Novell® Sentinel™

5.1.3

7 juillet 2006

www.novell.com

Volume IV : GUIDE DE RÉFÉRENCE 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 et sans préavis.

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 préavis.

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 tiers

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

Avis juridique tiers

Sentinel 5 peut comprendre les technologies tiers 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 au système Enterprise Security Management System de Novell. 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 d'intégration de produits tiers de Sentinel™

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 Sentinel Wizard
- Balises META de Wizard et de Sentinel
- Autorisations utilisateur
- Moteur de corrélation Sentinel
- 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 Introduction au guide des références utilisateur de Sentinel™ 5

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

Le guide des références utilisateur de Sentinel contient des informations de référence sur les éléments suivants :

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

Ce guide suppose que vous êtes déjà familiarisé avec la sécurité de réseau, l'administration des bases de données et les systèmes d'exploitation UNIX.

Sommaire

Ce guide contient les chapitres suivants :

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 Sentinel

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™ 5
- Guide d'utilisation du composant Wizard de Sentinel™ 5
- Guide des références utilisateur de Sentinel™ 5
- Guide d'intégration de produits 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 24 heures sur 24, 7 jours sur 7, appelez le 800-858-4000

2 Langage de script de Wizard

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

Ce chapitre ainsi que le suivant vous expliquent comment créer des scripts à l'aide du langage de script de Sentinel Wizard. Les opérateurs des différentes chaînes et commandes d'analyse utilisées dans la génération des collecteurs sont abordés.

Ce chapitre porte sur les points suivants :

Chaînes de décision

Les chaînes font la distinction entre les majuscules et les minuscules.

Lors de l'interrogation des collecteurs, diverses informations sont recueillies dans le tampon de réception interne. Les chaînes de type décision indiquent qu'une décision sera prise concernant les données reçues et stockées dans la mémoire tampon interne. Ces chaînes donnent soit le résultat « true », soit le résultat « false ». En cas d'erreur de syntaxe ou si le champ Decide Type (Type de décision) n'est pas renseigné, la décision est « false ».

La chaîne de décision est évaluée uniquement lorsque Decide Type (Type de décision) est défini sur « chaîne » ou « données ».

Utilisation du pointeur Rx Buffer (tampon de réception)

Chaque port du composant Wizard possède son propre pointeur Rx Buffer. Le pointeur Rx Buffer pointe vers les octets de données du tampon de réception. Avant chaque évaluation de chaîne de décision, le pointeur est réinitialisé sur sa valeur d'origine (normalement zéro, à moins qu'il ne soit modifié par une décision ayant utilisé l'opérateur de recherche (:)).

- 0 ne pointe vers aucun octet dans le tampon de réception.
- 1 pointe vers le premier octet de données, 2 vers le deuxième octet de données, etc.

Format

Une chaîne de décision se présente sous la forme d'une séquence d'opérateurs logiques et d'expressions régulières.

Il n'est pas nécessaire que ces opérateurs logiques et de chaîne soient présents dans chacune des séquences. Voici quelques règles concernant leur utilisation :

- Les opérateurs logiques sont utilisés dans les expressions booléennes (true ou false) au sein de la chaîne de décision et sont évalués dans l'ordre de priorité suivant :
  ```
  ~ Non
  & Et
  ```

- Un opérateur de chaîne indique une chaîne de caractères à rechercher dans le tampon de réception. Il permet d'effectuer une recherche octet par octet à partir de la position du pointeur Rx Buffer.

REMARQUE : le champ Decide Type (Type de décision) étant tronqué au niveau du dernier caractère imprimable, vous devez utiliser le code hexadécimal équivalent à un espace. L'opérateur « : » ne peut être employé avec l'opérateur NULL.

Paramètres

Pour spécifier un paramètre dans une chaîne de décision, il vous faut le placer entre accolades ({ }). Une fois le script créé, le nom du paramètre et les accolades sont remplacés par la valeur du paramètre.

Si le nom du paramètre spécifié ne figure pas dans le fichier des paramètres utilisé par le script, son expression et les accolades demeurent dans les données de la chaîne de décision.

Les expressions de nom de paramètre peuvent apparaître à tout endroit de la chaîne de décision, mais ne peuvent en aucun cas faire l'objet d'imbrications (c'est-à-dire contenir en leur sein une autre expression de nom de paramètre).

Hiérarchie des opérations dans une chaîne de décision

Toutes les opérations d'une chaîne de décision retournent soit « true » (1), soit « false » (0). Elles sont toujours réalisées dans l'ordre défini par la syntaxe de l'opérateur logique.

- Lorsque la chaîne comporte plusieurs opérations, celles-ci sont évaluées de gauche à droite.
- Lorsqu'elle comprend des parenthèses, l'opérateur logique au sein de chaque ensemble de parenthèses est évalué en premier.
- Les opérations logiques à être ensuite évaluées sont « non » (~) et « et » (&).

Un ordre bien précis des opérations est également respecté avec les opérateurs de chaîne :

- Le pointeur Rx Buffer réinitialisé est évalué en premier.
- Tous les autres caractères de syntaxe présentent la même priorité et sont évalués de gauche à droite.

Règles relatives au pointeur du tampon de réception

Les règles suivantes régissent la valeur du pointeur du tampon de réception :

- Lorsque la recherche d'une chaîne de caractères aboutit, le résultat est « true » et le pointeur se positionne au niveau du premier octet de la chaîne ainsi trouvée.

  Chaîne de décision : DE

```
 A BCDE F GH
^
 A BCDE F GH
      ^
```

- Lorsque la recherche d'une chaîne de caractères échoue, le résultat est « false » et le pointeur retourne à sa valeur d'origine.

Chaîne de décision : DEJ

```
 A BCDE F GH
^
 A BCDE F GH
^
```

Vérification d'un tampon de réception vide

Pour vérifier que le tampon de réception est vide, utilisez la chaîne de décision suivante :

```
NULL
```

Exemples d'évaluations de chaînes de décision et de résultats

Chaînes alphanumériques

Le tableau suivant répertorie des chaînes alphanumériques associées à un exemple de tampon de réception :

```
ABCDEFGHIJKLMNO (saut de ligne) YZ<[&
```

Chaîne de décision	Expression logique	Résultat
A	1	1
P	0	0
\41\(code hexadécimal du caractère A)	1	1
AB	1	1
\4142\(code hexadécimal des caractères AB)	1	1
ABD	0	0
A&B	1 & 1	1
A&P	1 & 0	0
A+P	1 + 0	1
A\42\(code hexadécimal du caractère B)	1	1
A&BC	1 & 1	1
DEF&ABC	1 & 0	0
ABC&DEF	1 & 1	1
ABC&BCD	1 & 1	1
ABC&ABC	1 & 0	0
\OA\(code hexadécimal du saut de ligne)	1	1
NULL *	0	0

Si la recherche ne trouve aucun caractère dans le tampon de réception, le résultat est TRUE.

Chaînes hexadécimales

Le tableau suivant répertorie des chaînes hexadécimales associées à un exemple de tampon de réception (HEX) :

```
02 0A 10 FF 1F 2E 3C 03
```

Chaîne de décision	Expression logique	Résultat
\020A\&\FF\	1 & 1	1
\02\	0	0
\02\&\03\	1 & 1	1
\03\&\02\	1 & 0	0

Expressions régulières

Les expressions régulières sont des modèles créés à l'aide de caractères spéciaux et de séquences de caractères.

Sentinel utilise une bibliothèque d'expressions régulières compatible avec la norme POSIX (Portable Operating System Interface for UNIX). POSIX est un ensemble de normes IEEE et ISO qui garantit la compatibilité entre les systèmes d'exploitation POSIX englobant la plupart des variétés d'UNIX.

Récapitulatif des caractères spéciaux utilisés dans les expressions régulières

Le tableau suivant répertorie les caractères spéciaux susceptibles d'être utilisés dans les expressions régulières pour les fonctions SEARCH et REPLACE.

Caractère	Utilisation/Exemple
\	Indique que le caractère qui suit est un caractère spécial. n correspond au caractère « n ». La séquence \n correspond à un caractère saut de ligne ou nouvelle ligne (fin de ligne), mais pour que « \ » soit transmis via l'analyseur, vous devez le faire précéder du caractère d'exception « / ». Ainsi, pour transmettre \n, vous devez utiliser /\n.
^	Indique le début du texte ou d'une ligne.
$	Indique la fin du texte ou d'une ligne.
*	Indique la répétition ou non du caractère le précédant. go* correspond soit à « g », soit à « goo ».
+	Indique la répétition du caractère le précédant. go* correspond à « goo », mais pas à « g ».
?	Indique la présence éventuelle du caractère le précédant. a?te? correspond aux lettres « te » du mot « eater ».
.	Représente un caractère unique, à l'exception du caractère nouvelle ligne (finde ligne).
x|y	Indique soit x, soit y. z|good? correspond à « goo » ou « good », ou encore « z ».
{n}	n est un entier non négatif. Indique une répétition exacte de n fois le caractère. e{3} ne correspond pas à « e » du mot « Ted », mais aux trois premiers « e » du mot « greeeeeed ».
{n,}	n est un entier non négatif. Indique une répétition d'au moins n fois le caractère. e{3,} ne correspond pas à « e » du mot « Ted » mais à tous les « e » du mot « greeeeeed ». e{1,} équivaut à e+.
{n,m}	m et n sont des entiers non négatifs. Indique une répétition d'au moins n fois et au plus m fois le caractère. e{1,3} correspond aux trois premiers « e » du mot « greeeeeed ».
[xyz]	Un jeu de caractères. Indique n'importe lequel des caractères entre crochets. [xyz] correspond à « y » dans le mot « play ».
[^xyz]	Un jeu de caractères négatif. Indique tout caractère non spécifié entre

	crochets. [^xyz]/ correspond à « v » dans « vain ».
[0-9]	Indique un chiffre.
[^0-9]	Indique un caractère autre qu'un chiffre.
[A-Za-z0-9_]	Indique tout type de caractère alphabétique, y compris le tiret de soulignement.
[^A-Za-z0-9_]	Indique tout caractère autre qu'alphabétique.
/n/	Indique n, où n est une valeur d'échappement décimale, hexadécimale ou octale. Permet l'intégration de codes ASCII dans les expressions régulières.

Caractères d'espacement dans les expressions régulières

Dans les expressions régulières, les caractères d'espacement consistent en un ou plusieurs espaces, soit n'importe lequel des caractères suivants :

Nom du symbole	**UCS**	**Description**
<tabulation>	<U0009>	TABULATION HORIZONTALE (HT)
<retour chariot>	<U000D>	RETOUR CHARIOT (CR)
<nouvelle ligne>	<U000A>	SAUT DE LIGNE (LF)
<tabulation verticale>	<U000B>	TABULATION VERTICALE (VT)
<saut de page>	<U000C>	SAUT DE PAGE (FF)
<espace>	<U0020>	ESPACE

Commandes d'analyse

Le langage d'analyse de Sentinel Wizard est un langage orienté fonctions. La plupart des fonctions d'analyse vous permettent de manipuler les variables de Wizard et leur contenu. Le langage d'analyse de Wizard prend en charge quatre types de variables :

- les entiers (le nom de la variable commence par un i) ;
- les variables flottantes (le nom de la variable commence par un f) ;
- les chaînes de longueur variable (le nom de la variable commence par une lettre autre que i ou f) ;
- les tableaux de variables (le nom de la variable se termine par [ ]). Ces derniers peuvent être des tableaux d'entiers, de valeurs flottantes ou de chaînes.

