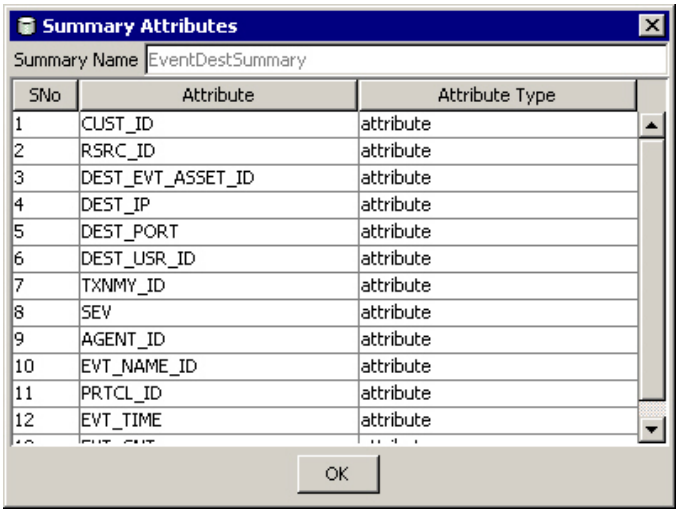
Sous Windows :

```
%ESEC_HOME%\sentinel\config\das_binary.xml
```

## Afficher les informations sur un récapitulatif

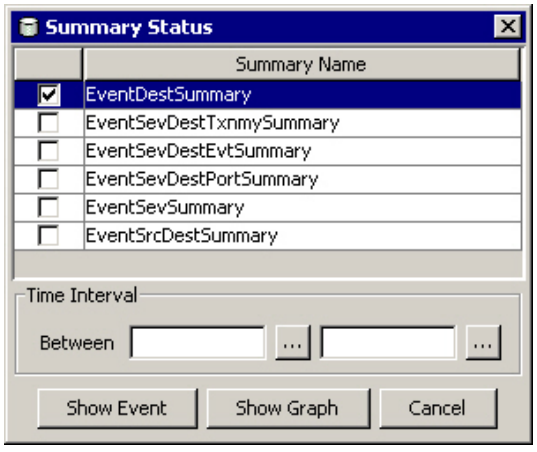
1. Cliquez sur l'onglet *Données de rapport*.
2. Cliquez sur « … » dans la colonne Attributs pour afficher les attributs qui composent un récapitulatif.



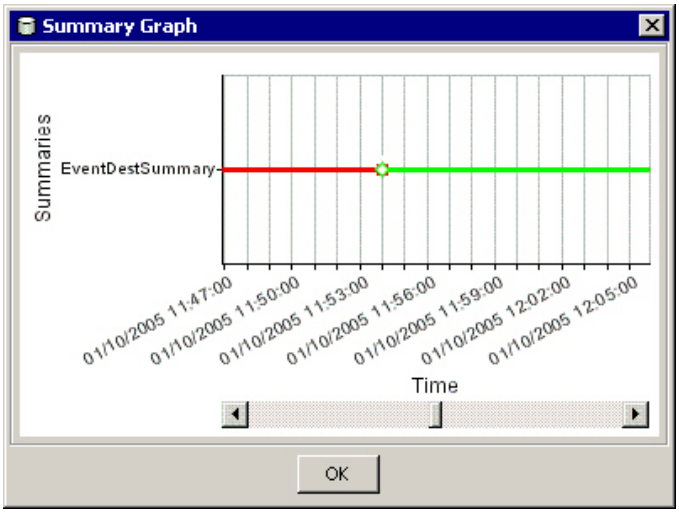

## Vérifier la validité d'un récapitulatif

1. Cliquez sur l'onglet *Données de rapport*.
2. Sélectionnez *Statut*.
3. Choisissez le ou les récapitulatifs que vous souhaitez interroger.




4. Sélectionnez un intervalle horaire.
5. Cliquez sur *Afficher le graphique*.

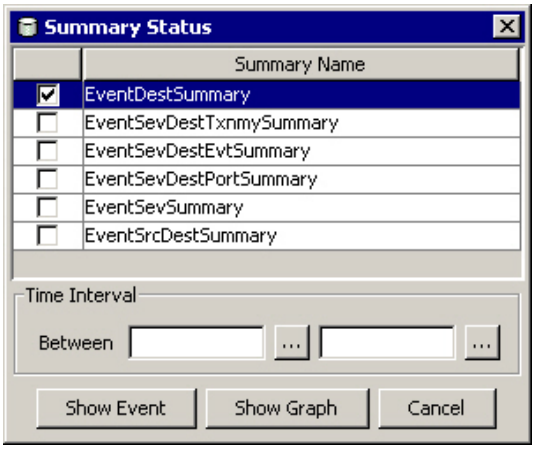
6. Les barres vertes indiquent que le récapitulatif est généré pour cette tranche horaire. Les parties en rouge indiquent que des données manquent pour le récapitulatif durant cette période.




**REMARQUE** : pour générer des récapitulatifs, reportez-vous à la section *Exécuter des fichiers d'événements pour un récapitulatif*.

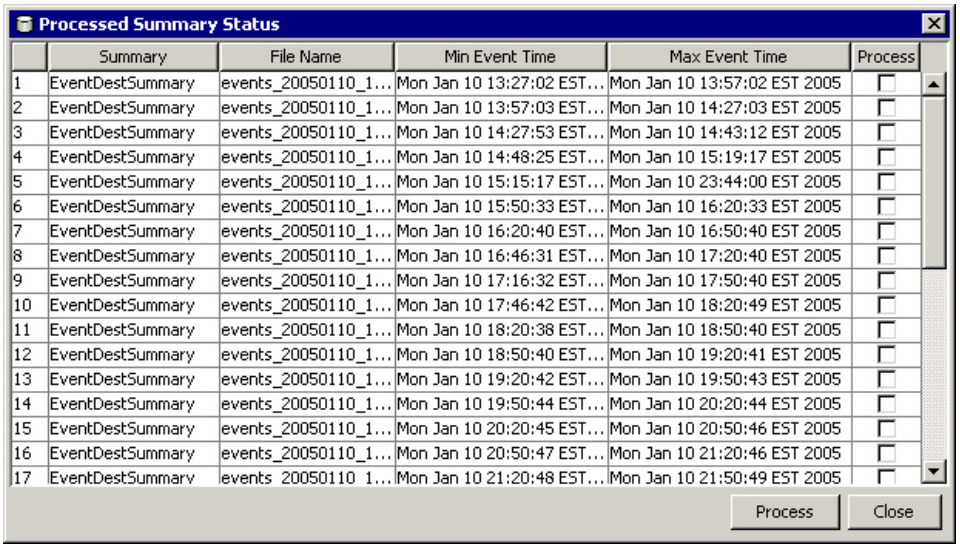
## Interroger les fichiers d'événements pour un récapitulatif

1. Cliquez sur l'onglet *Données de rapport*.
2. Sélectionnez *Statut*.
3. Choisissez le ou les récapitulatifs que vous souhaitez interroger.



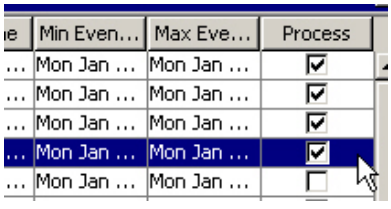

4. Sélectionnez un intervalle horaire.
5. Cliquez sur *Afficher l'événement*.
6. Les fichiers d'événements nécessaires pour générer le récapitulatif sont présentés sous forme de liste.

**REMARQUE** : pour générer des récapitulatifs, reportez-vous à la section *Exécuter des fichiers d'événements pour un récapitulatif*.




Exécution des fichiers d'événements pour un récapitulatif

1. Cliquez sur l'onglet *Données de rapport*.
2. Sélectionnez *Statut*.
3. Choisissez le ou les récapitulatifs que vous souhaitez interroger.
4. Sélectionnez un intervalle horaire.
5. Cliquez sur *Afficher l'événement*.
6. Les fichiers *d'événements* nécessaires pour générer le récapitulatif sont présentés sous forme de liste.
7. Vérifiez les fichiers *d'événements* que vous voulez exécuter pour que le récapitulatif soit généré.




8. Cliquez sur *Processus*.

# Ligne de commande du Gestionnaire de données Sentinel

**REMARQUE** : si votre ordinateur n'a pas accès à DAS_Binary et à DAS_Query, vous pouvez utiliser la ligne de commande du Gestionnaire de données Sentinel plutôt que son interface.

## Enregistrement des propriétés de connexion pour le Gestionnaire de données Sentinel

Ceci doit être effectué avant d'utiliser une opération de ligne de commande du Gestionnaire de données Sentinel autre que saveConnection.

Si vous avez exécuté l'interface du Gestionnaire de données Sentinel, vous pouvez utiliser le fichier sdm.connect créé à partir de celle-ci. Ce fichier est situé dans %ESEC_HOME%\sdm sous Windows et $ESEC_HOME/sdm sous UNIX.

La fonction d'enregistrement des connexions enregistre les détails de connexion suivants, ainsi que le mot de passe chiffré (en utilisant le keystore spécifié dans configuration.xml) dans le fichier spécifié.

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | saveConnection |
| -server | <oracle ou mssql> |
| -host | <adresse IP de l'hôte de la base de données ou nom de l'hôte auquel se connecter> |
| -port | <numéro du port de la base de données auquel se connecter [port par défaut Oracle : 1521/SQL Server port par défaut : 1433]> |
| -database | <nom/SID de la base de données à laquelle se connecter> |
| -user | <nom de l'utilisateur de la base de données> |
| -password | <mot de passe de la base de données> |
| -winAuth | Utilisé pour l'authentification Windows. Lorsque vous utilisez cette option, n'utilisez pas -user et -password. |
| -connectFile | <nom du fichier dans lequel enregistrer les détails de la connexion [nom de votre choix]> |

L'application enregistre tous les détails de connexion ci-dessus et le mot de passe chiffré dans le fichier spécifié. L'application utilise les détails de connexion enregistrés pour exécuter le reste des commandes. Cette procédure doit être effectuée la première fois que vous démarrez l'application et lorsque vous voulez changer les détails de connexion que l'application utilise.

### Exécution de saveConnection

1. Exécutez la commande comme suit :

```
sdm -action saveConnection -server <oracle/mssql> -
   host <Ip de l'hôte/Nom de l'hôte> -port <numéro du
   port> -database <Nom/SID de la base de données> [-
   driverProps <Fichier de propriétés>] {-user
   <Utilisateur de la base de données> -password <mot
   de passe de la base de données> | -winAuth} -
   connectFile <Nom du fichier d'enregistrement de la
   connexion>
```

   L'exemple suivant enregistre les connexions vers un hôte dont l'adresse IP est 172.16.0.36 au port 1521 (port par défaut pour Oracle ; pour SQL Server, le port par défaut est 1433).

   - Exemple pour Oracle :

```
./sdm -action saveConnection -server oracle -host
   172.16.0.36 -port 1521 -database esec -user esecdba
   -password XXXXXX -connectFile sdm.connect
```

   - Exemple pour SQL Server :

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

L'exemple suivant enregistre les connexions vers un hôte dont l'adresse IP est 172.16.0.36 au port 1433 avec une base de données nommée esec_51 pour l'authentification Windows.

- Exemple pour SQL Server (authentification Windows) :

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

Les détails de connexion sont enregistrés dans le fichier sdm.connect. Les autres commandes utilisent le nom de ce fichier pour se connecter à la base de données désignée et pour effectuer leurs opérations.

## Gestion des partitions

### Configuration des partitions

Pour Oracle seulement. Cette action (partitionConfig) permet de configurer les partitions de la base de données. Cette configuration détermine comment les partitions sont ajoutées aux tables Sentinel partitionnées. Cette action utilise les indicateurs suivants :

| | |
|---|---|
| -action | partitionConfig |
| -freq | <3D ou 2D ou 1D ou 1W><br><br>Les options suivantes sont les seules prises en charge.<br>▪ 3D - trois partitions par jour<br>▪ 2D - deux partitions par jour<br>▪ 1D - une partition par jour<br>▪ 1W - une partition par semaine |
| -days | <Nombre de jours à ajouter lorsque addPartitions est choisie> |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

Exécution de partitionConfig

1. Exécutez cette commande comme suit :

```
./sdm -action partitionConfig –freq <3D ou 2D ou 1D
   ou 1W> -days <Nombre de jours à ajouter lorsque
   « addPartitions » est choisie> -connectFile <chemin
   d'accès au fichier enregistré par
   « saveConnection » (par défaut :
   $ESEC_HOME/sdm/sdm.connect)>
```

Dans l'exemple suivant, le système ajoute trente partitions (3 partitions par jour = 3 * 10).

```
./sdm -action partitionConfig -freq 3D -days 10 -
   connectFile sdm.connect
```

Dans l'exemple suivant, le système ajoute dix partitions (1 partition par jour = 1 * 10).

```
./sdm -action partitionConfig -freq 1D -days 10 -
   connectFile sdm.connect
```

Dans l'exemple suivant, le système ajoute une partition (1 partition par 7 jours = 1 * 10/7).

```
./sdm -action partitionConfig -size 1W -days 10 -
   connectFile sdm.connect
```

### Ajout de partitions

Cette action (addPartitions) ajoute le nombre requis de partitions selon la configuration des partitions dans les tables suivantes :

- Oracle :
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server :
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Si la configuration choisie implique la création de partitions pour 10 jours, à chaque fois que vous exécutez *addPartitions*, cette action vérifie si des partitions existent pour les 10 jours à venir. Si vous disposez de suffisamment de partitions pour les 10 prochains jours, addPartitions n'ajoute aucune partition. Dans le cas contraire, elle ajoute le nombre requis de partitions pour 10 jours.

Cette action utilise les indicateurs suivants :

| | |
|---|---|
| -action | addPartitions |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

Exécution de addPartitions

1. Exécutez cette commande comme suit :

```
sdm -action addPartitions -connectFile <chemin d'accès
   au fichier enregistré
   par « saveConnection »>
```

Exemple pour Oracle :

```
./sdm -action addPartitions -connectFile sdm.connect
```

Exemple pour SQL Server :

```
sdm -action addPartitions -connectFile sdm.connect
```

### Suppression de partitions

Cette action (dropPartition) supprime des tables suivantes toutes les partitions plus anciennes que l'indicateur keepDays :

- Oracle :
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server :
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Cette action ne supprime pas les partitions qui ne sont pas archivées. Si vous voulez supprimer des partitions non archivées, utilisez l'indicateur *forceDelete*. Si forceDelete est utilisé :

| | |
|---|---|
| false ou non spécifié | Supprime uniquement les partitions plus anciennes que keepDays et celles qui sont archivées. |
| true | Supprime toutes les partitions plus anciennes que keepDays, y compris celles qui ne sont pas archivées. |

Cette action utilise les indicateurs suivants :

| | |
|---|---|
| -action | dropPartitions |
| -keepDays | <nombre de jours de conservation> |
| [-forceDelete] | <true ou false> |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

**REMARQUE :** si vous supprimez une partition qui n'est pas archivée, il n'est pas possible de l'importer.

Exécution de dropPartition

1. Exécutez cette commande comme suit :

```
sdm -action dropPartitions [-forceDelete <false>] -
   keepDays <nombre> -connectFile <chemin d'accès
   au fichier enregistré par « saveConnection »>
```

Dans les exemples suivants, toutes les partitions datant de plus de 30 jours sont supprimées et archivées. Toutes les partitions qui ont été ignorées (non supprimées), n'étant pas

archivées,
sont répertoriées une fois l'opération achevée.

Exemple pour Oracle :

```
./sdm -action dropPartitions -keepDays 30 -connectFile
   sdm.connect


./sdm -action dropPartitions -forceDelete false -
   keepDays 30 -connectFile sdm.connect
```

Exemple pour SQL Server :

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


sdm -action dropPartitions -forceDelete false -
   keepDays 30 -connectFile sdm.connect
```

## Affichage des récapitulatifs de partitions

Cette action (ViewPartitions) affiche le récapitulatif des partitions des tables prises en charge suivantes :

- Oracle :
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server :
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | startGui |
| -tableName | <nom de l'une des tables mentionnées ci-dessus> |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

Pour afficher les récapitulatifs des partitions

1. Exécutez cette commande comme suit :

```
sdm -action viewPartitions -tableName <nom de la
   table> –connectFile <chemin d'accès au fichier
   enregistré par « saveConnection »>
```

Dans l'exemple suivant, la liste des partitions de la table EVENTS est affichée et le statut de chaque partition est indiqué.

- Exemple pour Oracle :

```
./sdm -action viewPartitions -tableName EVENTS -
   connectFile sdm.connect
```

- Exemple pour SQL Server :

```
sdm -action viewPartitions –tableName EVENTS –
   connectFile sdm.connect
```

## Gestion des archives

### Configuration des archives

Cette action (archiveConfig) sert à configurer l'archivage. Cette configuration détermine comment les données sont archivées à partir des tables Sentinel.

Cette action utilise les indicateurs suivants :

| | |
|---|---|
| -action | archiveConfig |
| -dirPath | <chemin d'accès valide au répertoire dans lequel enregistrer les fichiers archivés> |
| -keepDays | <nombre de jours de conservation> |
| -fileSize | (Oracle seulement) <taille maximale de chaque fichier archivé. Spécifiez Ko, Mo ou Go.> |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

Pour Oracle, le chemin d'accès au répertoire dirPath doit être spécifié en tant que paramètre UTL_FILE_DIR dans le fichier init.ora selon les directives Oracle. Vous disposez normalement de l'un des paramètres suivants :

- UTL_FILE_DIR = *
- UTL_FILE_DIR = répertoire spécifique dans lequel vous voulez enregistrer des fichiers et qui doit être spécifié dans le fichier init.ora.

Exécution de archiveConfig

1. Exécutez cette commande comme suit :

```
sdm -action archiveConfig  -dirPath <chemin d'accès
   au répertoire dans lequel enregistrer les fichiers
   archivés> -keepDays <nombre de jours de
   conservation> -fileSize <taille maximale de chaque
   fichier archivé, spécifié en Ko, Mo ou Go> -
   connectFile <chemin d'accès au fichier enregistré
   par « saveConnection »>
```

- Exemple pour Oracle :

Dans l'exemple suivant, toutes les données datant de plus de 13 jours sont archivées dans le répertoire /tmp en morceaux d'un volume supérieur à 1 Go.

```
./sdm -action archiveConfig  -dirPath /tmp -keepDays
   13 -fileSize 1GB -connectFile sdm.connect
```

Dans l'exemple suivant, toutes les données datant de plus de 13 jours sont archivées dans le répertoire /tmp en morceaux d'un volume supérieur à 40 Mo.

```
./sdm -action archiveConfig -dirPath /tmp -keepDays 13
   -fileSize 40MB -connectFile sdm.connect
```

## Archivage de données

Exécutez cette action (archiveData) après avoir défini la configuration d'archivage (archiveConfig). Cette action archive les données d'une table donnée selon la configuration d'archivage définie. Cette action archive les données :

- Oracle :
  - EVENTS
  - CORRELATED_EVENTS
- SQL Server :
  - EVENTS
  - CORRELATED_EVENTS

**REMARQUE** : les tables Regroupement ne sont pas archivées.

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | archiveData |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

Exécution d'archiveData

1. Exécutez cette commande comme suit :

```
sdm -action archiveData -connectFile <chemin d'accès
   au fichier enregistré
   par « saveConnection »>
```

   - Exemple pour Oracle :

   Dans l'exemple suivant, les événements ainsi que leurs valeurs réservées et personnalisées et les événements corrélés des tables EVENTS, EVT_RESERVED_VALUES, EVT_CUSTOM_VALUES et ASSOCIATIONS sont archivés selon la valeur définie dans la configuration d'archivage (archiveConfig). À partir de la valeur définie dans l'exemple fourni sous la section sur Gestion des archives, les données datant de plus de 13 jours sont archivées.

```
./sdm -action archiveData -connectFile sdm.connect
```

   - Exemple pour SQL Server :

   Dans l'exemple suivant, les événements corrélés ou non sont archivés selon la valeur définie dans la configuration d'archivage archiveConfig). À partir de la valeur définie dans l'exemple fourni sous la section sur Gestion des archives, les données datant de plus de 13 jours sont archivées.

   sdm -action archiveData -connectFile sdm.connect

### Suppression de données

Cette action (deleteData) supprime les données d'une table donnée dont le nombre de jours de conservation est dépassé. Cette action supprime les données des tables suivantes :

- Oracle :
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server :
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
  -

Cette action ne supprime pas les partitions qui ne sont pas archivées. Si vous voulez supprimer des partitions non archivées, la valeur true doit être spécifiée pour l'indicateur facultatif *forceDelete*. Si forceDelete est utilisé :

| | |
|---|---|
| false ou non spécifié | Supprime uniquement les partitions plus anciennes que keepDays et celles qui sont archivées. |
| true | Supprime toutes les partitions plus anciennes que keepDays, y compris celles qui ne sont pas archivées. |

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | deleteData |
| -keepDays | <nombre de jours de conservation> |
| [-forceDelete] | <true ou false> |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

Exécution de deleteData

1. Exécutez cette commande comme suit :

```
sdm -action deleteData -keepDays <nombre de jours
   de conservation> -connectFile <chemin d'accès
   au fichier enregistré par « saveConnection »>
```

   - Exemple pour Oracle :

   Dans l'exemple suivant, les partitions de toutes les tables datant de plus de 13 jours sont supprimées et archivées. À la fin de l'opération, une liste des partitions qui n'ont pas été supprimées est générée, si ces partitions n'ont pas été archivées.

```
./sdm -action deleteData -keepDays 13 -connectFile
   sdm.connect
```

- Exemple pour SQL Server :

Dans l'exemple suivant, les partitions de toutes les tables datant de plus de 13 jours sont supprimées et archivées. À la fin de l'opération, une liste des partitions qui n'ont pas été supprimées est générée, si ces partitions n'ont pas été archivées.

```
sdm -action deleteData -keepDays 13 -connectFile
   sdm.connect
```

## Gestion des importations

### Répertorier les fichiers à importer

Cette action (filesToImport) permet de répertorier les fichiers nécessaires pour importer des données entre les dates indiquées dans les tables suivantes :

- Oracle :
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server :
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | filesToImport |
| -startDate | <mm/jj/aaaa hh24:min:ss> |
| -endDate | <mm/jj/aaaa hh24:min:ss> |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

**REMARQUE :** hh24 représente les heures représentées au format 24 heures. Par exemple, 1:15:00 p.m. représente 13:15:00 et 3:00:00 a.m. 03:00:00.

Exécution de filesToImport

1. Exécutez cette commande comme suit :

```
sdm -action filesToImport -startDate <mm/jj/aaaa
   hh24:min:ss> -endDate <mm/jj/aaaa hh24:min:ss> -
   connectFile <chemin d'accès au fichier enregistré
   par « saveConnection »>
```

Dans l'exemple suivant, tous les fichiers contenant des données entre les dates « 09/25/2003 00:00:00 » (25 septembre à minuit) et « 09/26/2003 00:00:00 » (26 septembre à minuit) qui ont été archivés plus tôt et peuvent être réimportés sont répertoriés.

- Exemple pour Oracle :

```
./sdm -action filesToImport -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

- Exemple pour SQL Server :

```
sdm -action filesToImport -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

Dans l'exemple suivant, tous les fichiers contenant des données entre les dates « 09/25/2003 16:00:00 » (25 septembre, 16 heures) et « 09/26/2003 18:00:00 » (26 septembre, 18 heures) qui ont été archivés plus tôt et peuvent être réimportés sont répertoriés.

- Exemple pour Oracle :

```
./sdm -action filesToImport -startDate 09/25/2003
   16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
   sdm.connect
```

- Exemple pour SQL Server :

```
sdm -action filesToImport -startDate 09/25/2003
   16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
   sdm.connect
```

### Importation de données

Cette action (importData) importe les données entre les dates indiquées dans les tables prises en charge suivantes :

- Oracle :
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server :
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Si les données ont déjà été importées ou si aucune donnée archivée n'est trouvée entre les dates spécifiées, un message est généré.

L'application importe chaque fichier dans une table et crée une vue historique sur toutes es tables historiques. La vue du rapport est ajoutée à la table d'origine et à la vue historique. Tous les rapports utilisent la vue de rapport et ont par conséquent accès aux données importées.

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | importData |
| -startDate | <mm/jj/aaaa hh24:min:ss> |
| -endDate | <mm/jj/aaaa hh24:min:ss> |
| -dirPath | <répertoire à partir duquel importer les fichiers> |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

**REMARQUE :** hh24 représente les heures représentées au format 24 heures. Par exemple, 1:15:00 p.m. représente 13:15:00 et 3:00:00 a.m. 03:00:00.

Exécution d'importData

1. Placez tous les fichiers que vous souhaitez importer dans un répertoire spécifique (à savoir, dirPath - <répertoire à partir duquel importer les fichiers>).
2. Exécutez cette commande comme suit :

```
sdm -action importData -dirPath <répertoire à partir
   duquel importer les fichiers> -startDate
   <mm/jj/aaaa hh24:min:ss> -endDate <mm/jj/aaaa
   hh24:min:ss> -connectFile <chemin d'accès au
   fichier enregistré par « saveConnection »>
```

Dans l'exemple suivant, les fichiers archivés dans le répertoire tmp contenant des données entre les dates « 09/25/2003 00:00:00 » (25 septembre à minuit) et « 09/26/2003 00:00:00 » (26 septembre à minuit) sont importés dans les tables mentionnées ci-dessus.

- Exemple pour Oracle :

```
./sdm -action importData -dirPath /tmp -startDate
   09/25/2003 00:00:00 -endDate 09/26/2003
   00:00:00 -connectFile sdm.connect
```

- Exemple pour SQL Server :

```
sdm -action importData -dirPath c:\tmp -startDate
   09/25/2003 00:00:00 -endDate 09/26/2003
   00:00:00 -connectFile sdm.connect
```

Dans l'exemple suivant, les fichiers archivés dans le répertoire tmp contenant des données entre les dates « 09/25/2003 08:30:00 » (25 septembre, 8 heures 30) et « 09/26/2003 20:00:00 » (26 septembre, 20 heures) sont importés dans les tables mentionnées ci-dessus.

- Exemple pour Oracle :

```
./sdm -action importData -dirPath /tmp -startDate
   09/25/2003 08:00:00 -endDate 09/26/2003
   20:00:00 -connectFile sdm.connect
```

- Exemple pour SQL Server :

```
sdm -action importData -dirPath c:\tmp -startDate
   09/25/2003 08:00:00 -endDate 09/26/2003
   20:00:00 -connectFile sdm.connect
```

### Suppression de données importées

Cette action (dropImported) supprime des tables prises en charge suivantes les données importées entre les dates indiquées :

- Oracle :
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server :
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

S'il n'existe aucune donnée importée entre deux dates spécifiées, un message est généré.

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | dropImported |
| -startDate | <mm/jj/aaaa hh24:min:ss> |
| -endDate | <mm/jj/aa hh24:min:ss> |
| -connectFile | <chemin d'accès au fichier enregistré par **saveConnection**> |

**REMARQUE :** hh24 représente les heures représentées au format 24 heures. Par exemple, 1:15:00 p.m. représente 13:15:00 et 3:00:00 a.m. 03:00:00.

Exécution de dropImported

1. Exécutez cette commande comme suit :

```
sdm -action dropImported -startDate <mm/jj/aaaa
   hh24:min:ss> -endDate <mm/jj/aaaa hh24:min:ss> -
   connectFile <chemin d'accès au fichier enregistré
   par « saveConnection »>
```

   Dans l'exemple suivant, les données importées entre les dates indiquées à partir des tables mentionnées ci-dessus sont supprimées.

   - Exemple pour Oracle :

```
./sdm -action dropImported -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

   - Exemple pour SQL Server :

```
sdm -action dropImported -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

## Tablespace Management

Dans Tablespace Management, vous pouvez utiliser soit la ligne de commande, soit l'interface. La ligne de commande permet d'afficher :

- l'utilisation de l'espace des tables de la base de données Sentinel.

L'interface permet d'afficher :

- les partitions ;
- les partitions archivées ;
- les partitions d'importation ;
- l'utilisation de l'espace.

### Affichage de l'utilisation de l'espace de la base de données Sentinel (ligne de commande)

Cette action (dbstats) affiche l'utilisation de la base de données Sentinel pour tous les espaces des tables Sentinel dans Oracle et les groupes de fichiers Sentinel dans MS SQL.

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | dbstats |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

Affichage de l'utilisation de l'espace de la base de données Sentinel (ligne de commande)

1. Exécutez la commande suivante :

```
sdm -action dbStats -connectFile <chemin d'accès
   au fichier enregistré par « saveConnection »>
```

- Exemple pour Oracle :

Dans l'exemple suivant, les espaces des tables de la base de données Sentinel sont affichés,
de même que leur espace total, l'espace utilisé et l'espace disponible.