Il s'agit de variables locales sur chaque port du composant Wizard qui ne sont pas partagées avec les autres ports de Wizard. Les commandes d'analyse vous permettent de copier les données du tampon de réception dans les variables chaînes.

Le tampon de réception contient toutes les données reçues depuis le processus, le fichier, le port de socket ou le port de communication du composant Wizard.

Pour contrôler la longueur des octets à copier ainsi que la position à partir de laquelle copier les octets, vous pouvez vous servir des commandes d'analyse suivantes :

- SEARCH()
- SKIP()
- SKIPWORD()
- NEGSEARCH()
- RESET()
- COPY()

Vous pouvez ajouter les données du tampon de réception à une variable chaîne à l'aide de la commande APPEND(). Le langage d'analyse de Wizard vous permet en outre de copier ou d'ajouter des données d'une variable chaîne à une autre.

Types de données simples

number

Les numéraux peuvent être uniquement précédés d'un signe + ou - dans le cadre des commandes SKIP, SKIPWORD et SET. Par exemple :

```
0, 10, 2.5
```

ivar (variables entières)

Les variables de type entier désignent des nombres de 32 bits signés. Le nom de la variable doit commencer par un I ou un i. Exemple :

```
i_count, I_severity, i, i[55], i[index]
```

La variable entière, i[55], représente le 55ème index du tableau des entiers, i[]. L'index d'un tableau peut également être une variable entière.

fvar (variables flottantes)

Les variables flottantes sont des nombres à virgule flottante de 32 bits. Le nom de la variable doit commencer par un F ou un f. Exemple :

```
f_rate, F_queue, f, f[1], f[index]
```

svar (variables chaînes)

Les variables chaînes contiennent des chaînes de longueur variable. Elles ne peuvent en aucun cas commencer par les lettres I, i, F ou f. Exemple :

```
resource, date, _message, string[1000], string[i_sev]
```

array (tableaux de variables)

Les tableaux de variables peuvent contenir des variables de type ivar, fvar et svar. Par exemple :

```
i_bits[], F_values[], s_resources[]
```

Les tableaux peuvent être indexés à l'aide de tout index numérique sans qu'il y ait perte d'espace mémoire. L'accès à ivar[1000] ne signifie pas que de la mémoire est allouée pour 1 000 variables de type entier.

Le traitement d'une variable de tableau indexé est identique à celui de tout autre variable (ivar, svar et fvar).

Par exemple, la syntaxe de la commande POPUP suivante est correcte :

```
POPUP(xterm_display[4], data[i_count])
```

Données entre guillemets

Les données entre guillemets sont analysées de la manière suivante :

- /=Caractère d'exception : inclut l'octet qui suit le signe / quelle qu'en soit la signification ; pour utiliser un caractère spécial dans la chaîne, vous devez le faire précéder du signe /. Par exemple, corp/\router est utilisé pour corp\router.
- \xx x xx\=Données hexadécimales (un ou deux caractères par octet) : \0ad\, \0a0d\, \a d\,\0a 0d\ et \0a d\ ont tous pour signification saut de ligne/retour chariot.

Tous les autres caractères doivent être directement spécifiés.

Types de données agrégées dérivées

Le tableau ci-dessous répertorie les types de données agrégées dérivées :

Type	Description
tous	number, ivar, fvar, svar, quotes
numérique	number, ivar, fvar, ivar[index], fvar[index]
chaîne	svar, svar[index], quotes
chaîne	ivar, fvar, svar, ivar[index], fvar[index], svar[index]
variable numérique (numvar)	ivar, fvar, ivar[index], fvar[index]
tableau	ivar[], fvar[], svar[]
tableau de variables numériques	ivar[], fvar[]
tableau de variables chaînes	svar[]

Règles spéciales sur les variables

Voici quelques règles spéciales relatives aux variables.

- Les noms de variables font la distinction entre les majuscules et les minuscules.
- Lorsqu'une variable numérique (numvar) est utilisée pour la première fois, elle est définie sur zéro, sauf lorsque sa valeur est déjà définie.
- Lorsqu'une variable svar est utilisée pour la première fois, elle est définie sur null (""), sauf lorsque sa valeur est déjà définie.
- Un tableau indexé est traité de la même façon que toute autre variable du même type, ivar, svar ou fvar.
- Pour ajouter des marques de commentaires à une ou plusieurs commandes d'analyse ou au sein du texte d'analyse, placez-les entre /* */.

Par exemple :

```
/* ceci est un commentaire */
/* il s'agit de commandes d'analyse commentées
COPY(s: "test")
DISPLAY()
*/
```

3 Commandes d'analyse de Wizard

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

Ce chapitre répertorie dans l'ordre alphabétique les commandes d'analyse de Sentinel Wizard utilisées dans le cadre de la génération des collecteurs. Le tableau ci-dessous liste les commandes d'analyse par fonction.

Fonction	Commande d'analyse
Interaction avec la base de données	DBCLOSE DBDELETE DBGETROW DBINSERT DBOPEN DBSELECT
Débogage	BREAKPOINT DISPLAY POPUP
Interaction avec les fichiers	FILEA FILEL FILER FILEW

Opérations logiques	COMPARE
	ELSE
	ENDFOR
	ENDIF
	ENDWHILE
	FOR
	IF
	LOOKUP
	WHILE

Interaction avec le réseau	SOCKETW
Notification	ALERT CLEARTAGS CONSTANTTAGS EVENT INDICATOR PAUSE

Fonction	Commande d'analyse
Manipulation des données brutes	BITFIELD BYTEFIELD CONVERT CRC DECODE DECODEMIME ENCODE ENDFOR HEXTONUM NUMTOHEX SETBYTES STRIP STRIP ou STRIP-ASCII-RANGE
Manipulation des chaînes	APPEND COPY COPY-FROM-RX-BUFF-UNTIL-SEARCH COPY-FROM-RX-BUFF COPY-FROM-STRING-TO-STRING-UNTIL-SEARCH COPY-STRING-TO-STRING LENGTH ou LENGTH-OPTION2 LENGTH ou LENGTH-OPTION2 NEGSEARCH PARSER_ATTACHVARIABLE PARSER_CREATEBASIC PARSER_NEXT PARSER_PARSESTRING PRINTF REGEXPREPLACE REGEXPSEARCH REGEXPSEARCH_EXPLICIT REGEXPSEARCH REPLACE SEARCH SKIP SKIPWORD STONUM TOKENIZE TOLOWER TOUPPER TOKENIZE TRANSLATE
Utilitaire	DATE DATETIME PAUSE SHELL TBOSSETCOMMAND TBOSSETREQUEST TIME

Fonction	Commande d'analyse
Traitement des variables	CLEAR DELETE GETCONFIG GETENV INC RESET RXBUFF SET SETCONFIG
Analyse de la vulnérabilité	INFO_CLEARTAGS INFO_CLOSE INFO_CONSTANTTAGS INFO_CREATE INFO_DUMP INFO_PUSH INFO_SEND INFO_SETTAG

Format des commandes et utilisation des tableaux

La syntaxe des commandes d'analyse utilise un certain nombre de symboles qui ont une signification particulière. Voici quelques exemples de ces symboles :

Exemple de symbole utilisé	Exemple de la signification du symbole
`[paramètre]`	Les crochets droits indiquent des paramètres facultatifs.
`<paramètre>`	Les crochets angulaires indiquent des paramètres obligatoires.
`a`	a doit être entré tel quel ici.
`a|b`	a ou b peut être utilisé tel quel, mais pas les deux.
`<élément> ::= <définition>`	L'élément peut être remplacé par la définition.

`<varList>`
où :
`<varList> ::= var [, <varList>]`
	Utilisé dans les définitions récursives pour décrire une liste de variables dont au moins une des variables est obligatoire.

`...`	La répétition du (des) paramètre(s) précédent(s) est autorisée.
`/`	La barre oblique est utilisée comme caractère d'échappement afin de permettre l'utilisation de caractères spéciaux, tels que la barre oblique inverse (\).

Les tableaux sont autorisés dans les expressions. Exemple :

Soit l'expression	Les expressions suivantes sont équivalentes
`SET(i_var = 2)`	`i_arr[3]`

`SET(i_arr[3]=2`	`i_arr[i_var]`
	`i_arr[1+2]`
	`i_arr[1+1_var]`
	`i_arr[i_arr[3]]`

Commandes

ALERT

La commande ALERT transmet les messages d'événement à Sentinel.

- Le premier paramètre obligatoire définit le nom de la ressource.
- Le deuxième paramètre obligatoire définit le texte du message relatif à l'événement.
- Le troisième paramètre obligatoire définit le degré de gravité de l'événement.
- La date et l'heure du message d'événement peuvent être définies en tant que paramètres facultatifs.
  - Le paramètre de date peut être utilisé seul.
  - Le paramètre de l'heure doit être associé au paramètre de date.

Format

```
ALERT(resource, message, iseverity)
```

ou

```
ALERT(resource, message, iseverity[, date[, time]])
```

Vous ne pouvez utiliser le paramètre de l'heure que s'il est associé à celui de la date.

REMARQUE : utilisez la commande STONUM pour convertir la chaîne « iseverity » en un entier.

Types de données

Argument	Type	Description
resource	chaîne (ENTRÉE)	Ressource, et éventuellement sous-ressource, auxquelles envoyer un événement (par exemple : `xterm:tcp_retransmits`).
chaîne du message	(ENTRÉE)	Texte du message relatif à l'événement.
iseverity	numérique (ENTRÉE)	Priorité du message d'événement représentée sous forme numérique (de 0 à 5). 0 = Informations 1 = Conseils 2 = Avertissement 3 = Mineure 4 = Majeure 5 = Critique

Argument	Type	Description
chaîne de date	(ENTRÉE) [FACULTATIF]	Définit la date du message d'événement au format MM-JJ-AAAA (par exemple : « 12-01-2002 ») (par défaut = date du jour).
chaîne de l'heure	(ENTRÉE) [FACULTATIF]	Définit l'heure du message d'événement au format HH:MM:SS (par exemple :« 15:14:34 ») (par défaut = l'heure actuelle) ; doit être associé au paramètre de date.

Exemple :

```
ALERT("xterm:tcp_retransmits", mesg_txt,ivar[3])
ALERT("router_subnet_15", msg_txt, "c")
ALERT(resource, "Server not responding", iseverity)
ALERT("Mux184:card1", "C1 not funct. properly.", 4)
ALERT("Firewall", "Connection lost to Firewall.", 5)
ALERT("CB5", "Channel Bank 5 being serviced", "Maint")
ALERT(resource, message, isev, thedate, thetime)
ALERT("Switch3", oos_msg, 5, "07-30-1997", "07:03:23")
```

APPEND

La commande APPEND permet d'ajouter des données du tampon de réception, d'une variable chaîne ou d'une chaîne entre guillemets à une variable chaîne. Les règles suivantes s'appliquent :

- Tous les paramètres de la commande APPEND sont facultatifs, à l'exception du paramètre de destination.
- La destination des données (variable chaîne) peut être spécifiée à l'aide des paramètres APPEND.
- Vous pouvez indiquer un décalage dans la source afin de contrôler précisément l'endroit où les données sources sont copiées.
- Vous pouvez préciser le nombre d'octets à ajouter à la variable de destination à l'aide du paramètre de longueur (ilen). À défaut, la longueur utilisée par défaut est celle des données sources.
- La longueur peut être spécifiée à l'aide d'un paramètre numérique ou d'une chaîne.
- Si vous faites appel à une chaîne, le paramètre source doit être le tampon de réception ou une variable svar.
- Si vous utilisez une chaîne comme paramètre de longueur, le moteur du collecteur ajoute les octets des données sources (en commençant à partir de la valeur de décalage) à la variable de destination, jusqu'au premier caractère (non inclus) de la chaîne (si cette dernière est trouvée, dans le cas contraire, aucun octet n'est ajouté).
- Si les paramètres de décalage ou de longueur spécifiés se situent hors de la plage de la variable source, le plus grand nombre possible d'octets est ajouté, jusqu'à la position de fin des données sources.
- Si le décalage est supérieur ou égal à la longueur des données sources, aucun octet n'est ajouté à la variable de destination. Si aucun décalage n'est spécifié, sa valeur par défaut est zéro.