```
./sdm -action dbStats -connectFile sdm.connect
```

- Exemple pour SQL Server :

Dans l'exemple suivant, les groupes de fichiers de la base de données Sentinel sont affichés, de même que leur espace total, l'espace utilisé et l'espace disponible.

```
sdm -action dbStats -connectFile sdm.connect
```

## Mise à jour des assignations (ligne de commande)

Cette action (updateMapData) permet de remplacer le fichier de données source d'une assignation par un autre fichier. Le nouveau fichier de données source doit comporter le même séparateur et les mêmes colonnes clés et colonnes activées que l'assignation précédente. Si ce n'est pas le cas, utilisez la fonctionnalité Éditer de l'interface utilisateur du Gestionnaire de données Sentinel.

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | updateMapData |
| -map | <nom de l'assignation> |
| -file | <nom du fichier> |
| -backup | <true/false> (par défaut : true) |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

L'indicateur –backup permet de sauvegarder le fichier d'origine de l'assignation dans le dossier map_data. Le fichier de l'assignation de données sauvegardé est enregistré en tant que fichier .bak et une suite de nombres aléatoires est ajouté après le nom du fichier. Par exemple : threat10197.bak.

### Mise à jour (remplacement) d'une assignation

1. Exécutez la commande suivante :

```
sdm -action updateMapData -map <nom de l'assignation>
   -file <nom du fichier> [-backup <true/false> (PAR
   DÉFAUT : true)] -connectFile <chemin d'accès
   au fichier enregistré par « saveConnection »>
```

Dans l'exemple suivant, les données de l'assignation 'threat' sont remplacées par celles du fichier d'assignation « vuln_attacks.txt ».

```
sdm -action updateMapData -map threat -file
   vuln_attacks.txt -connectFile sdm.connect
```

L'indicateur –backup n'ayant pas été utilisé, l'opération par défaut crée une sauvegarde de l'assignation d'origine avant de la mettre à jour avec les assignations du fichier « vuln_attack.txt ».

## Utilisation du script de gestion automatique fourni par Novell (Windows uniquement)

Novell a mis au point un fichier de commandes qui peut être programmé pour exécuter automatiquement plusieurs opérations du Gestionnaire de données Sentinel.

**REMARQUE** : si votre ordinateur n'a pas accès à DAS_Binary et à DAS_Query, vous pouvez utiliser la ligne de commande du Gestionnaire de données Sentinel plutôt que son interface.

Cette procédure ne s'applique qu'à Windows. Lorsque vous procédez à la préconfiguration et à la configuration du fichier de commandes, tenez compte de ce qui suit :

- Vérifiez que sdm.connect est initialisé à l'aide de l'interface du Gestionnaire de données Sentinel ou de la ligne de commande.
- Vérifiez qu'un répertoire d'archivage existe.
- Vérifiez que le nombre de jours est le même pour archiveConfig et dropPartitions.
- Vérifiez que le fichier de commandes s'exécute correctement à l'invite de la commande au moins une fois avant de le programmer pour qu'il s'exécute automatiquement.

**REMARQUE** : la tâche programmée n'enverra pas de notification si elle échoue. Elle consignera l'échec dans le journal SDM_*.log.

## Configuration du fichier Manage_data.bat pour archiver des données et ajouter des partitions

### Préconfiguration

Avant de définir automatiquement l'archivage des données et l'ajout de partitions, vous devez :

- enregistrer les propriétés de connexion,
- définir les paramètres d'archivage.

**REMARQUE** : si vous avez enregistré un fichier connect en spécifiant un emplacement ou un nom différent du chemin d'accès par défaut (%ESEC_HOME%\sdm\sdm.connect), vous devez modifier le chemin d'accès au fichier connect dans le fichier manage_data.bat.

### Définition des paramètres d'archivage

Utilisez pour cela la ligne de commande.

Cette action (archiveConfig) permet de configurer l'archivage. Cette configuration détermine comment les données sont archivées à partir des tables Sentinel.

Cette action utilise les indicateurs suivants :

| | |
|---|---|
| -action | archiveConfig |
| -dirPath | <chemin d'accès valide au répertoire dans lequel enregistrer les fichiers archivés> |
| -keepDays | <nombre de jours de conservation> |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

Définition des paramètres d'archivage via la ligne de commande

1. Créez un répertoire de sortie des archives appelé SDM_archive à la racine (c:\SDM_archive).

   **REMARQUE** : si vous créez un autre répertoire de sortie ou créez un répertoire de sortie dans un autre emplacement, vous devrez modifier le fichier manage_data.bat.

2. Exécutez cette commande comme suit :

   ```
   sdm -action archiveConfig  -dirPath <chemin d'accès
      au répertoire dans lequel enregistrer les fichiers
      archivés> -keepDays <nombre de jours de
      conservation> -connectFile <chemin d'accès
      au fichier enregistré par « saveConnection »>
   ```

   Dans l'exemple suivant, toutes les données datant de plus de 30 jours sont archivées dans le répertoire c:\SDM_archive.

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

Définition des paramètres d'archivage via l'interface

1. Créez un répertoire de sortie des archives appelé SDM_archive à la racine (c:\SDM_archive).

   **REMARQUE** : si vous créez un autre répertoire de sortie ou créez un répertoire de sortie dans un autre emplacement, vous devrez modifier le fichier manage_data.bat.

2. L'interface du Gestionnaire de données Sentinel ne requiert aucun paramètre d'archivage. Elle permet d'archiver directement des données sans qu'il soit nécessaire de définir des paramètres d'archivage.

## Supprimer des données (supprimer des partitions)

Cette action (deleteData) supprime les données d'une table donnée dont le nombre de jours de conservation est dépassé. Cette action supprime les données des tables suivantes :

- EVENTS
- CORRELATED_EVENTS
- EVT_DEST_EVT_NAME_SMRY_1
- EVT_DEST_SMRY_1
- EVT_DEST_TXNMY_SMRY_1
- EVT_PORT_SMRY_1
- EVT_SEV_SMRY_1
- EVT_SRC_SMRY_1

Cette action ne supprime pas les partitions qui ne sont pas archivées. Si vous voulez supprimer des partitions non archivées, la valeur true doit être spécifiée pour l'indicateur facultatif *forceDelete*. Si forceDelete est utilisé :

| | |
|---|---|
| false ou non spécifié | Supprime uniquement les partitions plus anciennes que keepDays et celles qui sont archivées. |
| true | Supprime toutes les partitions plus anciennes que keepDays, y compris celles qui ne sont pas archivées. |

Cette commande utilise les indicateurs suivants :

| | |
|---|---|
| -action | deleteData |
| -keepDays | <nombre de jours de conservation> |
| [-forceDelete] | <true ou false> |
| -connectFile | <chemin d'accès au fichier enregistré par saveConnection> |

Exécution de deleteData

1. Exécutez cette commande comme suit :

```
sdm -action deleteData -keepDays <nombre de jours
   de conservation> -connectFile <chemin d'accès
   au fichier enregistré par « saveConnection »>
```

   Dans l'exemple suivant, les partitions de toutes les tables datant de plus de 30 jours sont supprimées et archivées. À la fin de l'opération, une liste des partitions qui n'ont pas été supprimées est générée, si ces partitions n'ont pas été archivées.

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

## Programmation du fichier Manage_data.bat pour archiver des données et ajouter des partitions

**REMARQUE** : dans le fichier manage_data.bat, la durée de conservation des données est fixée à 30 jours, le répertoire de sortie des archives est c:\SDM_archive et le fichier connect est %ESEC_HOME%\sdm\sdm.connect. Si vous utilisez d'autres valeurs, vous devez modifier le fichier manage_data.bat.

Si vous avez défini les propriétés de connexion et les paramètres d'archivage, exécutez le fichier manage_data.bat à partir de l'invite de la commande pour vérifier qu'il fonctionne.

Pour archiver des données et ajouter des partitions automatiquement

**REMARQUE** : les instructions suivantes s'appliquent à Windows 2000 Édition professionnelle. Ces instructions peuvent différer pour Windows XP, mais sont similaires.

1. Dans Windows, cliquez sur *Démarrer* > *Paramètre* > *Panneau de configuration*.
2. Double-cliquez sur *Tâches planifiées*.
3. Double-cliquez sur *Création d'une tâche planifiée*. Cliquez sur Suivant.
4. Cliquez sur Parcourir et localisez le fichier manage_data.bat.
5. Entrez le nom de la tâche planifiée (par exemple, SDM_Archive). Sélectionnez *Tous* les jours sous *Exécuter cette tâche*. Cliquez sur *Suivant*.
6. Sélectionnez l'heure et le jour d'exécution de cette tâche. Cliquez sur Suivant.
7. Entrez une heure et une date. Cliquez sur *Suivant*.


8. Entrez l'utilisateur pour lequel cette tâche s'exécutera. L'utilisateur ne peut pas être le compte d'utilisateur du système local. Il doit s'agir d'un utilisateur spécifique. Cliquez sur *Suivant*.
9. Cliquez sur *Terminer* une fois la tâche planifiée configurée.

# 11 Utilitaires

## Démarrage et arrêt de Sentinel Server et du Gestionnaire de collecteurs - UNIX

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

### Démarrage de Sentinel Server sous UNIX

Sous UNIX, le démarrage de Sentinel Server entraîne le démarrage du serveur de communication.

Démarrage de Sentinel Server sous UNIX

1. En tant qu'utilisateur esecadm, accédez au répertoire $ESEC_HOME/sentinel/scripts avec la commande cd.
2. Exécutez la commande suivante :

```
./sentinel.sh start
```

### Arrêt de Sentinel Server sous UNIX

Sous UNIX, l'arrêt de Sentinel Server entraîne l'arrêt du serveur de communication.

Arrêt de Sentinel Server sous UNIX

1. En tant qu'utilisateur esecadm, accédez au répertoire $ESEC_HOME/sentinel/scripts avec la commande cd.
2. Exécutez la commande suivante :

```
./sentinel.sh stop
```

### Démarrage du Gestionnaire des collecteurs sous UNIX

Démarrage du Gestionnaire des collecteurs sous UNIX

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

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

## Arrêt du Gestionnaire des collecteurs sous UNIX

Arrêt du gestionnaire des collecteurs sous UNIX

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

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

# Démarrage et arrêt de Sentinel Server et du Gestionnaire de collecteurs - Windows

En fonction de votre configuration d'installation, votre machine peut exécuter jusqu'à trois services Sentinel. Ces types sont les suivants :

- Sentinel – Watchdog : démarre tous les autres processus serveur Sentinel.
- Sentinel Communication : constitue le serveur de communication Server chiffré.
- Gestionnaire des collecteurs : il s'agit de votre assistant.

Sous les services Windows, vous pouvez démarrer, redémarrer et arrêter manuellement n'importe lequel de ces services.

## Démarrage du Gestionnaire des collecteurs sous Windows

Démarrage du Gestionnaire des collecteurs sous Windows

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration.
2. Double-cliquez sur Outils d'administration.
3. Double-cliquez sur Services.
4. Cliquez avec le bouton droit, puis sélectionnez Gestionnaire des collecteurs > Démarrer.

## Arrêt du Gestionnaire des collecteurs sous Windows

Arrêt du Gestionnaire des collecteurs sous Windows

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration.
2. Double-cliquez sur Outils d'administration.
3. Double-cliquez sur Services.
4. Cliquez avec le bouton droit, puis sélectionnez Gestionnaire des collecteurs > Arrêter.

## Démarrage de Sentinel Server sous Windows

Démarrage de Sentinel Server sous Windows

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration.
2. Double-cliquez sur Outils d'administration.
3. Double-cliquez sur Services.

4. Dans la fenêtre Services, sélectionnez Sentinel.
5. Cliquez avec le bouton droit, puis sélectionnez Démarrer ou cliquez sur Démarrer dans la barre d'outils.

### Arrêt de Sentinel Server sous Windows

Arrêt de Sentinel Server sous Windows

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration.
2. Double-cliquez sur Outils d'administration.
3. Double-cliquez sur Services.
4. Dans la fenêtre Services, sélectionnez Sentinel.
5. Cliquez avec le bouton droit, puis sélectionnez Arrêter ou cliquez sur Arrêter dans la barre d'outils.

### Démarrage du serveur de communication Sentinel sous Windows

Démarrage du serveur de communication Sentinel sous Windows

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration.
2. Double-cliquez sur Outils d'administration.
3. Double-cliquez sur Services.
4. Dans la fenêtre Services, sélectionnez Sentinel Communication.
5. Cliquez avec le bouton droit, puis sélectionnez Démarrer ou cliquez sur Démarrer dans la barre d'outils.

### Arrêt du serveur de communication Sentinel sous Windows

Arrêt du serveur de communication Sentinel sous Windows

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration.
2. Double-cliquez sur Outils d'administration.
3. Double-cliquez sur Services.
4. Dans la fenêtre Services, sélectionnez Sentinel Communication.
5. Cliquez avec le bouton droit, puis sélectionnez Arrêter ou cliquez sur Arrêter dans la barre d'outils.

## Fichiers de script Sentinel

En fonction de votre configuration d'installation, le répertoire $ESEC_HOME/sentinel/scripts ou %ESEC_HOME%\sentinel\scripts peut contenir tout ou partir des fichiers de script suivants :

| Fichier de script : | Description : |
|---|---|
| remove_sonic_lock.bat | Ce script supprime les fichiers de verrouillage du serveur de communication. |
| start_broker.bat<br>start_broker.sh | Ces scripts démarrent le serveur de communication à partir de la ligne de commande en mode console. |

| | |
|---|---|
| ▪ stop_broker.bat<br>▪ stop_broker.bat | Ces scripts arrêtent le serveur de communication à partir de la ligne de commande en mode console. |
| ▪ stop_container.bat<br>▪ stop_container.sh | Ce script redémarre les conteneurs suivants :<br>DAS_Aggregation<br>DAS (RT)<br>DAS_iTRAC<br>DAS_Binary<br>DAS_Query |
| ▪ sentinel.sh | Ce script arrête ou démarre Sentinel Server.<br>Reportez-vous à Démarrage de Sentinel Server sous UNIX ou à Arrêt de Sentinel Server sous UNIX. |

## Suppression des fichiers de verrouillage du serveur de communication

Le serveur de communication risque de se verrouiller s'il ne s'est pas arrêté correctement. Si c'est le cas, vous devez supprimer les fichiers de verrouillage, puis redémarrer le serveur de communication. Ces fichiers se trouvent aux emplacements suivants :

Sous Windows :

```
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\esecDomain\data\_MFSys
   tem\lock
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\SonicMQStore\db.lck
```

Sous UNIX :

```
$ESEC_HOME/3rdparty/SonicMQ/MQ6.1/esecDomain/data/_MFSyst
   em/lock
$ESEC_HOME /3rdparty/SonicMQ/MQ6.1/SonicMQStore/db.lck
```

### Suppression du fichier de verrouillage du serveur de communication (Windows)

1. Accédez avec la commande cd ou avec Windows Explorer au répertoire :

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Double-cliquez (dans l'Explorateur Windows) sur le fichier suivant ou exécutez-le :

   ```
   remove_sonic_lock.bat
   ```

### Suppression du fichier de verrouillage du serveur de communication (UNIX)

Il n'est généralement pas nécessaire de supprimer le fichier de verrouillage sous UNIX, car il est presque toujours supprimé automatiquement lors du démarrage de Sentinel Server. Si vous devez procéder à une suppression manuelle, vous devez utiliser les commandes de système de fichiers UNIX (telles que rm).

## Démarrage du serveur de communication en mode console

Ces scripts démarrent le serveur de communication à partir de la ligne de commande en mode console. Grâce à eux, vous pouvez déboguez le serveur de communication sans exécuter le reste de Sentinel Server. En mode de fonctionnement normal, vous ne devriez pas avoir besoin de les exécuter (suivez les instructions fournies à la section Démarrage de Sentinel Server sous UNIX ou Démarrage de Sentinel Server sous Windows à la place).

### Démarrage du serveur de communication (Windows)

**REMARQUE** : lorsque vous lancez ce script dans Windows, la fenêtre Services n'indique pas qu'il a été lancé. En outre, il ne s'exécute pas tant que la fenêtre d'invite de commande reste ouverte.

1. Accédez avec la commande cd ou avec Windows Explorer au répertoire :

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Double-cliquez (dans l'Explorateur Windows) sur le fichier suivant ou exécutez-le :

   ```
   start_broker.bat
   ```

### Démarrage du serveur de communication (UNIX)

1. Ouvrez une session avec le nom d'utilisateur esecadm :
2. Avec la commande cd, accédez au répertoire :

   ```
   $ESEC_HOME/sentinel/scripts
   ```

3. Entrez :

   ```
   ./start_broker.sh
   ```

## Arrêt du serveur de communication en mode console

Ces scripts arrêtent le serveur de communication à partir de la ligne de commande en mode console. Grâce à eux, vous pouvez déboguez le serveur de communication sans arrêter le reste de Sentinel Server. En mode de fonctionnement normal, vous ne devriez pas avoir besoin de les exécuter (suivez les instructions fournies à la section Arrêt de Sentinel Server sous UNIX ou Arrêt de Sentinel Server sous Windows à la place).

### Arrêt du serveur de communication (Windows)

1. Accédez avec la commande cd ou avec Windows Explorer au répertoire :

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Double-cliquez (dans l'Explorateur Windows) sur le fichier suivant ou exécutez-le :

   ```
   stop_broker.bat
   ```

### Arrêt du serveur de communication (UNIX)

1. Ouvrez une session avec le nom d'utilisateur esecadm :
2. Avec la commande cd, accédez au répertoire :

   ```
   $ESEC_HOME/sentinel/scripts
   ```

3. Entrez :

```
./stop_broker.sh
```

## Redémarrage des conteneurs Sentinel

Les scripts suivants permettent de redémarrer les conteneurs répertoriés ci-dessous. Le script envoie un message au service spécifié lui indiquant de s'arrêter. Sentinel Watchdog redémarre ensuite le service.

La meilleure méthode pour arrêter, démarrer ou redémarrer ces services de conteneur consiste à utiliser les vues du serveur de l'onglet Admin du Centre de contrôle Sentinel.

| Nom | Description |
|---|---|
| DAS_Aggregation | (das_aggregation.xml) exécute et configure le service de regroupement. |
| DAS (RT) | (das_rt.xml) exécute et configure le service de vues en temps réel. |
| DAS_iTRAC | (das_itrac.xml) exécute et configure le service iTRAC. |
| DAS_Binary | (das_binary.xml) intervient dans les opérations d'insertion d'événements corrélés ou non. |
| DAS_Query | (das_query.xml) intervient dans toutes les autres opérations de base de données. |

### Redémarrage d'un conteneur Sentinel (Windows)

1. Avec la commande cd, accédez au répertoire :

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Entrez :

   ```
   stop_container.bat <machine hôte> <nom conteneur>
   ```

   Par exemple :

   ```
   stop_container.bat localhost DAS_RT
   ```

### Redémarrage d'un conteneur Sentinel (UNIX)

1. Ouvrez une session avec le nom d'utilisateur esecadm :
2. Avec la commande cd, accédez au répertoire :

   ```
   $ESEC_HOME/sentinel/scripts
   ```

3. Entrez :

   ```
   ./stop_container <machine hôte> <nom conteneur>
   ```

   Par exemple :

   ```
   ./stop_container localhost DAS_RT
   ```

# Informations de version

## Informations de version Sentinel Server

Sentinel Server dispose d'une option de ligne de commande qui permet d'afficher les informations de version des processus suivants :

- watchdog
- rulelg_checker
- correlation_engine
- data_synchronizer
- query_manager
- DAS

Obtention des informations de version Sentinel (UNIX)

1. Avec la commande cd, accédez au répertoire :

   ```
   $ESEC_HOME/sentinel/bin
   ```

2. Entrez :

   ```
   ./<processus> -version
   ```

   Par exemple :

   ```
   ./correlation_engine –version
   ```

Obtention des informations de version Sentinel (Windows)

1. Avec la commande cd, accédez au répertoire :

   ```
   %ESEC_HOME%\sentinel\bin
   ```

2. Entrez :

   ```
   <processus> -version
   ```

   Par exemple :

   ```
   correlation_engine –version
   ```

## Informations de version des fichiers dll et exe

Obtention des informations de version des fichiers dll et exe

1. Avec la commande cd, accédez au répertoire %ESEC_HOME%.
2. Dans les divers sous-répertoires, cliquez avec le bouton droit sur un fichier .dll ou .exe, puis sélectionnez Propriétés.
3. Cliquez sur l'onglet Version.
4. Dans le volet Item Name (Nom de l’élément), sélectionnez Product Version (Version du produit). Le numéro de version du fichier apparaît dans le volet Valeur.

### Informations de version des fichiers .jar Sentinel

Obtention des informations de version des fichiers .jar Sentinel

1. Ouvrez une session sur Sentinel Server en tant qu'utilisateur :

   Sous UNIX :

   ```
   esecadm
   ```

   Sous Windows, ouvrez une session en tant qu'utilisateur disposant des droits Sentinel Server appropriés.

2. Avec la commande cd, accédez au répertoire :

   Sous UNIX :

   ```
   $ESEC_HOME/utilities
   ```

   Sous Windows :

   ```
   %ESEC_HOME%\utilities
   ```

3. À la ligne de commande, entrez ce qui suit :

   Sous UNIX :

   ```
   ./versionreader.sh <chemin/nom fichier jar>
   ```

   Sous Windows :

   ```
   versionreader <chemin/nom fichier jar>
   ```

# Configuration de la messagerie Sentinel

Les paramètres de configuration de la messagerie Sentinel sont stockés dans le fichier execution.properties lors de l'installation. Ce fichier est modifiable après l'installation. Il réside sur la machine où le service DAS a été installé et se trouve dans le répertoire suivant :

Sous Windows :

```
%ESEC_HOME%\sentinel\config
```

Sous UNIX :

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

Deux scripts (mailconfig.sh et mailconfigtest.sh sous UNIX et mailconfig.bat et mailconfigtest.bat sous Windows) permettent de modifier les paramètres de messagerie au sein du fichier execution.properties et de les tester. Le script mailconfig.* permet de modifier les paramètres de messagerie et mailconfigtest.* de les tester. Le texte en gras correspond aux paramètres de messagerie modifiables.

Les propriétés du fichier execution.properties sont les suivantes :

| | |
|---|---|
| mail.authentication.user=<domaine\\utilisateur> | |
| correlated events retry wait=5000 | |
| mail.smtp.host=<HOTE_SMTP> | Hôte SMTP servant à envoyer les messages. |
| mail.events.max=1000 | Nombre maximal d'événements envoyé dans un message automatiquement déclenché par le moteur de corrélation. L'objectif est de limiter la taille des messages relatifs aux événements corrélés dotés d'un jeu volumineux d'événements déclencheurs. |
| correlated events retry count=10 | |
| mail.address.from=<ADRESSE_SMTP_DE> | Adresse de messagerie qui apparaît dans le champ De des messages envoyés à partir du service DAS. |
| mail.authentication.password=<mot de passe> | Mot de passe de mail.authentication.user. |

Les scripts mailconfig.sh et mailconfig.bat utilisent les arguments suivants :

| | |
|---|---|
| -host | Nom ou adresse IP de l'hôte SMTP |
| -from | Champ De du message |
| -user | Utilisateur d'authentification de messagerie |
| -password | Mot de passe de l'utilisateur d'authentification de messagerie |

**REMARQUE** : n'entrez pas votre mot de passe après l'argument –password. Vous serez invité à entrer un nouveau mot de passe après avoir entré la commande. Sur la console, le mot de passe est remplacé par des astérisques (*).

Les fichiers mailconfigtest.sh et mailconfig.bat utilisent les arguments suivants :

| | |
|---|---|
| -to | Adresse cible du message |

Pour définir les propriétés du message dans le fichier execution.properties

1. Sur la machine où le service DAS est installé, accédez avec la commande cd au répertoire suivant :

   Sous UNIX :

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

   Sous Windows :

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Exécutez mailconfig comme suit :

   Sous UNIX :

   ```
   ./mailconfig.sh -host <serveur SMTP> -from <adresse
      message source> -user <nom authentification
      messagerie> –password
   ```

   Sous Windows :

```
mailconfig.bat -host <serveur SMTP> -from <adresse
   message source> -user <utilisateur authentification
   messagerie> -password
```

Exemple sous UNIX :

```
./mailconfig.sh -host 10.0.1.14 -from
   mon_nom@domaine.com -user mon_nom_utilisateur –
   password
```

Exemple sous Windows :

```
mailconfig.bat -host 10.0.1.14 -from
   mon_nom@domaine.com -user mon_nom_utilisateur –
   password
```

Vous serez invité à entrer un nouveau mot de passe après avoir entré cette commande.

```
Enter your password:*********

Confirm your password:*********
```

**REMARQUE** : l'argument password doit toujours figurer en dernier.

Pour tester les paramètres de messagerie dans le fichier execution.properties

1. Sur la machine où le service DAS est installé, accédez avec la commande cd au répertoire suivant :

   Sous UNIX :

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

   Sous Windows :

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Exécutez mailconfigtest comme suit :

   Sous UNIX :

   ```
   ./mailconfigtest.sh -to <adresse destination message>
   ```

   Sous Windows :

   ```
   mailconfigtest.bat -to <adresse destination message>
   ```

   Si le message a été correctement envoyé, le message suivant s'affiche à l'écran.

   ```
   Email has been sent successfully!
   ```

   Accédez à la boîte de réception de la messagerie cible pour vérifier la réception du message. Voici à quoi devraient ressembler l'objet et le corps du message :

   ```
   Subject: Testing Sentinel mail property

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

# Mise à jour de votre clé de licence

Si votre clé de licence Sentinel a expiré et si Novell en a émis une nouvelle, vous devez exécuter le programme de mise à jour de clé de licence.

### Mise à jour de votre clé de licence (UNIX)

1. Ouvrez une session avec le nom d'utilisateur esecadm :
2. Accédez au répertoire $ESEC_HOME/utilities.
3. Entrez la commande suivante :

   ```
   ./softwarekey
   ```

4. Entrez le chiffre 1 pour définir la clé primaire. Appuyez sur Entrée.

### Mise à jour de votre clé de licence (Windows)

1. Ouvrez une session en tant qu'utilisateur doté des droits d'administrateur.
2. Accédez au répertoire %ESEC_HOME%\utilities.
3. Entrez la commande suivante :

   ```
   softwarekey.exe
   ```

4. Entrez le chiffre 1 pour définir la clé primaire. Appuyez sur Entrée.

# 12 Démarrage rapide

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

Ce chapitre aborde les procédures de démarrage rapide relatives aux sujets suivants :

- Security Analysts
- Report Analysts
- Administrateurs

Ce chapitre porte sur les points suivants :

- Active Views™
- Détection d'exploitation
- Données d'actif
- Requête d'événement
- Rapports d'analyse via les rapports Crystal Reports
- Corrélation de base

## Security Analysts

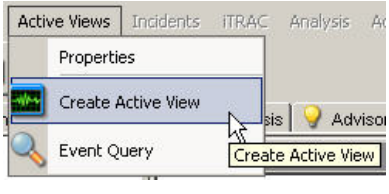
**REMARQUE** : il est supposé que vous ou votre administrateur Security avez conçu les filtres et configuré les collecteurs nécessaires à votre système.

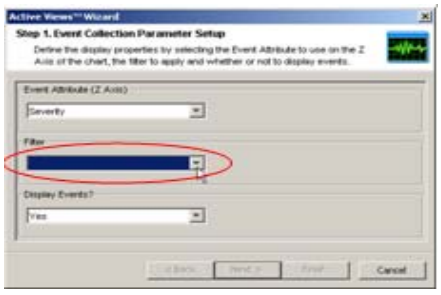
### Onglet Active Views

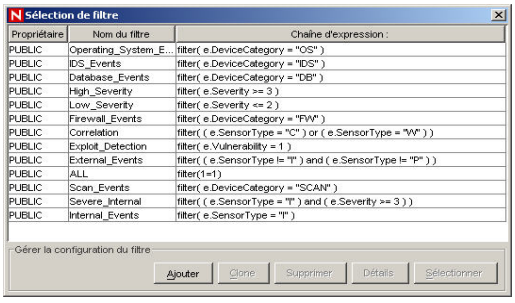
Dans l'onglet Active Views, vous pouvez surveiller les événements à mesure qu'ils se produisent et exécuter des requêtes sur ces événements. Vous pouvez les surveiller via un tableau ou via un graphique 3D.

Pour lancer un événement en temps réel

1. Cliquez sur Active *Views* > *Créer une vue active*, puis sur la flèche vers le bas Filtrer. Sélectionnez un filtre, puis cliquez sur *Sélectionner*.