Format

```
APPEND(<dest>: [source] [, [search] [, [ilen] [,
[ioffset] ]]])
APPEND(<dest>: [source] [, [ilen] [, [ioffset] ]])
APPEND(<dest>: [ilen] [, [offset]])
```

Type de données

Argument	Type	Description
dest	svar (SORTIE)	Variable chaîne à laquelle sont ajoutés les octets.
source	chaîne (ENTRÉE) [FACULTATIF] ou svar	Chaîne contenant les octets à ajouter à la chaîne de destination. (Par défaut = tampon de réception) Si le paramètre de recherche est utilisé.
search	chaîne (ENTRÉE) [FACULTATIF]	Chaîne signifiant : copier jusqu'aux octets à rechercher dans la chaîne source.
ilen	numérique (ENTRÉE) [FACULTATIF]	Nombre d'octets à ajouter de la chaîne source à la chaîne de destination.
ioffset	numérique (ENTRÉE) [FACULTATIF]	Décalage dans la chaîne source à partir duquel commencer l'ajout des données.

Dans les exemples suivants, des octets du tampon de réception sont ajoutés à une variable svar de destination (dest). La position du pointeur Rx Buffer est ajoutée à la valeur de décalage pour indiquer la première position des données à ajouter. Cette position est signalée par le symbole « ^ ».

```
APPEND(svar:ilen)
APPEND(svar:3)
APPEND(svar:,ioffset)
APPEND(source:ilen,ioffset)
APPEND(svar: 10, 12)
```

L'exemple ci-dessus se base sur les hypothèses suivantes.

```
rxbuff="receive buffer"
^ (position du pointeur Rx Buffer)
dest="A destination string"
source="A source string"
ilen=3
ioffset=3
```

Entrez ce qui suit :

```
APPEND(dest:)
```

Résultat :

```
dest = "A destination stringreceive buffer"
```

Ou, si vous avez entré :

```
APPEND(dest:ilen)
```

Résultat :

```
dest = "A destination stringrec"
```

Ou, si vous avez entré :

```
APPEND(dest:,ioffset)
```

Résultat :

```
dest = "A destination stringreceive buffer"
```

Dans les exemples suivants, des octets du tampon de réception sont ajoutés à une variable svar
de destination (dest), jusqu'à la chaîne de recherche (non incluse). Si la chaîne de recherche est introuvable dans le tampon de réception (après le pointeur Rx Buffer + position de décalage), aucun octet n'est ajouté.

Entrez ce qui suit :

```
APPEND(dest:,"buffer")
```

Résultat :

```
dest = "A destination stringreceive "
```

Entrez ce qui suit :

```
APPEND(dest:,"buffer", 9)
```

Résultat :

```
dest = "A destination string"
```

Dans les exemples suivants, une sous-chaîne du tampon de réception est ajoutée en considérant l'hypothèse suivante :

```
Rx Buffer = "Minor Alarm Firewall A"
```

Entrez ce qui suit :

```
COPY(message:"Resource Name is: ")
APPEND(message:,6)
```

Résultat :

```
message = "Resource Name is: Alarm Firewall A"
```

BITFIELD

La commande BITFIELD convertit les octets en bits. Elle convertit chaque octet d'une chaîne de longueur arbitraire en 8 bits (0 ou 1) en les plaçant dans un tableau d'entiers, un tableau de valeurs flottantes ou une chaîne.

> **ATTENTION :** la sortie étant 8 fois plus grande que l'entrée, la commande d'analyse bitfield peut monopoliser beaucoup de mémoire si vous ne l'utilisez pas correctement, par exemple, en utilisant des chaînes d'entrée contenant un nombre important d'octets.

Format

```
BITFIELD(s_bytes, dest_var)
```

Types de données

Argument	Type	Description
s_bytes	chaîne (ENTRÉE)	Nombre quelconque d'octets ASCII ou hexadécimaux contenu dans une chaîne.

Argument	Type	Description
dest_var	tableau de variables numériques (SORTIE)	Tableau d'entiers (définis sur 0 ou 1). Le nombre de bits équivaut au nombred'octets dans s_bytes multiplié par 8. Pour chaque ensemble de 8 bits, les bits sont placés dans l'ordre suivant : du bit le plus fort (MSB)au bit le plus faible (LSB). Exemple : idest_var[0] = MSB de l'octet 1 idest_var[1] = MSB suivant de l'octet 1 idest_var[2] = MSB suivant de l'octet 1 idest_var[3] = MSB suivant de l'octet 1 idest_var[4] = MSB suivant de l'octet 1 idest_var[5] = MSB suivant de l'octet 1 idest_var[6] = MSB suivant de l'octet 1 idest_var[7] = LSB de l'octet 1 idest_var[8] = MSB de l'octet 2 idest_var[9] = MSB suivant de l'octet 2 ... idest_var[n * 8 - 1] = LSB de l'octet n
	Ou svar (SORTIE)	Chaîne contenant un multiple de 8 octets où chaque octet représente un bit dans les octets en entrée. Les octets de cette chaîne sont toujours définis sur une valeur ASCII de 0 ou 1. Pour chaque ensemble de 8 bits consécutifs représentés dans chaque chaîne, les valeurs ASCII (des 0 et des 1) sont placées depuis le bit le plus fort (MSB) vers le bit le plus faible (LSB). Exemple : Si s_bytes = “\5AFE\” Alors, dest_var= "0101101011111110"

REMARQUE : le deuxième paramètre de la commande bitfield (`dest_var`) doit être une chaîne (par exemple, `ivar[]` ou `fvar[]`).

Par exemple :

```
BITFIELD("\00\", f_bit_array[])
BITFIELD(s_bytes, i_bit_array[])
BITFIELD(s_byte, string_out)
BITFIELD("This will work", i_bit_array[])
BITFIELD("\563F\", string_out)
```

Dans l'exemple suivant, la chaîne sbyte est définie sur un octet hexadécimal et envoyée à deux reprises à la commande BITFIELD (une fois pour un tableau d'entiers et une autre fois pour une chaîne).

```
COPY(sbyte:"\AE\")
BITFIELD(sbyte, ibits[])
BITFIELD(sbyte, sbits)
```

Contenu des variables de sortie

```
ibits[0] = 1
ibits[1] = 0
ibits[2] = 1
ibits[3] = 0
ibits[4] = 1
ibits[5] = 1
ibits[6] = 1
ibits[7] = 0
sbits = "10101110"
```

BREAKPOINT

La commande BREAKPOINT interrompt l'exécution d'un script d'analyse. Lorsque le débogueur de script de Wizard est en cours d'exécution, la commande Breakpoint arrête l'analyseur dans l'attente d'une intervention de l'utilisateur. Pour reprendre le processus de débogage, dans le panneau du débogueur de Wizard, sélectionnez le bouton Go (aller à) ou Step (pas à pas).

Format

```
BREAKPOINT()
```

BYTEFIELD

La commande BYTEFIELD représente les octets en bit (0 ou 1) et place les octets dans une variable chaîne.

Il peut s'agir en entrée :

- d'une chaîne ;
- d'un tableau d'entiers ;
- d'un tableau de variables flottantes.

La sortie est toujours une variable chaîne.

Format

ATTENTION : si le premier paramètre est un tableau d'entiers ou de variables flottantes, n'utilisez pas de valeurs supérieures à 100 pour i_num_bytes. Le tableau serait en effet initialisé en fonction de ce nombre d'entrées (ce qui demanderait une mémoire considérable).

```
BYTEFIELD(source_var, s_bytes[, i_num_bytes])
```

REMARQUE : le premier paramètre de la commande BYTEFIELD (`source_var`) doit être svar, `ivar[]` ou `fvar[]`.

Types de données

Argument	Type	Description
source_var	tableau de variables numériques (ENTRÉE)	Tableau d'entiers (définis sur 0 ou 1). Le nombre de bits équivaut au nombre d'octets dans s_bytes fois 8. Pour chaque ensemble de 8 bits, les bits sont placés dans l'ordre suivant : du bit le plus fort (MSB) au bit le plus faible (LSB) (voir ci-dessous pour les exemples).
	svar (ENTRÉE)	Chaîne contenant un multiple de 8 octets où chaque octet représente un bit dans les octets en entrée. Les octets de cette chaîne doivent toujours être définis sur la valeur ASCII 0 ou 1. Pour chaque ensemble de 8 bits consécutifs représenté dans chaque chaîne, les valeurs ASCII (des 0 et des 1) doivent être placées du bit le plus fort vers le bit le plus faible. Par exemple : Si source_var = "0101101011111110", et i_num_bytes = 2, Alors, s_bytes = “\5AFE\”
s_bytes	chaîne (SORTIE)	Nombre quelconque d'octets ASCII ou hexadécimaux contenu dans une chaîne.
i_num_bytes	numérique (ENTRÉE) [FACULTATIF]	Nombre d'octets à placer dans _bytes. Cet argument étant facultatif, la valeur par défaut est 1, à moins que l'entrée ne soit de type CHAÎNE. Dans ce cas, la valeur par défaut correspond à la taille de la chaîne divisée par 8.

Voici des exemples pour le paramètre source_var :

```
ISOURCE_VAR[0] = MSB de l'octet 1
ISOURCE_VAR[1] = MSB suivant de l'octet 1
ISOURCE_VAR[2] = MSB suivant de l'octet 1
ISOURCE_VAR[3] = MSB suivant de l'octet 1
ISOURCE_VAR[4] = MSB suivant de l'octet 1
ISOURCE_VAR[5] = MSB suivant de l'octet 1
ISOURCE_VAR[6] = MSB suivant de l'octet 1
ISOURCE_VAR[7] = LSB de l'octet 1
ISOURCE_VAR[8] = MSB de l'octet 2
ISOURCE_VAR[9] = MSB suivant de l'octet 2
...
```

```
ISOURCE_VAR[n * 8 - 1] = LSB de l'octet n
```

Quelques exemples de commande BYTEFIELD :

```
BYTEFIELD(i_bit_array[], s_bytes)
BYTEFIELD(string_bits_in, s_bytes)
BYTEFIELD(f_bit_array[], string_bytes, 2)
BYTEFIELD(i_bit_array[], string_bytes, i_num_bytes)
```

Dans l'exemple suivant, la chaîne sbyte et le tableau d'entiers ivar sont définis sur la représentation sous forme de bits d'un octet hexadécimal et envoyés à deux reprises à la commande BYTEFIELD (une fois pour le tableau d'entiers et une autre fois pour la chaîne).

```
SET(ivar[0] = 0)
SET(ivar[1] = 0)
SET(ivar[2] = 0)
SET(ivar[3] = 0)
SET(ivar[4] = 1)
SET(ivar[5] = 1)
SET(ivar[6] = 1)
SET(ivar[7] = 1)
COPY(sbits:"11110000")
BYTEFIELD(ivar[], sbyte1)
BYTEFIELD(sbits, sbyte2, 1)
```

Contenu des variables de sortie :

```
sbyte1 = "\0F\"
sbyte2 = "\F0\"
```

CLEAR

La commande CLEAR tronque les variables chaînes en les ramenant à zéro octet, ou définit sur zéro les variables entières ou flottantes. Vous pouvez spécifier un maximum de 100 variables dans une seule commande CLEAR.