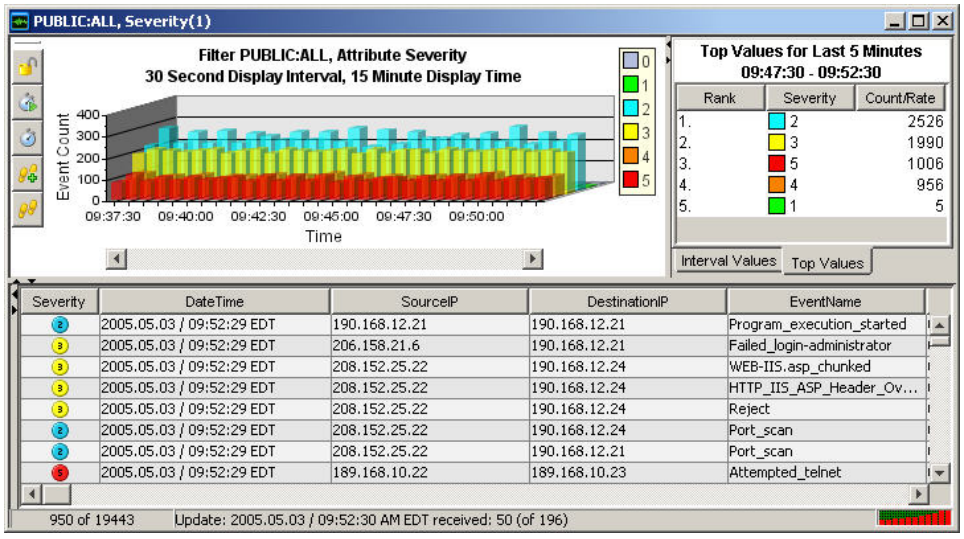





2. Cliquez sur *Terminer*. Si votre réseau est actif, une fenêtre semblable à la suivante peut s'afficher :

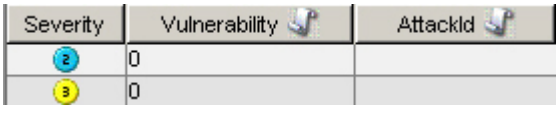
**REMARQUE** : pour afficher un graphique 3-D sans événements en temps réel, cliquez sur la flèche vers le bas Afficher les événements, puis sélectionnez *Non*.




## Détection d'exploitation

Pour afficher les événements qui signalent une exploitation possible, les fonctionnalités suivantes doivent être activées :

- Données de flux Advisor
- Détection d'intrusion
- Analyse de la vulnérabilité




Dans un événement, lorsque la valeur du champ Vulnérabilité (*vul*) est égale à 1, cela signifie que l'actif ou le périphérique cible est exploité. Si elle est égale à 0, l'actif ou le périphérique cible n'est pas exploité. Si le champ Vulnérabilité est vide, la fonction de détection d'exploitation de Sentinel n'est pas active.

Pour afficher les événements qui signalent une exploitation possible, créez une vue active comportant un filtre dont la valeur du champ Vulnérabilité est égale à 1. Si vous disposez

de Nmap et avez exécuté le connecteur Nmap, vous pouvez afficher les informations relatives à un actif, qu'il s'agisse de l'actif exploité ou d'un autre.

Pour plus d'informations sur le fonctionnement de la détection d'exploitation et connaître les systèmes de détection d'intrusion et les scanners de vulnérabilité pris en charge, reportez-vous au *Chapitre 1 : Introduction ou au Chapitre 10 : Gestionnaire de données Sentinel*.

## Données d'actif

Pour afficher les informations d'actif d'un événement, cliquez avec le bouton droit de la souris sur le ou les événements, puis sélectionnez *Analyse > Données de l'actif*. Une fenêtre semblable à celle-ci apparaît.

**Asset Report**

**desk.acmeinc.net**

**Hardware**

| | | | |
|---|---|---|---|
| **MAC Address** | A0:12:56:78:90:00 | | |
| **Name** | Build Machine | **Value** | 500 |
| **Type** | Server | **Criticality** | High |
| **Vendor** | Dell | **Sensitivity** | Low |
| **Product** | Precision | **Environment** | Production |
| **Version** | 360 | **Location** | Internal |

**Network**

| IP | Hostname |
|---|---|
| 199.16.2.23 | desk.acmeinc.net |

**Software**

| Name | Type | Vendor | Product | Version |
|---|---|---|---|---|
| ClearCase | APPLICATION | IBM | ClearCase | 5.0 |
| C++ | APPLICATION | Microsoft | Visual C++ | 6.0 |

**Contacts**

| Order | Name | Role | Email | Phone Number |
|---|---|---|---|---|
| 1 | Erickson, Stein | USER | serickson@acmedomain.net | (703) 555-8865 |
| 2 | IT | Administrator | LAN_FOLKS@acemedomain.net | (703) 555-9876 |

**Location**

| | |
|---|---|
| **Room** | server room |
| **Rack** | #17 |
| **Address** | HQ<br>Agent 86 Security Circle<br>Suite 86<br>Washington DC 12345 USA |

## Requête d'événement

Exemple de scénario : lors de la surveillance du système, vous constatez de nombreuses tentatives Telnet en provenance de l'adresse IP source 189.168.10.22. Les tentatives Telnet peuvent constituer une attaque. Telnet peut permettre à un attaquant de se connecter à un ordinateur distant comme s'il était connecté localement. Ceci peut donner lieu à des modifications de configuration non autorisées, à l'installation de programmes, de virus, etc.

Vous pouvez procéder à une requête d'événement pour savoir de combien de tentatives Telnet cet attaquant est à l'origine et configurer un filtre pour générer une requête spécifique à cet attaquant. Par exemple, vous disposez des informations suivantes :

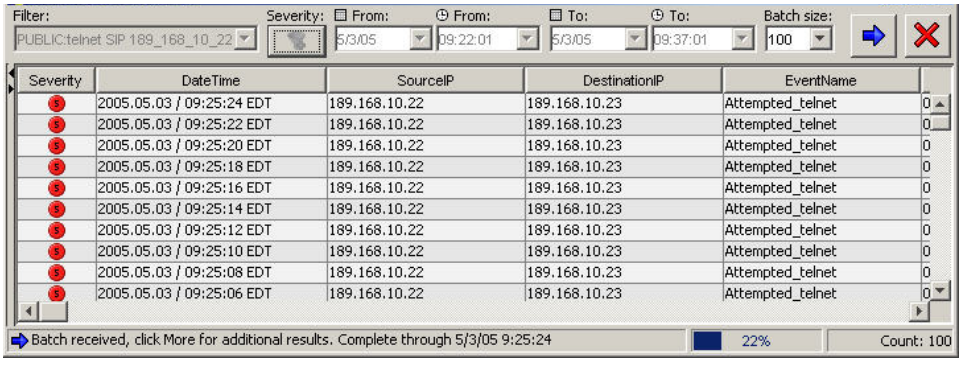
IP source : 189.168.10.22
IP cible : 189.168.10.23
Gravité : 5

Nom de l'événement : Attempted_telnet
Type de capteur : H (détection d'intrusion d'hôte)

Pour effectuer une requête d'événement

1. Cliquez sur *Requête d'événement* (icône de loupe), puis sur la flèche vers le bas du champ Filtre.
2. Cliquez sur *Ajouter*, puis entrez le nom de filtre « telnet SIP 189_168_10_22 ». Dans le champ figurant sous le filtre, entrez :

   SourceIP = 189.168.10.22 — Severity = 5
   EventName = Attempted_telnet — SensorType = H
   Match if, select (and) — DestinationIP = 189.168.10.23
3. Cliquez sur *Enregistrer*. Mettez votre filtre en surbrillance, puis cliquez sur Sélectionner.
4. Entrez la période qui vous intéresse, puis cliquez sur Rechercher (icône de loupe). Les résultats de la requête apparaissent.




Pour savoir de combien de tentatives Telnet cet attaquant est à l'origine en général, supprimez les champs DestinationIP, SensorType et Severity de votre filtre ou créez un nouveau filtre. Les résultats indiqueront toutes les adresses IP cibles faisant l'objet de tentatives Telnet de la part de cet utilisateur.

Si certains événements sont corrélés (SensorType = C ou W), vous pouvez cliquer avec le bouton droit de la souris sur > *Afficher les événements déclencheurs* pour savoir quels événements les ont déclenchés.

D'autres événements pouvant présenter un intérêt sont les événements FTP en surnombre. Il peut également s'agir d'une connexion distante, qui permet le transfert, la copie et la suppression de fichiers.

Voici une liste brève d'attaques présentant un intérêt. Les types d'attaques sont répertoriés dans une liste complète. Pour plus d'informations sur les attaques de réseau/d'hôte, de nombreuses ressources (manuels et Internet) sont disponibles. Elles décrivent en détail les différents types d'attaques.

| | | |
|---|---|---|
| Inondation SYN | Reniflage de paquets | Attaque de type Smurf et Fraggle |
| Inondation ICMP et UDP | Refus de service | Attaque de dictionnaire |

# Report Analysts

**REMARQUE** : il est supposé que votre administrateur Security a configuré votre serveur Web Crystal Enterprise et publié une liste de rapports disponibles.

## Onglet Analyse

L'onglet Analyse permet de générer des rapports d'historique. Les rapports d'historique et ceux relatifs aux vulnérabilités sont publiés sur un serveur Web Crystal et sont générés directement à partir de la base de données Sentinel. Ces rapports peuvent s'avérer utiles pour effectuer le suivi des activités sur une longue période (par exemple, une semaine ou un mois) et examiner ces activités. Ces rapports constituent également une base pour générer des rapports consolidés destinés à vos superviseurs. Si votre serveur Web de rapports est installé, consultez la barre de votre navigateur pour savoir quels rapports sont disponibles.

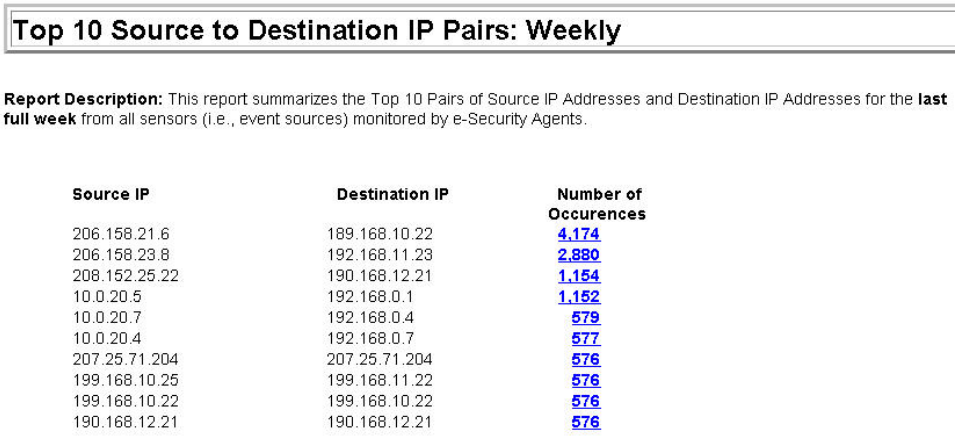
**REMARQUE** : le rapport suivant est un exemple de rapport Crystal 9. Les procédures sont les mêmes pour Crystal 11, quel que soit le nom des rapports.

Par exemple, vous êtes chargé de générer des rapports pour votre direction. Il est probable que vous exécutiez le rapport SourceDestinationReports. Ces rapports sont les 10 premières paires IP source - IP cible sur les noms d'hôte, les ports, les adresses IP et les utilisateurs. Pour exécuter ce rapport, procédez comme suit :

Exécution d'un rapport Crystal

1. Développez les dix premiers rapports et mettez en surbrillance les 10 premières paires IP source - IP cible, puis cliquez sur le bouton *Créer un rapport* (loupe).
2. Entrez esecrpt (pour l'authentification SQL et Oracle) comme nom d'utilisateur ou votre nom d'utilisateur d'authentification Windows, puis votre mot de passe.
3. Dans la zone Report Type (Type de rapport), sélectionnez *Weekly Report* (Rapport hebdomadaire). Sélectionnez Specific Date Range (Période spécifique) si vous souhaitez une plage de dates spécifique.

   **REMARQUE** : d'autres rapports peuvent comporter des paramètres supplémentaires (par exemple, le nom de la ressource et la plage de gravité).
4. Cliquez sur *Afficher le rapport*.

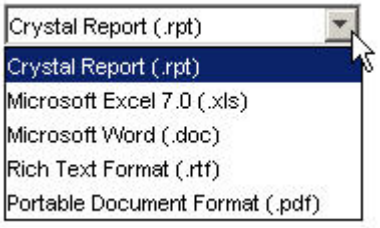


**Top 10 Source to Destination IP Pairs: Weekly**

**Report Description:** This report summarizes the Top 10 Pairs of Source IP Addresses and Destination IP Addresses for the **last full week** from all sensors (i.e., event sources) monitored by e-Security Agents.

| Source IP | Destination IP | Number of Occurences |
|---|---|---|
| 206.158.21.6 | 189.168.10.22 | 4,174 |
| 206.158.23.8 | 192.168.11.23 | 2,880 |
| 208.152.25.22 | 190.168.12.21 | 1,154 |
| 10.0.20.5 | 192.168.0.1 | 1,152 |
| 10.0.20.7 | 192.168.0.4 | 579 |
| 10.0.20.4 | 192.168.0.7 | 577 |
| 207.25.71.204 | 207.25.71.204 | 576 |
| 199.168.10.25 | 199.168.11.22 | 576 |
| 199.168.10.22 | 199.168.10.22 | 576 |
| 190.168.12.21 | 190.168.12.21 | 576 |

5. Vous pouvez exporter ce fichier en tant que fichier Word, PDF, rtf ou Excel ou en tant que rapport Crystal Report en cliquant sur Exporter (enveloppe).




## Requête d'événement

De même qu'avec Security Analysts, si vos rapports comportent un ou plusieurs événements qui vous intéressent, vous pouvez exécuter une requête d'événement dans l'onglet Analyse. Pour exécuter une requête, sélectionnez *Historical Events (Événements historiques)* > *Requêtes d'événements historiques*, puis cliquez sur *Créer un rapport* (loupe). Pour plus d'informations, reportez-vous à Requête d'événement.

# Administrateurs

## Corrélation de base

La corrélation est un processus consistant à analyser les événements de sécurité pour identifier les relations potentielles existant entre deux événements ou plus. La corrélation permet une association rapide des attaques prioritaires en fonction d'éléments communs des données d'événement.

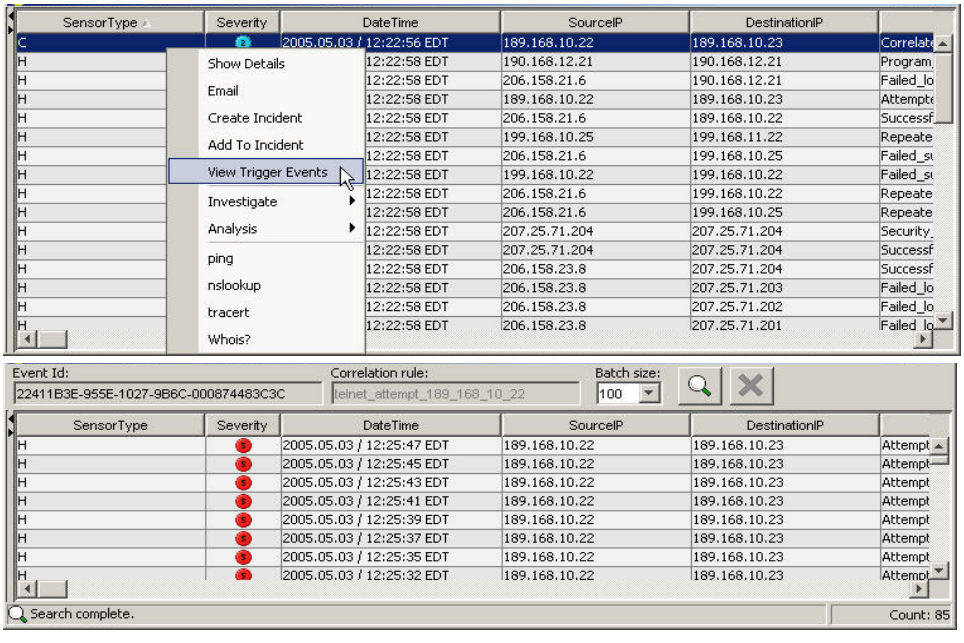
Par rapport au scénario Telnet de la section Requête d'événement, une règle de corrélation de base peut être créée qui déclenchera un événement corrélé lorsque 4 tentatives Telnet sont effectuées dans un laps de temps de 10 secondes.

Pour créer une règle de corrélation

1. Ouvrez l'onglet Admin et sélectionnez Règles de corrélation dans la barre de navigation.
2. Créez un nouveau dossier et placez-y votre règle. Pour ce faire, utilisez une option du menu du bouton droit de la souris.
3. Sélectionnez Basic Correlation (Corrélation de base), entrez un nom, puis cliquez sur *Suivant*. Dans le panneau suivant, cliquez sur la flèche vers le bas, puis sélectionnez Gestionnaire de filtres. Cliquez sur la flèche vers le bas Filtre sélectionné, puis, dans le panneau Sélection de filtre, cliquez sur *Ajouter*.
4. Entrez les informations suivantes :
   - Nom : telnet_attempt_189_168_10_22
   - Nom du filtre : telnet_attempt_189_168_10_22
   - SourceIP = 189.168.10.22
   - Nom de l'événement = $Attempted_telnet
   - Sélectionnez *Et*
   - Severity = 5
   - SensorType = H
   - DestinationIP = 189.168.10.23

5. Cliquez sur *Enregistrer*. Mettez votre filtre en surbrillance, puis cliquez sur *Sélectionner*.
6. Cliquez sur Suivant, entrez la valeur 4 pour les cas où la condition est remplie et 10 secondes dans le panneau Threshold Grouping Criteria (Critères de regroupement et de seuil). Cliquez sur Suivant.
7. Dans le panneau Événements et opérations corrélés, redéfinissez le niveau de gravité sur 2 (cliquez sur la flèche vers le bas). Cliquez sur Terminer.
8. Pour déployer cette règle, sélectionnez Gestionnaire de moteurs de corrélation dans le panneau de navigation, sélectionnez un moteur de corrélation, puis cliquez avec le bouton droit de la souris sur > *Déployer les règles*. Dans le panneau Déployer les règles, recherchez votre règle et cochez-la. Cliquez sur OK. Vérifiez que votre moteur de corrélation et votre règle de corrélation comportent une coche verte indiquant qu'ils sont activés. Pour ce faire, cliquez avec le bouton droit de la souris.
9. Diverses méthodes vous permettent de vérifier la présence d'événements corrélés. En voici quelques-unes :
   - Création d'une fenêtre Active View Events (Événements de la vue active) à l'aide du filtre de corrélation que vous avez créé
   - Création d'une fenêtre Active View Events (Événements de la vue active) à l'aide du filtre de corrélation fourni.
   - Création d'une fenêtre Active View Events (Événements de la vue active) à l'aide du filtre Tout fourni, prise d'un instantané, tri de la liste par SensorType et affichage de tous les événements dont le champ SensorType a la valeur C.
   - Réalisation d'une requête rapide à l'aide du filtre que vous avez créé ou du filtre de corrélation.

   Cliquez avec le bouton droit de la souris sur l'événement corrélé et sélectionnez *Afficher les événements déclencheurs* pour savoir combien de tentatives Telnet (peut-être plus de 4) ont déclenché cette règle de corrélation.



# A Événements système de Sentinel 5

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

Dans les tableaux de description ci-dessous, les mots en italique entourés de <…> sont remplacés par les valeurs appropriées dans les messages réels.

## Événements d'authentification

### Échec d'authentification

Lorsqu'une authentification d'utilisateur échoue, l'événement suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | AuthenticationFailed (EchecAuthentification) |
| Ressource | UserAuthentication (AuthentificationUtilisateur) |
| Sous-ressource | Authenticate (Authentifier) |
| Message | Authentication of user <*name*> with OS name <*domUser*> from <*IP*> failed (Échec de l'authentification de l'utilisateur <nom> doté du nom OS <UtilisateurDomaine> de <IP>) |

### Aucun événement utilisateur de ce type

Lorsqu'un utilisateur tente d'ouvrir une session sur l'application et que l'authentification a réussi, alors que l'utilisateur n'est pas un utilisateur de Sentinel, l'événement suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | NoSuchUser (AucunUtilisateurDeCeType) |
| Ressource | UserAuthentication (AuthentificationUtilisateur) |
| Sous-ressource | Authenticate (Authentifier) |
| Message | No existing user with name <*name*> found (Aucun utilisateur existant doté du nom <*nom*> n'a été trouvé) |

### Objets utilisateur en double

En présence d'un second objet utilisateur actif inattendu, l'événement suivant est généré. Il s'agit d'une erreur interne.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | TooManyActiveUsers (TropUtilisateursActifs) |
| Ressource | UserAuthentication (AuthentificationUtilisateur) |
| Sous-ressource | Authenticate (Authentifier) |
| Message | Error in user table : Multiple users with the name <*name*> found (Erreur dans la table des utilisateurs : plusieurs utilisateurs dotés du nom <*nom*> ont été trouvés) |

### Compte verrouillé

Lorsqu'un compte utilisateur verrouillé tente d'ouvrir une session, l'événement suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | LockedUser (UtilisateurVerrouillé) |
| Ressource | UserAuthentication (AuthentificationUtilisateur) |
| Sous-ressource | Authentication (Authentification) |
| Message | Attempt to login using locked account <*acct*> (Tentative de connexion à l'aide du compte verrouillé <*compte*>) |

## Sessions utilisateur

### Session utilisateur fermée

Lorsqu'un utilisateur ferme une session, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | UserLoggedOut (Utililateurdéconnecté) |
| Ressource | UserSessionManager (GestionnaireSessionUtilisateur) |
| Sous-ressource | User (Utilisateur) |
| Message | Closing session for <*user*> OS name <*osName*> from <*IP*> was on since <*date*>; currently <*num*> active users (Fermeture de la session pour <*utilisateur*> doté du nom OS <*NomOS*> de <*IP*> active depuis <*date*> ; actuellement, <*nombre*> utilisateurs actifs) |

### Session utilisateur ouverte

Lorsqu'un utilisateur ouvre une session, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | UserLoggedIn (UtilisateurConnecté) |
| Ressource | UserSessionManager (GestionnaireSessionUtilisateur) |
| Sous-ressource | User (Utilisateur) |
| Message | User <*user*> with OS name <*osName*> at <*IP*> logged in; currently <*num*> active users (Utilisateur <*utilisateur*> doté du nom OS <*NomOS*> à <*IP*> connecté ; actuellement <*nombre*> utilisateurs actifs) |

### Utilisateur détecté

Lorsque le serveur redémarre, il perd les informations de session. Il reconstruit la session au moment où il reçoit des messages provenant des utilisateurs actifs. Lorsqu'il détecte un utilisateur connecté, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | UserLoggedIn (UtilisateurConnecté) |
| Ressource | UserSessionManager (GestionnaireSessionUtilisateur) |
| Sous-ressource | User (Utilisateur) |
| Message | Discovered active user <*user*> with OS name <*osName*> at <*IP*> logged in; currently <*num*> active users (Découverte de l'utilisateur actif <*utilisateur*> doté du nom OS <*NomOS*> à <*IP*> connecté ; actuellement, <*nombre*> utilisateurs actifs) |

## Événement

### Erreur lors du déplacement d'un fichier terminé

Lorsqu'un fichier d'événement est terminé, il est placé dans le répertoire de sortie. Si cette opération échoue, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 3 |
| Nom de l'événement | MoveArchiveFileFailed (ÉchecDéplacementFichierArchive) |
| Ressource | *<DAS name> (<Nom DAS>)* |

| | |
|---|---|
| Sous-ressource | ArchiveFile (FichierArchive) |
| Message | Error moving completed archive file <*fname*> to <*dir*> (Erreur lors du déplacement du fichier archive terminé <*nom_fichier*> vers <*rép*>) |

## Erreur lors de l'insertion d'événements

Lorsque l'insertion d'événements dans la base de données échoue, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 5 |
| Nom de l'événement | InsertEventsFailed (ÉchecInsertionÉvénements) |
| Ressource | EventSubsystem (Sous-systèmeÉvénement) |
| Sous-ressource | Events (Événements) |
| Message | Error inserting events into the Database—the events may be permanently lost. (Erreur lors de l'insertion d'événements dans la base de données : les événements peuvent être définitivement perdus.) Please check the Database and backend server logs <*Exception*> (Veuillez vérifier la base de données et le paramètre <*Exception*> des journaux du serveur principal) |

## Échec de l'ouverture d'un fichier d'archive

Lorsque l'ouverture d'un fichier d'archive dans lequel sont stockés les événements à regrouper échoue, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 3 |
| Nom de l'événement | OpenArchiveFileFailed (ÉchecOuvertureFichierArchive) |
| Ressource | <*Das name*> (<*Nom DAS*>) |
| Sous-ressource | ArchiveFile (FichierArchive) |
| Message | Error opening archive file <*name*> in <*dir*> (Erreur lors de l'ouverture du fichier archive <*nom*> du répertoire <*rép*>) |

## Échec de l'écriture d'un fichier d'archive

Lorsque l'écriture d'un fichier d'archive dans lequel sont stockés les événements à regrouper échoue, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 3 |
| Nom de l'événement | WriteArchiveFileFailed (ÉchecÉcritureFichierArchive) |
| Ressource | <*Das name*> (<*Nom DAS*>) |

| Balise | Valeur |
|---|---|
| Sous-ressource | ArchiveFile (FichierArchive) |
| Message | Error writing newly received events to aggregation archive file <*fname*> (Erreur lors de l'écriture d'événements récemment reçus vers le fichier d'archive de regroupement <*nom_fichier*>) |

## Écriture sur la partition de dépassement (P_MAX)

Un événement notifiant l'utilisateur que des événements sont en cours d'écriture sur la partition de dépassement (P_MAX) est envoyé environ toutes les 5 minutes. Lorsque cela se produit, l'administrateur doit ajouter des partitions supplémentaires à l'aide du Gestionnaire de données Sentinel sans quoi les performances commenceront à se dégrader.

| Balise | Valeur |
|---|---|
| Gravité | 5 |
| Nom de l'événement | InsertIntoOverflowPartition (InsertionDansPartitionDépassement) |
| Ressource | EventSubSystem (Sous-systèmeÉvénement) |
| Sous-ressource | Events (Événements) |
| Message | Error: (Erreur :) currently inserting into the overflow partitions (P_MAX), add more partitions (actuellement en cours d'insertion dans les partitions de dépassement (P_MAX), ajouter des partitions supplémentaires) |

## Insertion d'événements bloquée

Si DAS écrit des données dans la partition de dépassement et si l'utilisateur tente d'ajouter des partitions, le Gestionnaire de données Sentinel envoie une requête à DAS pour qu'il suspende temporairement l'insertion d'événements dans la base de données. Lorsque cela se produit, DAS envoie des événements internes chaque fois qu'il tente d'insérer des événements dans la base de données.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | EventInsertionIsBlocked (InsertionÉvénementBloquée) |
| Ressource | EventSubSystem (Sous-systèmeÉvénement) |
| Sous-ressource | Événements |
| Message | Event insertion is blocked, waiting <*num*> sec (Insertion événement bloquée, attente de <*nombre*> secondes) |

## Reprise de l'insertion d'événements

Lorsque l'insertion d'événements reprend après avoir été bloquée, l'événement suivant est transmis.

| Balise | Valeur |
|---|---|
| Gravité | 2 |
| Nom de l'événement | EventInsertionResumed (RepriseInsertionÉvénement) |
| Resource | EventSubSystem (Sous-systèmeÉvénement) |
| SubResource | Events (Événements) |
| Message | Event insertion has resumed after being blocked (Insertion d'événement reprise après avoir été bloquée) |

## Seuil de temps spécifié atteint par l'espace de base de données

Lorsque l'insertion d'événements reprend après avoir été bloquée, l'événement suivant est transmis.

| Balise | Valeur |
|---|---|
| Gravité | 0 |
| Nom de l'événement | DbSpaceReachedTimeThrshld (EspaceBddAtteintSeuilTemps) |
| Ressource | Database (BaseDeDonnées) |
| Sous-ressource | Database (BaseDeDonnées) |
| Message | Tablespace <*string*> has <*num*> MB left and growing <*num*> bytes per second and will run out space within the time threshold specified <*num*> seconds (L'espace des tables <*chaîne*> a <*nombre*> Mo restants et augmente de <*nombre*> octets par seconde et manquera d'espace avant le seuil de temps spécifié <*nombre*> secondes) |

## Seuil de pourcentage spécifié atteint par l'espace de base de données

Lorsque l'insertion d'événements reprend après avoir été bloquée, l'événement suivant est transmis.