Format

```
CLEAR(<varlist>)
```

où :

```
varlist ::= var [, <varlist>]
Var ::= variable à effacer (fvar, ivar ou svar)
```

Nombre maximal de variables : 100

Types de données

Argument	Type	Description
var1	variable (ENTRÉE/ SORTIE)	Variable à effacer (fvar, ivar ou svar).
var2	variable (ENTRÉE/ SORTIE) [FACULTATIF]	Variable à effacer (fvar, ivar ou svar).
var3	variable (ENTRÉE/ SORTIE) [FACULTATIF]	Variable à effacer (fvar, ivar ou svar).
...	variable (ENTRÉE/ SORTIE) [FACULTATIF]	Autres variables à effacer (fvar, ivar ou svar).

Par exemple :

```
CLEAR(var1)
CLEAR(var1,var2)
CLEAR(var1,var2,var3)
CLEAR(svar[45])
CLEAR(imatrix[5][5])
CLEAR(ivar, fvar, i_len, data_string[i_var])
CLEAR(temp)
CLEAR(sdata[index_x][index_y])
CLEAR(f_bits[3], i_var_array[2])
CLEAR(i_counter, temp)
```

Dans les exemples suivants, les valeurs sont attribuées à des variables chaînes qui sont ensuite utilisées dans un message d'événement, puis les valeurs sont effacées.

```
COPY(res_var: "Firewall")
COPY(msg_var: "Firewall 116 Minor Alarm")
ALERT(res_var, msg_var, 4)
CLEAR(res_var, msg_var)
RÉSULTAT :
res_var = “”
```

```
msg_var = “”
```

CLEARTAGS

La commande CLEARTAGS efface toutes les variables réservées relatives aux événements et à l'heure/la date non protégées par la commande CONSTANTTAGS.

Vous devez utiliser cette commande lors de l'initialisation du collecteur (état 4 pour le modèle Sentinel standard) avant que les données entrées ne soient analysées dans les variables réservées.

La commande CLEARTAGS agit sur les variables réservées relatives aux événements et à la date/l'heure. Elle n'accepte aucun paramètre. Les variables chaînes sont définies sur une chaîne vide “”. Exemple :

```
s_EVT et s_Sec.
```

La variable entière i_Severity est définie sur zéro.

Format

```
CLEARTAGS ()
```

Par exemple :

```
SET(i_Severity = 3)
COPY(s_BM:"Base Message")
COPY(s_Example:"Test")
CLEARTAGS()
```

Résultat :

```
i_Severity = 0
s_BM = ""
s_Example = "Test"
```

REMARQUE : s_Example n'étant pas une variable réservée aux événements ou à la date/heure, elle n'est pas supprimée.

COMMENT

Cette commande s'utilise avec un seul argument facultatif : une chaîne. Elle permet d'entrer des commentaires dans le fichier de modèle du collecteur. Ce faisant, vous pouvez ajouter des commentaires directement dans l'éditeur plein écran sans avoir à basculer vers un éditeur de texte.

Format

```
/*[string]*/
```

Par exemple :

```
/* COLLECTOR INFORMATION
; ------------------------------------------------
Collector_Name:              Standard Template
Collector_Description:       Template to base new
Wizard Collectors on
Collector_Manufacturer:      N/A
Collector_Product/Version:   N/A
Collector_Version:           release 4.1
Collector_Date:              August 2003
; ------------------------------------------------
*/
```

COMPARE

La commande COMPARE examine deux arguments et définit une variable en fonction du résultat. Le résultat d'une comparaison impliquant un type chaîne ou numérique peut être stocké dans une variable. Si la variable est de type ivar, fvar ou chaîne, elle contiendra la valeur -1, 0 ou 1.

- -1 est utilisé lorsque arg1 est inférieur à arg2.
- 0 est utilisé lorsque arg1 est égal à arg2.
- 1 est utilisé lorsque arg1 est supérieur à arg2.

Format

```
COMPARE(arg1, arg2, dest)
```

Types de données

Argument	Type	Description
arg1	tous (ENTRÉE)	Données de comparaison 1. Doivent être de type chaîne ou numérique.
arg2	tous (ENTRÉE)	Données de comparaison 2. Doivent être du même type que les données de comparaison 1.
dest	variable (SORTIE)	Variable dans laquelle seront placés les résultats de la comparaison : svar = “-1”, “0” ou “1” ivar = -1, 0 ou 1 fvar = -1.0, 0.0 ou 1.0

REMARQUE : les arguments arg1 et arg2 doivent être tous les deux soit de type chaîne, soit de type numérique.

Par exemple :

```
COMPARE(i_counter, 0, temp)
COMPARE(sdata, "ALM", i_sdata_cmp_val)
COMPARE(i_counter, i_counter2, temp)
COMPARE(i_counter, i_counter2, i_result[i_counter])
```

Dans l'exemple suivant, le texte est comparé au contenu d'une variable chaîne, et le résultat de cette comparaison est stocké dans une variable entière. Si le texte diffère de la valeur de la variable chaîne, un événement est généré.

```
COMPARE(s_data_var, "ALARM", i_compare_var)
IF(i_compare_var = 0)
ALERT(res_var, "Major ALARM", 5)
ENDIF()
```

REMARQUE : les commandes IF( ), ELSE( ) et ENDIF( ) ont une fonction identique à la commande COMPARE, à cette exception près qu'elles permettent de comparer des nombres négatifs.

CONSTANTTAGS

La commande CONSTANTTAGS accepte un certain nombre de paramètres de noms de variables réservées (événement et date/heure). Le fait de déclarer une variable réservée constante évite qu'elle ne soit supprimée lors de l'utilisation de la commande CLEARTAGS.

À titre d'exemple, la variable s_PN, qui contient le nom de produit actuellement traité par le collecteur, fait partie de ces variables réservées. La variable s_PN doit être déclarée constante et définie une fois lors de la configuration du collecteur.

Vous devez utiliser cette commande lors de la configuration du collecteur (état 1 pour le modèle standard 4.1) pour les variables réservées qui doivent rester constantes lors du traitement des événements par le collecteur.

La commande CONSTANTTAGS agit sur les variables réservées relatives aux événements et à la date/l'heure.

Format

```
CONSTANTTAGS (<reserved_variable> [, ...])
```

Types de données

Argument	Type	Description
reserved_variable		Liste des variables réservées à définir comme constantes de sorte qu'elles ne soient pas supprimées par la commande CLEARTAGS.

Par exemple :

```
COPY(s_PN:"PN")
COPY(s_ST:"ST")
COPY(s_BM:"BM")
CONSTANTTAGS(s_PN,s_ST)
CLEARTAGS()
```

Résultat :

```
s_PN = "PN"
s_ST = "ST"
s_BM = ""
```

Sur les trois variables réservées relatives aux événements, s_BM n'ayant pas été protégée de la suppression par CLEARTAGS à l'aide de la commande CONSTANTTAGS, elle a donc été supprimée.

CONVERT

La commande CONVERT transforme une chaîne d'entrée de type binaire, octal, décimal, hexadécimal ou brut en une variable chaîne de sortie de type binaire, octal, décimal, hexadécimal ou brut.

Format

```
CONVERT(string_in, type_in, svar_out, type_out)
```

Types de données

Argument	Type	Description
string_in	chaîne (ENTRÉE)	Chaîne d'entrée à convertir.
type_in	Liste de choix chaîne variable chaîne (ENTRÉE)	Type de la chaîne d'entrée. (string_in) : Binaire = “B” ou “b” Octal = “O” ou “o” Décimal = “D” ou “d” Hexadécimal = “H” ou “h” Brut = “R” ou “r”
svar_out	svar (SORTIE)	Variable chaîne contenant les données de chaîne converties.
type_out	Liste de choix chaîne variable chaîne (ENTRÉE)	Type dans lequel convertir les données (la chaîne convertie sera placée dans svar_out) : Binaire = “B” ou “b” Octal = “O” ou “o” Décimal = “D” ou “d” Hexadécimal = “H” ou “h” Brut = “R” ou “r”

Par exemple :

```
CONVERT("10101010", "b", shex, "h")
CONVERT(sdata, "B", sraw, "r")
CONVERT("2356", "d", soctal, "o")
CONVERT("\3A\", "r", sbinary, "b")
CONVERT("2A3E", "h", sraw, "r")
CONVERT(data, "r", sdecimal, "d")
CONVERT(data, "o", shex, "H")
```

Dans l'exemple suivant, la commande CONVERT permet de réaliser diverses conversions.

```
CONVERT("\0afe\", "R", sdecimal, "D")
CONVERT("63", "d", sbinary, "b")
CONVERT("63", "b", shex, "h")
CONVERT("63", "d", soctal, "o")
CONVERT("1101010111110101", "b", sraw, "r")
```

Contenu des variables de sortie :

```
sdecimal = "2814"
sbinary = "00111111"
shex = "3F"
soctal = "077"
sraw = "\d5 f5\"
```

COPY

La commande COPY permet de dupliquer les données issues du tampon de réception ou d'une chaîne source et de les placer dans une variable chaîne, ou de copier une chaîne entre guillemets dans une variable chaîne. Le pointeur Rx Buffer n'est pas modifié lorsque vous utilisez cette commande.

La destination des données (svar) doit être spécifiée à l'aide des paramètres de la commande COPY.

> **REMARQUE :** au sein de l'éditeur plein écran du Générateur de collecteurs, les commandes COPY, COPY-FROM-RX-BUFF-UNTIL-SEARCH, COPY-FROM-RX-BUFF, COPY-FROM-STRING-TO-STRING-UNTIL-SEARCH et COPY-STRING-TO-STRING sont répertoriées en tant que commandes distinctes. Il s'agit en fait d'une seule et même commande. Elles ne font que décrire différentes variantes de la commande. Si vous deviez utiliser une variante de la commande COPY dans l'éditeur de texte, vous entreriez COPY.

Lors de l'utilisation de cette commande :

- Spécifiez un décalage dans la source afin de contrôler précisément l'endroit où les données sources sont copiées.
- Vous pouvez préciser le nombre d'octets à copier dans la variable de destination à l'aide du paramètre de longueur (ilen). La longueur utilisée par défaut est celle des données sources.
- La longueur peut être spécifiée à l'aide d'un paramètre numérique ou d'une chaîne. Si vous utilisez une chaîne, le moteur du collecteur copie les octets des données sources (en commençant à partir de la valeur de décalage) dans la variable de destination, jusqu'au premier caractère (non inclus) de la chaîne (si cette dernière est trouvée, sinon, aucun octet n'est copié).
- Si les paramètres de décalage (ioffset) ou de longueur (ilen) spécifiés se situent hors de la plage de la variable source, le plus grand nombre possible d'octets est copié, jusqu'à la position de fin des données sources.

  Si le décalage est supérieur ou égal à la longueur des données sources, aucun octet n'est copié dans la variable de destination.

  Si aucun décalage n'est indiqué, sa valeur par défaut est zéro.

Format

```
COPY(<dest>: [source] [, [search] [, [ilen] [,
[ioffset] ]]])
COPY(<dest>: [source] [, [ilen] [, [ioffset] ]])
COPY(<dest>: [ilen] [, [offset]])
```

Types de données

Argument	Type	Description
dest	svar (SORTIE)	Variable chaîne dans laquelle sont copiés les octets.
source string	(ENTRÉE) [FACULTATIF] Ou svar	Chaîne d'où sont issus les octets à copier (par défaut = tampon de réception). Si le paramètre de recherche est utilisé.
search	chaîne (ENTRÉE) [FACULTATIF]	Chaîne signifiant : copier jusqu'aux octets à rechercher dans la chaîne source.
ilen	numérique (ENTRÉE) [FACULTATIF]	Nombre d'octets à copier de la chaîne source dans la chaîne de destination.

Argument	Type	Description
ioffset	numérique (ENTRÉE) [FACULTATIF]	Décalage dans la source à partir duquel débuter la copie des données ; copie tous les caractères depuis le tampon de réception vers le tampon de transmission.

Dans les exemples suivants, des octets du tampon de réception sont copiés dans une variable svar
de destination (dest). La position du pointeur Rx Buffer est ajoutée à la valeur de décalage pour indiquer la position de début des données à copier. Cette position est signalée par le symbole « ^ ».

Les hypothèses sont les suivantes :

```
rxbuff="receive buffer"
^ (position du pointeur Rx Buffer)
dest=""
source="A source string"
ilen=3
ioffset=3
```

Commande	Résultat
COPY(dest:)	dest = "receive buffer"
COPY(dest:5)	dest = "recei"
COPY(dest:,5)	dest = "ve buffer"

Dans les exemples suivants, des octets d'une chaîne source sont copiés dans une variable svar de destination (dest).

Commande	Résultat
COPY(dest:source)	dest = "A source string"
COPY(dest:source,5)	dest = "A sou"
COPY(dest:source,5,6)	dest = "ce st"

Dans les exemples suivants, des octets du tampon de réception sont copiés dans une variable chaîne, jusqu'à la chaîne de recherche (non incluse). Si la chaîne de recherche est introuvable dans le tampon de réception (après le pointeur Rx Buffer + position de décalage), aucun octet n'est copié.

REMARQUE : en cas de remplacement hexadécimal, \0000\ termine une chaîne. Ainsi, « xxxx\0000\yyyy » devient « xxxx ».

Dans les exemples suivants, des octets du tampon de réception sont copiés dans une variable svar de destination (dest), jusqu'à la chaîne de recherche (non incluse). Si la chaîne de recherche est introuvable dans le tampon de réception (après le pointeur Rx Buffer + position de décalage), aucun octet n'est copié.

Commande	Résultat
COPY(dest:,"buffer")	dest = "receive"
COPY(dest:,"receive")	dest = ""

Dans les exemples suivants, des octets d'une chaîne source (obligatoirement une variable chaîne) sont copiés dans une variable chaîne de destination (dest), jusqu'à la chaîne de

recherche (non incluse). Si la chaîne de recherche est introuvable dans le tampon de réception (après le pointeur Rx Buffer + position de décalage), aucun octet n'est copié.

Commande	Résultat
`COPY(dest:source," string")`	`dest = "a source"`
`COPY(dest:source," .string")`	`dest = ""`

CRC

La commande CRC effectue
un contrôle de redondance cyclique dans une chaîne d'octets (hexadécimale
ou ASCII).

Format

```
CRC(source_data, dest_crc)
```

Type de données

Argument	Type	Description
source_data	chaîne (ENTRÉE)	Chaîne sur laquelle porte la commande CRC.
dest_crc	svar (SORTIE)	Variable chaîne dans laquelle le résultat CRC à 2 octets est stocké.

Par exemple :

Dans l'exemple suivant, la valeur CRC calculée est comparée à une valeur enregistrée. Si les deux valeurs CRC sont identiques, un message d'événement est généré.

```
CRC(svar, s_crc_var)
IF(s_crc_var = "\0A5F\")
EVENT(res, "Correct CRC generated", 0)
ENDIF()
```

REMARQUE : en cas de remplacement hexadécimal, \0000\ termine une chaîne. Ainsi, « xxxx\0000\yyyy » devient « xxxx ».

DATE

La commande DATE copie la date actuelle (au format MM-JJ-AAAA) dans une variable chaîne. Elle peut éventuellement copier le jour courant de la semaine dans une variable flottante, entière ou chaîne.

Format

```
DATE(date_string [, day_of_week] [, i_day_of_week]
[, f_day_of_week])
```

Type de données

Argument	Type	Description
date_string	svar	Variable chaîne dans laquelle la date sera stockée

Argument	Type	Description
	(SORTIE)	(par exemple, svar = “11-18-2002”).
day_of_week	svar (SORTIE) [FACULTATIF] ivar (SORTIE) [FACULTATIF] Ou fvar (SORTIE) [FACULTATIF]	(Facultatif) Variable chaîne dans laquelle le jour de la semaine sera stocké, sous la forme de son nom complet (par exemple, svar = samedi) (Facultatif) Variable entière ou flottante dans laquelle le jour de la semaine sera stocké, sous la forme de son nomcomplet = nombre : lundi = 1 mardi = 2 mercredi = 3 jeudi = 4 vendredi = 5 samedi = 6 dimanche = 7 (par exemple : lundi correspond à ivar = 1)

Par exemple :

Dans l'exemple suivant, la date système est comparée à une chaîne de date.
Si les deux dates sont identiques, un message d'événement est généré.

```
DATE(date_var, day_of_week)
IF(date_var = "11-18-2002")
ALERT(res, "Happy 23rd birthday!", 0)
ENDIF()
IF(day_of_week = "Saturday")
ALERT(res, "Time to go to the beach," 0)
ENDIF()
```

DATETIME

La commande DATETIME convertit la représentation sous forme d'entiers du nombre de secondes écoulées depuis le 1er janvier 1970 en variables chaînes de date et d'heure. Elle peut éventuellement copier le jour courant de la semaine dans une variable flottante, entière ou chaîne.

Format

```
DATETIME(itime_secs, svar_date, svar_time
[, day_of_week] [, i_day_of_week] [, f_day_of_week])
```

Types de données

Argument	Type	Description
itime_secs	numérique (ENTRÉE)	Nombre entier contenant le nombre de secondes écoulées depuis 1970.
svar_date	svar	Variable chaîne dans laquelle la date sera stockée

Argument	Type	Description
	(SORTIE)	(par exemple, 02-19-96).
svar_time	svar (SORTIE)	Variable chaîne dans laquelle l'heure sera stockée (par exemple, 15:14:33).
day_of_week	svar (SORTIE) [FACULTATIF] ivar (SORTIE) [FACULTATIF] Ou fvar (SORTIE) [FACULTATIF]	(Facultatif) Variable chaîne dans laquelle le jour de la semaine sera stocké, sous la forme de son nom complet (par exemple, svar = samedi) (Facultatif) Variable entière ou flottante dans laquelle le jour de la semaine sera stocké, sous la forme de son nom complet = nombre : lundi = 1 mardi = 2 mercredi = 3 jeudi = 4 vendredi = 5 samedi = 6 dimanche = 7 (par exemple : lundi correspond à ivar = 1)

Par exemple :

Dans l'exemple suivant, la commande DATETIME convertit le nombre de secondes écoulées depuis 1970 en chaînes d'heure et de date :

```
DATETIME(0, sdatevar, stimevar)
```

Dans l'exemple suivant, la commande DATETIME donne le jour de la semaine, ainsi que la date et l'heure :

```
DATETIME(946728000, sdate, stime, sday)
```

Contenu des variables de sortie :

```
sdatevar = "01-01-70"
stimevar = "00:00:00"
sdate = "01-01-2000"
stime = "12:00:00"
sday = "Saturday"
```

DBCLOSE

La commande DBCLOSE ferme la connexion à la base de données. Deux paramètres sont obligatoires :

- l'identificateur de base de données retourné par la commande DBOPEN un entier ou une variable entière) ;
- le statut de la fermeture (une variable entière ou une variable flottante). En cas de succès, un « 1 » est retourné.

Format

```
DBCLOSE(i_dbhandle, i_closestatus)
```

DBDELETE

La commande DBDELETE supprime des lignes de la table sélectionnée en fonction des critères de sélection. Quatre paramètres sont obligatoires :

- l'identificateur de base de données retourné par la commande DBOPEN (un entier ou une variable entière) ;
- le statut de la suppression (une variable entière ou une variable flottante). En cas de succès, le nombre de lignes supprimées est retourné, 0 inclus ;
- le nom de la table dans laquelle supprimer les lignes (une chaîne ou une variable chaîne) ;
- la clause where qui permet aux utilisateurs de filtrer les données indésirables en fonction d'un critère de sélection. Si cette clause n'est pas renseignée, la suppression porte sur toutes les lignes de la table.

Les codes d'erreur associés à la commande DBDELETE sont les suivants :

```
>0 Pas d'erreur
0 Aucune ligne supprimée
-1 Identificateur de base de données incorrect
```

Format

```
DBDELETE(i_dbhandle, i_deletestatus, "tablename",
"where clause")
```

Par exemple :

```
DBDELETE(i_dbhandle, i_deletestatus, "tablename")
DBDELETE(i_dbhandle, i_deletestatus, s_tablename,
"where clause")
```

DBGETROW

La commande DBGETROW s'utilise avec la commande DBSELECT. L'utilisateur doit commencer par obtenir une sélection, à l'aide de la commande DBSELECT, avant d'extraire les lignes à l'aide de la commande DBGETROW. Cette commande extrait la ligne disponible suivante d'une sélection, laissant un curseur actif de sorte qu'elle peut être appelée en boucle, extrayant la ligne suivante à chaque appel. Quatre paramètres sont obligatoires :

- l'identificateur de base de données retourné par la commande DBOPEN (un entier ou une variable entière) ;
- l'identificateur de la sélection (une chaîne ou une variable chaîne). Il s'agit du même identificateur que celui attribué dans la commande DBSELECT ;
- le statut de l'extraction (une variable entière ou une variable flottante). En cas de succès, un « 1 » est retourné ;
- le quatrième paramètre obligatoire et les paramètres facultatifs suivants sont les données de colonne retournées par la commande. Il peut s'agir de variables de chaîne, de variables flottantes ou entières. Les données de colonne dont le type diffère de celui du paramètre sont converties dans le type approprié, le cas échéant. Ainsi, si la table contient une colonne de type flottant, mais que le paramètre est de type chaîne, les données sont converties en chaîne. L'utilisateur peut inclure jusqu'à 48 paramètres de ce type.

REMARQUE : la commande s'exécute en tenant compte de la valeur moindre du nombre de paramètres définis et du nombre courant de colonnes contenues dans la base de données. Ainsi, si la base de données comporte 4 colonnes mais que vous indiquez 7 de ces paramètres, seuls les 4 premiers seront traités.

Les codes d'erreur associés à la commande DBGETROW sont les suivants :

```
1 Pas d'erreur
-1 Erreur lors de l'extraction de la ligne
```

Format

```
DBGETROW(i_dbhandle, "select1", i_selectstatus,
s_col1, s_col2, s_col3, ..., s_col48)
```

Par exemple :

```
DBGETROW(i_dbhandle, s_selecthandle, i_selectstatus,
s_col1, s_col2)
```

DBINSERT

La commande DBINSERT insère une ligne de données dans la base de données pour la table sélectionnée. Quatre paramètres sont obligatoires :

- l'identificateur de base de données retourné par la commande DBOPEN (un entier ou une variable entière) ;
- le statut de l'insertion (une variable entière ou une variable flottante). En cas de succès, un « 1 » est retourné ;
- le nom de la table dans laquelle insérer les données ;
- le quatrième paramètre obligatoire et les paramètres facultatifs suivants sont les données de colonne à insérer. Les colonnes peuvent être de n'importe quel type. L'utilisateur peut inclure jusqu'à 48 de ces paramètres.