| Balise | Valeur |
|---|---|
| Gravité | 0 |
| Nom de l'événement | DbSpaceReachedPercentThrshld (EspaceBddAtteintPourcentSeuil) |
| Ressource | Database (BaseDeDonnées) |
| Sous-ressource | Database (BaseDeDonnées) |
| Message | Tablespace <*string*> has current size of <*num*> MB with a max size of <*num*> MB and has reached the percentage threshold of <*num*> % (L'espace des tables <*chaîne*> a une taille actuelle de <*nombre*> Mo avec une taille max de <*nombre*> Mo et a atteint le seuil de pourcentage de <*nombre*> %) |

### Espace de base de données très faible

Lorsque l'insertion d'événements reprend après avoir été bloquée, l'événement suivant est transmis.

| Balise | Valeur |
|---|---|
| Gravité | 5 |
| Nom de l'événement | EspaceBddTrèsFaible |
| Ressource | Database (BaseDeDonnées) |
| Sous-ressource | Database (BaseDeDonnées) |
| Message | Tablespace <*string*> has current size of <*num*> MB and has reached the physical threshold of <*num*> MB (L'espace des tables <*chaîne*> a une taille actuelle de <*nombre*> Mo et a atteint le seuil physique de <*nombre*> Mo) |

## Regroupement

### Erreur lors de l'insertion de données récapitulatives dans la base de données

Si une erreur se produit lors du regroupement de données dans la base de données, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | SummaryUpdateFailure (ÉchecMiseÀJourRécapitulatif) |
| Ressource | Aggregation (Regroupement) |
| Sous-ressource | Summary (Récapitulatif) |
| Message | Error saving summary batch to the database for summary <*summaryName*> (Erreur lors de l'enregistrement vers la base de données du récapitulatif <*NomRécapitulatif*>) |

## Service d'assignation

### Erreur lors de l'initialisation de l'assignation portant l'ID

L'événement interne ErrorNoSuchMap est généré par le côté client du service d'assignation (celui qui fait partie du Gestionnaire des collecteurs). Cette erreur est générée lorsque le Gestionnaire des collecteurs tente de récupérer une assignation qui n'existe pas. Bien que cet événement ne devrait pas se produire, il peut être déclenché si des assignations sont créées, puis supprimées.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | ErrorNoSuchMap (ErreurAucuneAssignationDeCeType) |
| Ressource | MappingService (ServiceAssignation) |

| Balise | Valeur |
|---|---|
| Sous-ressource | ReferentialDataObjectMap (AssignationObjetDonnéesRéférence) |
| Message | Error initializing map with id <ID>: no such map (Erreur lors de l'initialisation de l'assignation avec l'ID <ID> : aucune assignation de ce type) |

## Actualisation de l'assignation à partir du cache

L'événement interne LoadingMapFromCache est généré par le côté client du service d'assignation (celui qui fait partie du Gestionnaire des collecteurs). Lorsque le Gestionnaire des collecteurs reçoit une demande d'actualisation de l'assignation pour prendre en compte les modifications dont elle ou sa définition a fait l'objet, il envoie un événement interne. Cela signifie que le cache est à jour et qu'il rafraîchit l'assignation à partir du cache.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | LoadingMapFromCache (ChargementAssignationDuCache) |
| Ressource | MappingService (ServiceAssignation) |
| Sous-ressource | ReferentialDataObjectMap (AssignationObjetDonnéesRéférence) |
| Message | Loading from cache v<*version*> of map <*mapName*> (ID <*id*>) (Chargement à partir du cache de la version <*version*> de l'assignation <*nomAssignation*> (ID <*id*>) |

## Actualisation de l'assignation à partir du serveur

L'événement interne RefreshingMapFromServer est généré par le côté client du service d'assignation (celui qui fait partie du Gestionnaire des collecteurs). Lorsque le Gestionnaire des collecteurs reçoit une demande d'actualisation de l'assignation pour prendre en compte les modifications dont elle ou sa définition a fait l'objet, il envoie un événement interne. Cela signifie que l'assignation ne se trouvait pas dans le cache ou la version en cache n'était pas à jour et que le Gestionnaire des collecteurs extrait l'assignation du serveur.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | RefreshingMapFromServer (ActualisationAssignationDuServeur) |
| Ressource | MappingService (ServiceAssignation) |
| Sous-ressource | ReferentialDataObjectMap (AssignationObjetDonnéesRéférence) |
| Message | Refreshing from server map <name> with id <ID> (Actualisation à partir de l'assignation du serveur <nom> avec l'ID <ID>) |

## Timeout lors de l'actualisation de l'assignation

L'événement interne TimeoutRefreshingMap est généré par le côté client du service d'assignation (celui qui fait partie du Gestionnaire des collecteurs). Lorsque le Gestionnaire des collecteurs reçoit une demande d'actualisation de l'assignation pour prendre en compte les

modifications dont elle
ou sa définition a fait l'objet, il envoie un événement interne. Cela signifie que le Gestionnaire des collecteurs a tenté d'extraire une assignation du serveur. Celui-ci n'ayant jamais accusé réception de la requête, la requête a expiré. Cette erreur est considérée comme transitoire et le Gestionnaire des collecteurs effectuera une nouvelle tentative.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | TimeoutRefreshingMap (TimeoutActualisationAssignation) |
| Ressource | MappingService (ServiceAssignation) |
| Sous-ressource | ReferentialDataObjectMap (AssignationObjetDonnéesRéférence) |
| Message | Request timed out while refreshing map <name>: (Expiration du délai de la requête lors de l'actualisation de l'assignation <nom> : <exception>) |

## Erreur lors de l'actualisation de l'assignation

Cet événement interne est généré par le côté client du service d'assignation (celui qui fait partie du Gestionnaire de collecteurs). Lorsque le Gestionnaire des collecteurs reçoit une demande d'actualisation de l'assignation pour prendre en compte les modifications dont elle ou sa définition a fait l'objet, il envoie un événement interne. Cela signifie qu'une erreur non transitoire s'est produite lors de la tentative d'actualisation de l'assignation. Le Gestionnaire des collecteurs attendra 15 minutes avant d'effectuer une nouvelle tentative. Si cet événement se produit au cours de l'initialisation, l'initialisation se poursuit et cette assignation est ignorée jusqu'à ce qu'elle soit correctement chargée.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | ErrorRefreshingMapData (ErreurActualisationDonnéesAssignation) |
| Ressource | ServiceAssignation |
| Sous-ressource | ReferentialDataObjectMap (AssignationObjetDonnéesRéférence) |
| Message | Error refreshimg map <*mapName*>: (Erreur lors de l'actualisation de l'assignation <*nomAssignation*> : <*exc*>) |

## Assignation volumineuse chargée

L'événement interne LoadedLargeMap est un événement d'information envoyé par le service d'assignation qui indique qu'une assignation volumineuse a été chargée vers le Gestionnaire des collecteurs. Une assignation est considérée comme volumineuse lorsqu'elle contient plus de 100 000 lignes.

| Balise | Valeur |
|---|---|
| Gravité | 0 |
| Nom de l'événement | LoadedLargeMap (AssignationVolumineuseChargée) |
| Ressource | MappingService (ServiceAssignation) |

| | |
|---|---|
| Sous-ressource | ReferentialDataObjectMap |
| Message | Finished loading map <name> with id <ID> and <num> entries and total size <#>Kb in <##>sec (Chargement terminé de l'assignation <nom> avec l'ID <ID> et <nombre> entrées dont la taille totale est <#>Ko en <##> secondes) |

## Durée de chargement d'assignation longue

L'événement interne LongTimeToLoadMap est un événement d'information envoyé par le service d'assignation qui indique que le chargement d'une assignation a pris un temps anormalement long (durée supérieure à une minute).

| Balise | Valeur |
|---|---|
| Gravité | 0 |
| Nom de l'événement | LongTimeToLoadMap (TempsChargementAssignationLong) |
| Ressource | MappingService (ServiceAssignation) |
| Sous-ressource | ReferentialDataObjectMap |
| Message | It took <##>sec to load map <name> with id <ID> and <num> entries and total size <##>Kb (<##> secondes ont été nécessaires pour charger l'assignation <nom> avec l'ID <ID> et <nombre> entrées et dont la taille totale est <##> Ko) |

## Timeout dépassé lors de l'attente du rappel

Lorsque le Gestionnaire des collecteurs doit rafraîchir une assignation, il envoie une requête au système principal. La requête comporte un rappel. Le système principal génère l'assignation et lorsque celle-ci est prête, il l'envoie au Gestionnaire des collecteurs à l'aide du rappel. Si la réponse prend trop longtemps à arriver (plus de dix minutes), le Gestionnaire des collecteurs envoie une seconde demande car il suppose que la première a été perdue. Si tel est le cas, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 2 |
| Nom de l'événement | TimedoutWaitingForCallback (TimeoutDépasséAttenteRappel) |
| Ressource | MappingService (ServiceAssignation) |
| Sous-ressource | ReferentialDataObjectMap (AssignationObjetDonnéesRéférence) |
| Message | Map <name> timed out waiting for callback with new map data-retrying (Timeout dépassé pour l'assignation <nom> en attente du rappel avec nouvelles données d'assignation : nouvelle tentative) |

### Erreur lors de l'application d'une mise à jour par incrément

L'événement ErrorApplyingIncrementalUpdate est envoyé lorsque le service d'assignation ne parvient pas appliquer une mise à jour à une assignation client existante.

| Balise | Valeur |
|---|---|
| Gravité | 4 |
| Nom de l'événement | ErrorApplyingIncrementalUpdate (ErreurApplicationMiseÀJourParIncrément) |
| Ressource | MappingService (ServiceAssignation) |
| Sous-ressource | ReferentialDataObjectMap (AssignationObjetDonnéesRéférence) |
| Message | The error <error> occurred while applying updates to map <*mapName*> (ID <*mapId*>) v.<*version*>. Rescheduling a refresh to complete map update. (L'erreur <erreur> s'est produite lors de l'application de mises à jour de l'assignation <*nomAssignation*> (ID <*IDAssignation*>) version <*version*>. Planification d'une nouvelle actualisation pour terminer la mise à jour de l'assignation.) |

### Erreur de synchronisation détectée

L'événement OutOfsyncDetected est envoyé lorsque le service d'assignation détecte qu'une assignation est périmée. Le service d'assignation planifie automatiquement une actualisation.

| Balise | Valeur |
|---|---|
| Gravité | 2 |
| Nom de l'événement | OutOfsyncDetected (ErreurSynchronisationDétectée) |
| Ressource | MappingService (ServiceAssignation) |
| Sous-ressource | ReferentialDataObjectMap (AssignationObjetDonnéesRéférence) |
| Message | Map <*mapName*> detected the map data is out-of-sync, probably due to a missed update notification--scheduling a refresh (L'assignation <*nomAssignation*> a détecté que les données d'assignation ne sont plus à jour, probablement à cause d'une notification de mise à jour manquée – planification d'actualisation en cours) |

# Routeur d'événements

## Routeur d'événements en cours d'exécution

Le routeur d'événements est le composant principal du Gestionnaire des collecteurs (il est celui qui réalise les assignations, qui applique les filtres globaux et qui publie les événements). L'événement interne EventRouterIsRunning est envoyé au routeur lors de l'initialisation lorsque celui-ci est prêt. Au redémarrage du Gestionnaire des collecteurs, un autre événement est envoyé lorsqu'il est prêt.

L'événement n'est envoyé que lorsque le routeur d'événements a correctement chargé tous les filtres globaux et l'intégralité des informations d'assignation.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | EventRouterIsRunning (RouteurÉvénementsEnCoursExécution) |
| Ressource | AgentManager (GestionnaireAgents) |
| Sous-ressource | EventRouter (RouteurÉvénements) |
| Message | Event router completed its initialization in <mode> mode (Le routeur d'événements à terminé son initialisation en mode <mode>) |

## Routeur d'événements en cours d'initialisation

L'événement interne EventRouterInitializing est envoyé lorsqu'un routeur d'événements commence son initialisation, c'est-à-dire lorsqu'il a établi une connexion avec le système principal (DAS Query).

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | EventRouterInitializing (InitialisationRouteurÉvénements) |
| Ressource | AgentManager (GestionnaireAgents) |
| Sous-ressource | EventRouter (RouteurÉvénements) |
| Message | Le routeur d'événements lance l'initialisation en mode <mode> |

## Routeur d'événements en cours d'arrêt

L'événement EventRouterStopping est envoyé lorsque le routeur d'événements reçoit une requête lui indiquant de s'arrêter au cours du processus d'arrêt.

| Balise | Valeur |
|---|---|
| Gravité | 2 |
| Nom de l'événement | EventRouterStopping (RouteurÉvénementsArrêt) |
| Ressource | AgentManager (GestionnaireAgents) |
| Sous-ressource | EventRouter (RouteurÉvénements) |
| Message | Routeur d'événements en cours d'arrêt |

## Routeur d'événements en cours d'achèvement

L'événement EventRouterTerminating est envoyé lorsque le routeur d'événements reçoit une requête lui indiquant de s'arrêter au cours du processus d'arrêt.

| Balise | Valeur |
|---|---|
| Gravité | 2 |
| Nom de l'événement | RouteurÉvénementsAchèvement |
| Ressource | AgentManager (GestionnaireAgents) |
| Sous-ressource | EventRouter (RouteurÉvénements) |
| Message | Event router is terminating (Routeur d'événements en cours d'achèvement) |

# Moteur de corrélation

## Moteur de corrélation en cours d'exécution

Le processus du moteur de corrélation peut être rendu inactif par l'utilisateur. Son état d'exécution détermine si le processus actif est en train de traiter ou non des événements. Le processus démarre avec l'état inactif (arrêté) et attend de récupérer la configuration depuis la base de données. L'événement EngineRunning est envoyé lorsque le moteur change d'état (arrêt à en cours d'exécution).

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | EngineRunning (MoteurEnCoursExécution) |
| Ressource | CorrelationEngine (MoteurCorrélation) |
| Sous-ressource | CorrelationEngine (MoteurCorrélation) |
| Message | Correlation Engine is processing events. (Le moteur de corrélation est en train de traiter les événements.) |

## Moteur de corrélation arrêté

L'événement EngineStopped est envoyé lorsque le moteur change d'état (en cours d'exécution à arrêt).