La commande doit comporter le nombre exact de paramètres requis pour l'insertion d'une ligne de données. DBINSERT n'ajoute aucun enregistrement si une seule contrainte n'est pas respectée.

Les codes d'erreur associés à la commande DBINSERT sont les suivants :

```
1 Pas d'erreur
-1 Identificateur de la base de données incorrect /
aucune ligne insérée
-2 Impossible de créer la requête de données
-7 Erreur d'exécution SQL
-16 Erreur de syntaxe SQL
```

Format

```
DBINSERT(i_dbhandle, i_insertstatus, "theTableName",
"data1", "data2", ..., "data48")
```

Par exemple :

```
DBINSERT(i_dbhandle, i_insertstatus, s_theTableName,
"data1", I_data2, f_data3)
DBINSERT(i_dbhandle, i_insertstatus, "theTableName",
s_data1, "data2")
```

DBOPEN

La commande DBOPEN ouvre une connexion à la base de données prise en charge.

Pour le collecteur Microsoft Windows NT seulement : la commande DBOPEN ne fonctionne pas lorsque le nom de la base de données pointe vers un « lecteur assigné ». Le collecteur s'exécutant en tant que service, il s'exécute (habituellement) sous le compte « système ». Or ce compte ne dispose pas d'autorisations d'accès aux partages distants, notamment aux lecteurs assignés. Autrement dit, toute connexion à une base de données

(même via ODBC) sur un collecteur Windows doit s'effectuer avec une base de données entièrement locale.

Cinq paramètres sont obligatoires :

- Le premier paramètre obligatoire est le type de base de données. Vous pouvez sélectionner ce dernier dans une liste, ou via une chaîne ou une variable chaîne. La valeur acceptable pour ce paramètre est Oracle9i.
- Le deuxième paramètre obligatoire est le nom de la base de données à laquelle se connecter. Il peut s'agir d'une chaîne ou d'une variable chaîne.
- Le troisième paramètre obligatoire est le nom d'utilisateur de la base de données. Il peut s'agir d'une chaîne ou d'une variable chaîne. Ce champ peut contenir n'importe quel texte si aucun utilisateur n'a été configuré pour l'accès à la base de données.
- Le quatrième paramètre obligatoire est le mot de passe de l'utilisateur. Il peut s'agir d'une chaîne ou d'une variable chaîne. Ce champ peut contenir n'importe quel texte si aucun utilisateur n'a été configuré pour l'accès à la base de données.
- Le cinquième et dernier paramètre obligatoire est l'identificateur de base de données, retourné par cette commande dans une variable entière ou flottante. En cas de succès, cet identificateur est supérieur à 0.

Format

```
DBOPEN("oracle9i", "Database name", "username",
"password", i_dbhandle)
```

Par exemple :

```
DBOPEN(s_dbtype, s_dbname, s_username, s_password,
i_dbhandle)
DBOPEN(s_dbtype, "dbname", s_username, "password",
i_dbhandle)
```

DBSELECT

La commande DBSELECT s'utilise avec la commande DBGETROW. La commande DBSELECT rend actif un curseur de sélection dans la base de données. Cette opération prend un instantané des enregistrements actuels contenus dans la base de données répondant aux critères de sélection. Les enregistrements entrés après l'exécution de la commande DBSELECT ne figurent pas dans l'extraction. Pour qu'ils s'y trouvent, la sélection doit être mise à jour par l'exécution d'une autre commande DBSELECT.

Sept paramètres sont obligatoires :

- l'identificateur de base de données retourné par la commande DBOPEN (un entier ou une variable entière) ;
- le statut de la sélection (une variable entière ou une variable flottante). En casde succès, un « 1 » est retourné ;
- l'identificateur de la sélection (une chaîne ou une variable chaîne). Cet identificateur doit être unique si vous exécutez plusieurs commandes DBSELECT ;
- le nombre de lignes à ignorer après exécution de la sélection. Ce paramètre permet à l'utilisateur de positionner le pointeur de la commande DBGETROW

sur de nouvelles données et d'ignorer les anciennes. Il peut s'agir d'un entier ou d'une variable entière ;
- la table à partir de laquelle extraire les données (une chaîne ou une variable chaîne) ;
- la clause where qui permet aux utilisateurs de filtrer les données indésirables en fonction d'un critère de sélection. Si cette clause n'est pas renseignée, la sélection porte sur toutes les lignes de la table. Le format de la clause where est le suivant : where nom-colonne=’données’.
- les colonnes retournées par la commande DBSELECT. Si ce paramètre n'est pas renseigné, la sélection porte sur toutes les colonnes de la table.

Les codes d'erreur associés à la commande DBSELECT sont les suivants :

```
1 Pas d'erreur
-1 Identificateur de base de données incorrect
-2 Impossible de créer la requête de données
-3 Échec du paramètre d'autovalidation
-4 Erreur d'allocation mémoire
-5 Erreur de syntaxe SQL
-6 Erreur d'exécution SQL
```

Format

```
DBSELECT( i_dbhandle, i_selectstatus, "select1",
i_rows_to_skip, "f_atom"<, "where clause"><,
"col1<col2><...>">)
```

Par exemple :

```
DBSELECT(i_dbhandle, i_selectstatus, "select1",
i_rows_to_skip, "f_atom")
DBSELECT(i_dbhandle, i_selectstatus, s_select1, 23,
S_TABLENAME, s_whereclause)
DBSELECT(i_dbhandle, i_selectstatus, s_select1, 23,
S_TABLENAME, "where fname=’BOB’")
DBSELECT(i_dbhandle, i_selectstatus, s_select1, 23,
S_TABLENAME, "where fname=’BOB’", "FIRST, LAST,
ADDRESS")
```

DEC

La commande DEC décrémente les variables numériques de 1. Vous devez spécifier soit une variable ivar, soit une variable fvar.

Format

```
DEC(i_numvar)
```

Types de données

Argument	Type	Description
i_numvar	variable numérique (numvar) (ENTRÉE/ SORTIE)	Variable à décrémenter (ivar ou fvar).

Par exemple :

```
SET(icounter = 2)
DEC(icounter)
DEC(icounter)
```

Résultat :

```
icounter = 0
```

DECODE

La commande DECODE décode une chaîne qui avait fait l'objet d'un codage pour préserver l'identification d'un paquet. Cette commande distingue les octets à rechercher (ou caractères) des octets d'échappement (ou caractères) afin de supprimer ces derniers. Elle supprime chaque occurrence de chaîne d'échappement qui précède les octets trouvés.

Format

```
DECODE(data_decode, match, escape)
```

Types de données

Argument	Type	Description
data_decode	svar (ENTRÉE/ SORTIE)	Variable de données chaîne à décoder. Le résultat est replacé dans cette variable.
match	chaîne (ENTRÉE)	Chaîne des octets à chercher dans la variable chaîne data_decode.
escape	chaîne (ENTRÉE)	Chaîne d'échappement à supprimer de la variable chaîne data_decode.

Par exemple :

L'exemple suivant code une chaîne, la copie pour enregistrer la version codée, puis la décode avec les mêmes paramètres.

```
COPY(svar:"This is just a test of decode")
ENCODE(svar, " ", "\00\")
COPY(svar_encode:svar)
DECODE(svar, " ", "\00\")
```

Contenu des variables de sortie :

```
svar = "This is just a test of decode"
svar_encode = "This\00\ is\00\ just\00\ a\00\ test\00\
of\00\ decode"
```

DECODEMIME

La commande DECODEMIME permet à l'utilisateur de décoder une chaîne codée sur 64 bits ou une variable chaîne qui utilise un décodage sur 64 bits, et de stocker la chaîne décodée finale sous forme de variable chaîne. Si une erreur se produit lors du décodage, la chaîne de données finale est d'une longueur égale à zéro et l'argument Success de la variable numérique facultative est défini sur 0. Si le décodage fonctionne correctement, l'argument est défini sur 1.

Format

```
DECODEMIME(encoded_data, data, success)
```

Types de données

Argument	Type	Description
encoded_data	chaîne/variable chaîne(ENTRÉE)	Chaîne codée sur 64 bits nécessitant un décodage.
data	variable chaîne(SORTIE)	Données décodées finales.
success	variable entière/variable flottante(SORTIE) [FACULTATIF]	Variable définie sur 1 lorsque le décodage s'effectue correctement, et sur 0 en cas d'erreur.

Par exemple :

```
DECODEMIME("VGVzdGluZyBEYXRhIEVuY29kaW5n", s_data,
i_success)
```

Dans l'exemple ci-dessus, la commande DECODEMIME décode la chaîne entre guillemets doubles par un décodage sur 64 bits et stocke la chaîne décodée dans s_data. La variable S_data est renseignée de la manière suivante :

```
test encode64 command
```

À partir du moment où le décodage s'effectue correctement, la valeur 1 est assignée à la variable entière i_success.

Voir également la commande ENCODEMIME.

DELETE

La commande DELETE supprime les variables du système pour libérer la mémoire utilisée pour leur stockage (très utile pour les variables de chaîne).

Afin d'économiser de la mémoire, il est recommandé de supprimer les variables svar une fois que vous avez terminé. Vous pouvez spécifier un maximum de 100 variables dans une seule commande DELETE.

Format

```
DELETE(<varlist>)
```

où :

```
varlist ::= var [, <varlist>]
Var ::= variable à supprimer (fvar, ivar ou svar)
```

Nombre maximal de variables : 100

Types de données

Argument	Type	Description
var1	variable (ENTRÉE/ SORTIE)	Variable à supprimer (fvar, ivar ou svar).
var2	variable (ENTRÉE/ SORTIE) [FACULTATIF]	Variable à supprimer (fvar, ivar ou svar).
var3	variable (ENTRÉE/ SORTIE) [FACULTATIF]	Variable à supprimer (fvar, ivar ou svar).
...	variable (ENTRÉE/ SORTIE) [FACULTATIF]	Autres variables à supprimer (fvar, ivar ou svar).

Par exemple :

```
DELETE(ivar1)
DELETE(sdata, i_len, i_count, svar[22])
DELETE(imatrix3d[ix][iy][iz])
```

```
DELETE(f_array[i_count], svar[4], sdata)
DELETE(ichart[3][icount])
```

DISPLAY

La commande DISPLAY affiche les variables de script et leurs valeurs actuelles dans une fenêtre contextuelle.

Notez les points suivants :

- Utilisez la commande lors du débogage des scripts.
- Si vous transmettez une chaîne en tant que paramètre, son contenu s'affiche.
- Les chaînes contenant des données hexadécimales sont affichées au format hexadécimal (à savoir, chaîne="\0a 0d\").

Le programme tente dans un premier temps d'afficher la chaîne au format ASCII. Si elle contient des données hexadécimales imprimables et non imprimables, les caractères hexadécimaux imprimables sont affichés en codage ASCII et le reste de la chaîne au format hexadécimal. En cas de remplacement hexadécimal, \0000\ termine une chaîne. Ainsi, « xxxx\0000\yyyy » devient « xxxx ».

Format

```
DISPLAY(string_data)
```

Types de données

Argument	Type	Description
string_data	chaîne (ENTRÉE) [FACULTATIF]	Toute chaîne à afficher. Si vous l'omettez, le contenu de toutes les variables est affiché (chaînes, nombres et tableaux) pour chaque script.

Par exemple :

```
DISPLAY( )
DISPLAY(sdata_var)
DISPLAY("Hello This is String Data")
DISPLAY(sdata_var)
```

ELSE

La commande ELSE marque la fin de la partie true de la commande if() précédemment associée. Les commandes d'analyse qui suivent la commande ELSE() sont exécutées si le résultat
de l'instruction IF() est FALSE. Elles sont exécutées jusqu'à la commande ENDIF() correspondante suivante.

Format

```
ELSE()
```

Par exemple :

```
IF(i = 10)
ALERT("I is 10")
ELSE()
ALERT("I is not 10")
ENDIF()
```

La comparaison directe avec un nombre négatif est impossible. Pour cela, utilisez l'une des deux méthodes suivantes :

- Utilisez la fonction d'analyse compare.
- Effectuez une comparaison indirecte comme suit :

```
SET(i_compare_val=-10)
IF(ivar > i_compare_val)
ALERT("ivar is greater than -10")
endif()
```

ENCODE

La commande ENCODE permet de préserver l'identification d'un paquet. Elle cherche des octets
(ou caractères) dans les données et introduit une chaîne d'échappement (ou des préfixes) devant ces mêmes octets et ce, chaque fois que ces octets sont détectés dans les données.

Format

```
ENCODE(data_encode, match, escape)
```

Types de données

Argument	Type	Description
data_encode	svar (ENTRÉE/ SORTIE)	Variable de données de chaîne à coder. Le résultat est replacé dans la variable.
match	chaîne (ENTRÉE)	Chaîne d'octets à rechercher dans la variable chaîne data_encode.
escape	chaîne (ENTRÉE)	Chaîne d'échappement à placer devant chaque octet trouvé dans la variable data_encode.

Par exemple :

Dans l'exemple suivant, deux chaînes de données sont codées : la première de sorte que le symbole « # » soit placé devant tous les espaces et la seconde de sorte que des « !! » soient placés devant tous les « t » et tous les « h ».

```
COPY(data:"Preface all spaces with ‘#’")
ENCODE(data, " ", "#")
COPY(svar:"Preface ‘t‘s and ‘h’s with ‘!!’")
ENCODE(svar, "th", "!!")
```

Résultat :

```
data = "Preface# all# spaces# with# ‘#’"
svar = "Preface ‘!!t’s and !!h’s wi!!t!!h ‘!!’"
```

ENCODEMIME

La commande ENCODEMIME permet à l'utilisateur de coder une chaîne ou une variable chaîne à l'aide d'un codage sur 64 bits, et de stocker la chaîne codée finale sous forme de variable chaîne.

Format

```
ENCODEMIME(data, encoded_data)
```

Types de données

Argument	Type	Description
data	chaîne/variable chaîne(ENTRÉE)	Chaîne de données nécessitant un codage.
encoded_data	variable chaîne (SORTIE)	Données codées finales.

Par exemple :

```
COPY(s_data:"test encode64 command")
ENCODEMIME(s_data, s_encd_data)
```

Dans l'exemple ci-dessus, la commande ENCODEMIME code la chaîne de la variable s_data par un codage sur 64 bits et stocke la chaîne codée dans s_encd_data. La variable S_encd_data est renseignée de la manière suivante :

```
VGVzdGluZyBEYXRhIEVuY29kaW5n
```

Voir également la commande DECODEMIME.

ENDFOR

La commande ENDFOR marque la fin du bloc for() précédent.

Format

```
ENDFOR()
Exemple
FOR(i=0,i<3,i=i+1)
ALERT("Still in loop")
ENDFOR()
```

ENDIF

La commande ENDIF marque la fin du bloc if() précédent.

Format

```
ENDIF()
```

Par exemple :

```
IF(i = 10)
ALERT("I is 10")
ELSE()
ALERT("I is not 10")
ENDIF()
```

La comparaison directe avec un nombre négatif est impossible. Pour cela, utilisez l'une des méthodes suivantes :

- Utilisez la fonction d'analyse compare.
- Effectuez une comparaison indirecte comme suit :

```
SET(i_compare_val=-10)
IF(ivar >i_compare_val)
ALERT("ivar is greater than -10")
ENDIF()
```

ENDWHILE

La commande ENDWHILE marque la fin du bloc while() précédent.

Format

```
ENDWHILE()
Exemple :
WHILE(i<3)
SET(i=i+1)
ENDWHILE()
```

EVENT

La commande EVENT crée et envoie un message d'alerte. Elle ne prend aucun paramètre. La commande EVENT construit automatiquement le message d'alerte en se servant du contenu des variables réservées.

La plupart des variables réservées assignent directement vers les balises META du modèle de l'assistant v3.2. Les seules variables envoyées sont celles qui sont utilisées dans le script et qui ne sont pas définies sur “”. Pour qu'un message d'alerte puisse être traité par le Gestionnaire des collecteurs, les variables comme i_Severity et s_Res sont requises.

Variables réservées relatives aux événements

REMARQUE : si une étiquette est précédée d'un « e », comme e.crt, celle-ci se rapporte à des événements actuels. Si une étiquette est précédée d'un « w », comme w.crt, elle se rapporte à des événements historiques.

Variable	Description courte	Mappe vers la balise META (étiquette)
s_BM	Message de base	Message (msg)
i_Severity	Gravité	Gravité (sev)
s_Res	Ressource	Ressource (res)
s_SubRes	Sous-ressource	Sous-ressource (sres)
s_ET	Heure de l'événement	EventTime (et)
s_P	Protocole	Protocol (prot)
s_DP	Port de destination	DestinationPort (dp)
s_SP	Port source	SourcePort (sp)
s_EVT	Nom de l'événement	EventName (evt)
s_SN	Nom du capteur	SensorName (sn)
s_SIP	IP source	Source IP (sip)
s_DIP	IP de destination	DestinationIP (dip)
s_SHN	Nom de l'hôte source	SourceHostName (shn)
s_DHN	Nom de l'hôte de destination	DestinationHostName (dhn)
s_SUN	Nom d'utilisateur source	SourceUserName (sun)
s_DUN	Nom d'utilisateur de destination	DestinationUserName (dun)
s_FN	Nom du fichier	FileName (fn)

Variable	Description courte	Mappe vers la balise META (étiquette)
s_EI	Informations développées	ExtendedInformation (ei)
s_RN	Nom de programme reporteur	ReporterName (rn)
s_ST	Type de capteur	Sensor Type (st)
s_PN	Nom du produit	ProductName (pn)
s_CRIT	Sévérité	Criticality (crt)
s_VULN	Vulnérabilité	Vulnerability (vul)
s_CT1	Réservée aux clients 1	Ct1 (ct1)
s_CT2	Réservée aux clients 2	Ct2 (ct2)
s_CT3	Réservée aux clients 3	Ct3 (ct3)
s_RT1	Nom d'attaque du périphérique (réservée à Sentinel 1)	Rt1 (rt1)
s_RT2	Réservée à Sentinel 2	Rt2 (rt2)
s_RT3	Réservée à Sentinel 3	Rt3 (rt3)
s_CV1 à s_CV100	Variable client 1 à 100 **REMARQUE** : 1 à 10 est de type long (nombre) 11 à 20 de type date 21 à 100 de type chaîne	Cv1 à Cv100 (cv1 à cv100)
s_RV1 to s_RV29	Valeur réservée 1 à 29 **REMARQUE** : réservé à Novell.	Rv1 à Rv31 (rv1 à rv29)
s_RV30	AttackId	Rv30
s_RV31	DeviceName	Rv31
s_RV32	DeviceCategory	Rv32 (rv32)
s_RV33	EventContext	Rv33 (rv33)
s_RV34	SourceThreatLevel	Rv34 (rv34)
s_RV35	SourceUserContext	Rv35 (rv35)
s_RV36	DataContext	Rv36 (rv36)
s_RV37	SourceFunction	Rv37 (rv37)
s_RV38	SourceOperationalContext	Rv38 (rv38)
s_RV39	MSSPCustomerName	Rv39 (rv39)
s_RV40 à s_RV43	Valeur réservée 40 à 43 **REMARQUE :** réservé à Novell.	Rv40 à Rv43 (rv40 à rv43)
s_RV44	DestinationThreatLevel	Rv44 (rv44)
s_RV45	DestinationUserContext	Rv45 (rv45)
s_RV46	VirusStatus	Rv46 (rv46)
s_RV47	DestinationFunction	Rv47 (rv47)
s_RV48	DestinationOperationalContext	Rv48 (rv48)

Variable	Description courte	Mappe vers la balise META (étiquette)
s_RV49	ReservedVar49 **REMARQUE :** réservé à Novell.	Rv49 (rv49)
s_RV50	eSecTaxonomyLevel1	Rv50 (rv50)
s_RV51	eSecTaxonomyLevel2	Rv51 (rv51)
s_RV52	eSecTaxonomyLevel3	Rv52 (rv52)
s_RV53	eSecTaxonomyLevel4	Rv53 (rv53)
s_RV54 à s_RV100	Valeur réservée 54 à 100 **REMARQUE :** réservé à Novell.	Rv54 à Rv100 (rv54 à rv100)

Mise en forme automatique

Les variables réservées s_DP, s_SP et s_P sont en minuscules, et les variables réservées s_ST et s_PN en majuscules avant l'envoi du message d'événement. La variable relative à l'heure de l'événement s_ET est définie par défaut sur le format d'heure standard comme suit :

```
s_Year-s_Month-s_Day~sHour:s_Min:s_Sec~s_AMPM24~s_TZ
```

Vous pouvez définir la variable s_ET sur d'autres données. s_Hour et s_Month doivent être tous deux définis, au minimum, pour que ET soit créée. Tous les champs vides apparaissent avec la valeur NULL dans le champ ET.

Variables réservées relatives à la date/l'heure

La variable s_ET de la balise META ET est automatiquement renseignée lorsqu'elle n'est pas définie et que s_Hour et s_Month ne sont pas vides. Vous devez attribuer des valeurs aux variables réservées relatives à la date/l'heure. Tout champ vide affiche la valeur NULL. Le format du champ s_Day est un format à deux chiffres 01-09. Le rédacteur du script peut choisir de convertir la valeur mois en un nombre à deux chiffres à l'aide de la commande TRANSLATE et du fichier months.csv. Les balises réservées relatives à la date/l'heure sont les suivantes :

- s_Year
- s_Month
- s_Day
- s_Hour
- s_Min
- s_Sec
- s_TZ
- s_AMPM24

Variables réservées relatives au contrôle des événements

Deux variables, s_SendEITag et s_SendETTag, sont utilisées pour déterminer si la commande EVENT doit inclure les champs EI et ET, respectivement, dans un message d'alerte. Pour désactiver l'envoi de ces deux champs, vous devez définir les variables sur INACTIF.

Format

```
EVENT ()
```

Par exemple :

```
COPY(s_Res:"Resource")
SET(i_Severity = 3)
COPY(s_BM:"Alert")
EVENT()
```

FILEA

La commande FILEA ajoute le contenu d'une chaîne à la fin d'un fichier plat sur un disque. Lors de l'utilisation de cette commande :

- Indiquez le nom du fichier à l'aide d'une chaîne.
- Sous Windows, le nom de fichier doit être introduit par une lettre de lecteur, le caractère deux-points et une barre oblique inverse (tel que c:\).
- Vous devez spécifier le chemin complet du fichier.
- Si le fichier n'existe pas, il est créé.
- S'il ne peut être créé, la commande FILEA n'a aucun effet.
- Le fichier se ferme une fois que les données y ont été ajoutées.