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | EngineStopped (MoteurArrêté) |
| Ressource | CorrelationEngine (MoteurCorrélation) |
| Sous-ressource | CorrelationEngine (MoteurCorrélation) |
| Message | Correlation Engine has stopped processing events. (Le moteur de corrélation a arrêté de traiter les événements.) |

## Déploiement de règles démarré

L'événement DeploymentStarted est envoyé lorsque le moteur a correctement chargé un déploiement de règles, et ce quel que soit l'état d'exécution du moteur.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | DeploymentStarted (DéploiementDémarré) |
| Ressource | CorrelationEngine (MoteurCorrélation) |
| Sous-ressource | Deployment (Déploiement) |
| Message | deployment <name> started (déploiement <nom> démarré) |

## Déploiement de règles arrêté

L'événement DeploymentStopped est envoyé lorsque le moteur a correctement déchargé un déploiement de règles,  et ce quel que soit l'état d'exécution du moteur.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | DeploymentStopped (DéploiementArrêté) |
| Ressource | CorrelationEngine (MoteurCorrélation) |
| Sous-ressource | Deployment (Déploiement) |
| Message | deployment  <name> stopped<br>(déploiement <nom> arrêté) |

## Déploiement de règles modifié

L'événement DeploymentModified est envoyé lorsque le moteur a correctement rechargé un déploiement de règles, et ce quel que soit l'état d'exécution du moteur.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | DeploymentModified (DéploiementModifié) |
| Ressource | CorrelationEngine (MoteurCorrélation) |
| Sous-ressource | Déploiement |
| Message | Deployment <name> modified (Déploiement <nom> modifié) |

# Watchdog

## Processus contrôlé démarré

Watchdog est exécuté en tant que service.  Sa principale fonction est de maintenir les processus Sentinel en cours d'exécution.  Si un processus s'arrête, Watchdog le redémarre automatiquement. L'événement ProcessStart est envoyé lorsqu'un processus est redémarré.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | ProcessStart (ProcessusDémarré) |
| Ressource | Watchdog |
| Sous-ressource | Process (Processus) |
| Message | Process <ProgramName> spawned (<pid>)<br>(Processus <NomProgramme> régénéré (<pid>)) |

## Processus contrôlé arrêté

L'événement ProcessStop est envoyé lorsqu'un processus est arrêté. La gravité est définie sur 5 si le processus a été configuré pour se régénérer de façon dynamique (par exemple lorsque son arrêt n'était pas prévu). La gravité est définie sur 1 si le processus a été configuré pour ne s'exécuter qu'une seule fois.

| Balise | Valeur |
|---|---|
| Gravité | 1/5 |
| Nom de l'événement | ProcessStop (ProcessusArrêté) |

| | |
|---|---|
| Ressource | Watchdog |
| Sous-ressource | Process (Processus) |
| Message | Process <ProgramName> exited with code <exit_code> (Processus <NomProgramme> quitté avec le code <code_fermeture>) |

### Processus Watchdog démarré

Lorsque le processus Watchdog démarre, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | ProcessStart (ProcessusDémarré) |
| Ressource | Watchdog |
| Sous-ressource | Watchdog |
| Message | Service WatchDog en cours de démarrage |

### Processus Watchdog arrêté

Lorsque le processus Watchdog est arrêté, l'événement interne suivant est généré.

| Balise | Valeur |
|---|---|
| Gravité | 5 |
| Nom de l'événement | ProcessStop (ProcessusArrêté) |
| Ressource | Watchdog |
| Sous-ressource | Watchdog |
| Message | WatchDog Service Ended (Service WatchDog terminé) |

## Moteur/Gestionnaire des collecteurs

### Port démarré

Le Gestionnaire des collecteurs envoie l'événement PortStart lorsqu'un port est démarré.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | PortStart (PortDémarré) |
| Ressource | AgentManager (GestionnaireAgents) |
| Sous-ressource | AgentManager (GestionnaireAgents) |
| Message | Processing started for port_<port id> (Traitement démarré pour le port_<ID port>) |

### Port arrêté

Le Gestionnaire des collecteurs envoie l'événement PortStop lorsqu'un port est arrêté.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | PortStop (PortArrêté) |
| Ressource | AgentManager (GestionnaireAgents) |

| | |
|---|---|
| Sous-ressource | AgentManager (GestionnaireAgents) |
| Message | Processing stopped for port_<port id><br>(Traitement arrêté pour le port_<ID port>) |

### Processus persistant interrompu

Le Moteur du collecteur envoie l'événement PersistentProcessDied lorsque le connecteur de processus persistant détecte que son processus contrôlé a été interrompu.

| Balise | Valeur |
|---|---|
| Gravité | 5 |
| Nom de l'événement | PersistentProcessDied<br>(ProcessusPersistantInterrompu) |
| Ressource | AgentManager (GestionnaireAgents) |
| Sous-ressource | AgentManager (GestionnaireAgents) |
| Message | Persistent Process on port <port id> has died.<br>(Processus persistant sur le port <ID port><br>a été interrompu.) |

### Processus persistant redémarré

Le Moteur du collecteur envoie l'événement PersistentProcessRestarted lorsque le connecteur de processus persistant est en mesure de redémarrer le processus contrôlé interrompu.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | PersistentProcessRestarted<br>(ProcessusPersistantRedémarré) |
| Ressource | AgentManager (GestionnaireAgents) |
| Sous-ressource | AgentManager (GestionnaireAgents) |
| Message | Persistent Process on port <ID port> has restarted.<br>(Processus persistant sur le port <ID port><br>a redémarré.) |

## Service d'événements

### Dépendance cyclique

Le Service d'événements envoie l'événement CyclicalDependency lorsqu'il détecte un cycle dans la définition d'événement (dans les dépendances entre balises émanant d'assignations référentielles). Vérifiez la configuration d'événements dans le Gestionnaire de données Sentinel et résolvez la dépendance.

| Balise | Valeur |
|---|---|
| Gravité | 5 |
| Nom de l'événement | CyclicalDependency (DépendanceCyclique) |
| Ressource | EventService (ServiceÉvénements) |

| | |
|---|---|
| Sous-ressource | ObjectAttrInfos (InfosAttrObjet) |
| Message | Cyclical dependency detected in event transformations. Check event configuration. (Dépendance Cyclique détectée dans les transformations d'événements. Vérifiez la configuration des événements.) |

# Vues actives

## Vue active créée

DAS_Binary envoie l'événement RtChartCreated lorsqu'une vue active est créée.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | RtChartCreated (GraphiqueTRCréé) |
| Ressource | RealTimeSummaryService (ServiceRécapitulatifTempsRéel) |
| Sous-ressource | ChartManager (GestionnaireGraphiques) |
| Message | Creating new Active View with filter <filter> and attribute <attribute> for users with security filter <security filter>. Currently <n> Active View(s) Collecting. (Création d'une nouvelle vue active avec le filtre <filtre> et l'attribut <attribut> pour les utilisateurs doté du filtre de sécurité <filtre de sécurité>. Actuellement, <n> vue(s) active(s) recueille(nt) des données.) |

## Vue active atteinte

DAS_Binary envoie l'événement RtChartJoiningExistingData lorsqu'un utilisateur se connecte à une vue active existante.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | RtChartJoiningExistingData (GraphiqueTRAtteintDonnéesExistantes) |
| Ressource | RealTimeSummaryService (ServiceRécapitulatifTempsRéel) |
| Sous-ressource | ChartManager (GestionnaireGraphiques) |
| Message | Joining existing Active View with filter <filter> and attribute <attribute> for users with security filter <security filter>. Currently <n> Active View(s) Collecting. (Ajout de vue active existante doté du filtre <filtre> et de l'attribut <attribut> pour les utilisateurs se servant du filtre de sécurité <filtre de sécurité>. Actuellement, <n> vue(s) active(s) recueille(nt) des données.) |

## Vue active inactive supprimée

DAS_Binary envoie l'événement RtChartInactiveAndRemoved lorsqu'une vue active non permanente est supprimée en raison de son inactivité.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | RtChartInactiveAndRemoved (GraphiqueTRInactifSupprimé) |
| Ressource | RealTimeSummaryService (ServiceRécapitulatifTempsRéel) |
| Sous-ressource | ChartManager (GestionnaireGraphiques) |
| Message | Removed idle Active View with filter <filter> and attribute <attribute> for users with security filter <security filter>. Currently <n> Active View(s) Collecting. (Suppression de la vue active inactive dotée du filtre <filtre> et de l'attribut <attribut> pour les utilisateurs se servant du filtre de sécurité <filtre de sécurité>. Actuellement, <n> vue(s) active(s) recueille(nt) des données.) |

## Vue active permanente inactive supprimée

DAS_Binary envoie l'événement RtPermanentChartRemoved lorsqu'une vue active permanente est supprimée en raison de son inactivité. Les vues actives permanentes sont celles enregistrées dans les préférences utilisateur et qui expirent par défaut après plusieurs jours d'inactivité.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | RtPermanentChartRemoved (GraphiquePermanentTRSupprimé) |
| Ressource | RealTimeSummaryService (ServiceRécapitulatifTempsRéel) |
| Sous-ressource | ChartManager (GestionnaireGraphiques) |
| Message | Removed idle permanent Active View with filter <filter> and attribute <attribute> for users with security filter <security filter>. Currently <n> Active View(s) Collecting. (Suppression de la vue active permanente inactive dotée du filtre <filtre> et de l'attribut <attribut> pour les utilisateurs se servant du filtre de sécurité <filtre de sécurité>. Actuellement, <n> vue(s) active(s) recueille(nt) des données.) |

## Vue active désormais permanente

DAS_Binary envoie l'événement RtChartIsNowPermanent lorsqu'il détecte une vue active qui vient d'être rendue permanente. Comme cette vérification se produit à intervalle régulier, plusieurs minutes peuvent s'écouler entre le moment où la vue active est enregistrée dans les préférences et celui où l'événement est généré.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | RtChartIsNowPermanent (GraphiqueTRDésormaisPermanent) |
| Ressource | RealTimeSummaryService (ServiceRécapitulatifTempsRéel) |
| Sous-ressource | ChartManager (GestionnaireGraphiques) |
| Message | Active View with filter <filter> and attribute <attribute> for users with security filter <security filter> is now permanent. (La vue active dotée du filtre <filtre> et de l'attribut <attribut> pour les utilisateurs se servant du filtre de sécurité <filtre de sécurité> est désormais permanente.) |

## Vue active désormais non permanente

DAS_Binary envoie l'événement RtChartNotPermanent lorsqu'il détecte une vue active précédemment permanente qui n'est plus permanente. Comme cette vérification se produit à intervalle régulier, plusieurs minutes peuvent s'écouler entre le moment où la vue active est supprimée des préférences et celui où l'événement est généré.

| Balise | Valeur |
|---|---|
| Gravité | 1 |
| Nom de l'événement | RtChartNotPermanent |
| Ressource | RealTimeSummaryService (ServiceRécapitulatifTempsRéel) |
| Sous-ressource | ChartManager (GestionnaireGraphiques) |
| Message | Active View with filter <filter> and attribute <attribute> for users with security filter <security filter> is no longer permanent. (La vue active dotée du filtre <filtre> et de l'attribut <attribut> pour les utilisateurs se servant du filtre de sécurité <filtre de sécurité> n'est plus permanente.) |

## Résumé

| Nom de l'événement | Gravité | Source | Sous-ressource | Composant |
|---|---|---|---|---|
| AuthenticationFailed | 4 | UserAuthentication | Authenticate | Authentication |
| NoSuchUser | 4 | UserAuthentication | Authenticate | Authentication |
| TooManyActiveUsers | 4 | UserAuthentication | Authenticate | Authentication |
| LockedUser | 4 | UserAuthentication | Authenticate | Authentication |
| UserLoggedOut | 1 | UserSessionManager | User | User Session |
| UserLoggedIn | 1 | UserSessionManager | User | User |
| UserLoggedIn | 1 | UserSessionManager | User | User |
| MoveArchiveFileFailed | 3 | *Nom DAS* | ArchiveFile | Event |
| InsertEventsFailed | 5 | EventSubSystem | Events | Event |
| OpenArchiveFileFailed | 3 | *Nom DAS* | ArchiveFile | Event |
| WriteArchiveFileFailed | 3 | *Nom DAS* | ArchiveFile | Event |
| SummaryUpdateFailure | 4 | Aggregation | Summary | Aggregation |
| InsertIntoOverflowPartition | 5 | EventSubSystem | Events | Event |
| EventInsertionIsBlocked | 4 | EventSubSystem | Events | Event |
| EventInsertionResumed | 2 | EventSubSystem | Events | Event |
| EventRouterIsRunning | 1 | AgentManager | EventRouter | EventRouter |
| EventRouterInitializing | 1 | AgentManager | EventRouter | EventRouter |
| EventRouterStopping | 2 | AgentManager | EventRouter | EventRouter |
| EventRouterTerminating | 2 | AgentManager | EventRouter | EventRouter |
| ErrorNoSuchMap | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| LoadingMapFromCache | 1 | MappingService | ReferentialDataObjectMap | Mapping |
| RefreshingMapFromServer | 1 | MappingService | ReferentialDataObjectMap | Mapping |
| TimeoutRefreshingMapData | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| ErrorRefreshingMapData | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| LoadedLargeMap | 0 | MappingService | ReferentialDataObjectMap | Mapping |
| LongTimeToLoadMap | 0 | MappingService | ReferentialDataObjectMap | Mapping |
| TimedoutWaitingForCallback | 2 | MappingService | ReferentialDataObjectMap | Mapping |

| Nom de l'événement | Gravité | Source | Sous-ressource | Composant |
|---|---|---|---|---|
| ErrorApplyingIncrementalUpdate | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| OutOfSyncDetected | 2 | MappingService | ReferentialDataObjectMap | Mapping |
| EngineRunning | 1 | CorrelationEngine | CorrelationEngine | |
| EngineStopped | 1 | CorrelationEngine | CorrelationEngine | |
| DeploymentStarted | 1 | CorrelationEngine | Deployment | |
| DeploymentStopped | 1 | CorrelationEngine | Deployment | |
| DeploymentModified | 1 | CorrelationEngine | Deployment | |
| ProcessStart | 1 | Watchdog | Process | |
| ProcessStop | 1/5 | Watchdog | Process | |
| ProcessStart | 1 | Watchdog | Watchdog | |
| ProcessStop | 5 | Watchdog | Watchdog | |
| PortStart | | AgentManager | AgentManager | |
| PortStop | | AgentManager | AgentManager | |
| PersistentProcessDied | 5 | AgentManager | AgentManager | |
| PersistentProcessRestarted | 1 | AgentManager | AgentManager | |
| SortDependencies | 5 | EventService | ObjectAttrInfo | EventService |
| DbSpaceReachedTimeThrshld | 0 | Database | Database | Event |
| DbSpaceReachedPercentThrshld | 0 | Database | Database | Event |
| DbSpaceVeryLow | 5 | Database | Database | Event |
| RtChartCreated | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartJoiningExistingData | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartInactiveAndRemoved | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartPermanentAndRemoved | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartIsNowPermanent | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartNotPermanent | 1 | RealTimeSummaryService | ChartManager | Active Views |