Si vous écrivez cette commande dans le cadre d'un script qui doit être exécuté par un collecteur, veillez à employer la syntaxe appropriée pour les chemins, notamment les barres obliques (/). N'oubliez pas d'utiliser le caractère d'échappement pour les barres obliques et les barres obliques inverses lorsque vous spécifiez le chemin. Le zéro placé à la fin de la chaîne ne figurera pas dans le fichier.

Format

```
FILEA("filename", data)
```

Types de données

Argument	Type	Description
filename	chaîne (ENTRÉE)	Nom du fichier auquel ajouter les données.
data	chaîne (ENTRÉE)	Chaîne de données à ajouter au fichier.

Par exemple :

Dans l'exemple suivant, le fichier \temp\mux_data est créé et le contenu de s_variable lui est ajouté :

```
FILEA("c:/\temp/\mux_data", s_variable)
FILEA("mux_data", "literal")
FILEA("mux_data", s_variable)
```

Dans l'exemple suivant, une chaîne est ajoutée à la fin d'un fichier journal d'audit :

```
COPY(audit_str: "Sent 20 severity 5 alerts.")
FILEA("h:/\temp/\audit.log", audit_str)
```

FILEL

La commande FILEL récupère la longueur (en octets) d'un fichier plat et la place dans une variable numérique. Lors de l'utilisation de cette commande :

- Indiquez le nom du fichier à l'aide d'une chaîne.
- Sous Windows, le nom de fichier doit être introduit par une lettre de lecteur, le caractère deux-points et une barre oblique inverse (tel que c:\).
- Si le fichier n'existe pas, la commande FILEL n'a aucun effet et le contenu de la variable numérique demeure inchangé.
- Le fichier se ferme une fois que les données y ont été lues.

Si vous écrivez cette commande dans le cadre d'un script qui doit être exécuté par un collecteur, veillez à employer la syntaxe appropriée pour les chemins, notamment les barres obliques (/). N'oubliez pas d'utiliser le caractère d'échappement pour les barres obliques et les barres obliques inverses lorsque vous spécifiez le chemin.

Format

```
FILEL("filename", i_length)
```

Types de données

Argument	Type	Description
filename	chaîne (ENTRÉE)	Nom du fichier pour lequel déterminer la longueur.
i_length	variable numérique (numvar) (SORTIE)	Longueur du fichier, en octets.

Par exemple :

```
FILEL("h:/\tmp/\onfotron.log", i_length)
```

Retourne la longueur du fichier infotron.log, en octets. Par exemple :

```
i_length = 2390
```

FILER

La commande FILER copie le contenu d'un fichier plat du disque dans une variable chaîne. Lors de l'utilisation de cette commande :

- Indiquez le nom du fichier à l'aide d'une chaîne.
- Sous Windows, le nom de fichier doit être introduit par une lettre de lecteur, le caractère deux-points et une barre oblique inverse (tel que c:\).

- Si le fichier n'existe pas, la commande FILER n'a aucun effet et le contenu de la variable chaîne (svar) demeure inchangé.
- Le fichier se ferme une fois que les données y ont été lues.
- Vous pouvez éventuellement entrer le nombre maximal d'octets à lire. Vous ne pouvez utiliser le paramètre max_bytes que s'il est associé au paramètre i_offset.

Si vous écrivez cette commande dans le cadre d'un script qui doit être exécuté par un collecteur, veillez à employer la syntaxe appropriée pour les chemins, notamment les barres obliques (/). N'oubliez pas d'utiliser le caractère d'échappement pour les barres obliques et les barres obliques inverses lorsque vous spécifiez le chemin.

Format

```
FILER("filename", dest, [i_offset [, i_max_bytes]])
```

REMARQUE : vous ne pouvez utiliser le paramètre max_bytes que s'il est associé au paramètre i_offset.

Types de données

Argument	Type	Description
filename	chaîne (ENTRÉE)	Nom du fichier dans lequel lire la chaîne de données.
data	svar (SORTIE)	Variable chaîne dans laquelle sont placées les données lues dans le fichier.
i_offset	entier (ENTRÉE) [FACULTATIF]	Indique un nombre de caractères pour le décalage à partir duquel commencer la lecture.
max_bytes	entier (ENTRÉE) [FACULTATIF]	Indiquez éventuellement le nombre maximum d'octets à lire. **REMARQUE :** si vous employez cet argument, l'argument i_offset doit également être spécifié.

Par exemple :

```
CLEAR(data)
FILER("filename", data, 0, 20)
if(data = "")
ALERT(s_res_var, "Data file doesn’t exist or is
empty.", 0)
ENDIF()
```

FILEW

La commande FILEW écrit le contenu d'une chaîne dans un fichier plat du disque. Lors de l'utilisation de cette commande :

- Le contenu précédent du fichier est remplacé.
- Indiquez le nom du fichier à l'aide d'une chaîne.
- Sous Windows, le nom de fichier doit être introduit par une lettre de lecteur, le caractère deux-points et une barre oblique inverse (tel que c:\).
- Si le fichier n'existe pas, il est créé.
- S'il ne peut être créé, la commande FILEW n'a aucun effet.
- Le fichier se ferme une fois que les données y ont été écrites.

Si vous écrivez cette commande dans le cadre d'un script qui doit être exécuté par un collecteur, veillez à employer la syntaxe appropriée pour les chemins, notamment les barres obliques (/). N'oubliez pas d'utiliser le caractère d'échappement pour les barres obliques et les barres obliques inverses lorsque vous spécifiez le chemin.

Format

```
FILEW("filename", data)
```

Types de données

Argument	Type	Description
filename	chaîne (ENTRÉE)	Nom du fichier dans lequel écrire la chaîne de données.
data	svar (SORTIE)	Données à écrire dans le fichier.

Par exemple :

```
FILEW("filename", data)
FILEW("h:/\tmp/\infotron.stat", "SUCCESSFUL EXEC")
```

FOR

La commande FOR permet de mettre en boucle un flux de contrôle. Lors de l'utilisation de cette commande :

- L'instruction d'initialisation est toujours exécutée.
- Si le résultat de l'instruction de comparaison FOR() est true, les commandes d'analyse placées après FOR() et avant l'instruction ENDFOR() suivante, sont exécutées. L'instruction d'incrémentation est ensuite exécutée et le flux de contrôle retourne à l'instruction de comparaison.
- Si le résultat de l'instruction de comparaison FOR() est false, aucune commande d'analyse n'est exécutée entre les instructions FOR() et ENDFOR(). L'instruction d'incrémentation n'est pas exécutée.

- Bien que vous puissiez utiliser tous les types de données des deux côtés de l'instruction de comparaison for(), vous ne pouvez comparer que des valeurs de même type entre elles (numérique avec numérique, chaîne avec chaîne par exemple).
- L'opérateur de l'instruction de comparaison FOR() peut être le suivant : <, =, >, <=, >=, <>, &, + ou ^.

La comparaison directe avec un nombre négatif est impossible. Pour cela, utilisez l'une des méthodes suivantes :

- Utilisez la fonction d'analyse COMPARE.
- Effectuez une comparaison indirecte comme suit :

```
SET(i_compare_val=-10)
FOR(ivar=0, ivar>i_compare_val, ivar=ivar-1)
ALERT("Still in loop")
ENDFOR()
```

Format

```
FOR(initialization, compare, increment)
```

Types de données

Argument	Type	Description
initialization	SET() paramètre	Tout paramètre valide pouvant être transmis à la commande SET(). Reportez-vous à la définition de la commande SET().
conditional	IF() conditionnel	Tout paramètre valide pouvant être transmis à la commande IF(). Reportez-vous à la définition de la commande IF().
increment	SET() paramètre	Tout paramètre valide pouvant être transmis à la commande SET(). Reportez-vous à la définition de la commande SET().

Par exemple :

```
FOR(i=0, i<3, i=i+1)
```

GETCONFIG

Extrait le paramétrage actuel d'une propriété système. Cette commande récupère les propriétés système définies à l'aide de la commande SETCONFIG. Ces commandes permettent
de définir des variables et de récupérer les valeurs actuelles des propriétés système susceptibles
de changer de manière périodique, comme un fichier journal qui est renommé quotidiennement avec la date du jour.

Les propriétés système disponibles sont les suivantes :

Propriété système	Exemple(s)
▪ System.OS.Family	Solaris et Windows
▪ System.OS.Name	Windows 2000

▪ System.OS.Version.Major	5
▪ System.OS.Version.Minor	0
▪ System.Net.Hostname	ESECServer
▪ System.Net.IP_List	liste des adresses IP de cet hôte séparées par un point-virgule, comme « 172.163.3.45;172.45.2.1 ».

Voir également la commande SETCONFIG.

Deux paramètres sont obligatoires :

- Le premier définit l'option de configuration (FileConnector.InputFile ou FileConnector.OutputFile).
- Le deuxième définit la valeur de configuration à extraire.

Format

```
GETCONFIG(Config Option, Value)
```

Types de données

Argument	Type	Description
Config Option	chaîne (ENTRÉE)	Nom de la variable de configuration à extraire. Fichier d'entrée = “FileConnector.InputFile” Fichier de sortie = “FileConnector.OutputFile”
Value	chaîne (ENTRÉE)	Paramètre de configuration à extraire.

Par exemple :

```
GETCONFIG(“FileConnector.InputFile”, s_inputfilename)
GETCONFIG(“FileConnector.OutputFile”,
s_outputfilename)
```

Contenu des variables de sortie

```
“C:/\filename.txt”
```

GETENV

La commande GETENV extrait la valeur d'une variable d'environnement.

Format

```
GETENV(Environment Key, Variable to store value)
```

Type de données

Argument	Type	Description
Environment Key	chaîne (ENTRÉE)	Nom de la variable d'environnement.

Argument	Type	Description
Variable to store value	variable chaîne (ENTRÉE)	Destination de la variable d'environnement.

Par exemple :

```
GETENV("ESEC_HOME", s_EsecHome)
```

HEXTONUM

La commande HEXTONUM convertit une chaîne comportant un maximum de 4 octets de données hexadécimales en un nombre décimal, et place ce résultat dans une variable flottante ou entière. Si les données font plus de 4 octets, le résultat n'est pas correct.

Format

```
HEXTONUM(bytes_data, i_val [,[-]i_4] [, ioffset])
```

Types de données

Argument	Type	Description
bytes_data	chaîne (ENTRÉE)	Chaîne de 1 à 4 octets. Par exemple : « \FF\ », « \FF FF\ », « \3C 4A F2\ », « \43 76 F3 FF\ » ou « TEST ». Le nombre hexadécimal représenté par ces octets sera converti en une valeur entière, i_val.
i_val	variable numérique (numvar) (SORTIE)	Valeur décimale, équivalant au nombre hexadécimal, placée dans cette variable, ivar ou fvar.
i_len	numérique (ENTRÉE) [FACULTATIF]	Nombre d'octets hexadécimaux à convertir en un entier (doit être compris entre 1 et 4). Si ceparamètre n'est pas défini, la valeur par défaut est le nombre d'octets contenus dans la chaîne d'entrée, bytes_data, jusqu'à un maximum de 4 octets. Si i_len est positif, les octets sont alors interprétés de gauche à droite (de l'octet le plus fort vers l'octet le plus faible). Si i_num_bytes est négatif, les octets sont interprétés de droite à gauche (de l'octet le plus faible vers l'octet le plus fort).
ioffset	numérique (ENTRÉE) [FACULTATIF]	Nombre d'octets du décalage à ignorer dans bytes_data.

Par exemple :

Dans l'exemple suivant, les données de la chaîne hexadécimale « \5A32\ » sont converties en une valeur entière, interprétées de l'octet le plus fort vers l'octet le plus faible, puis inversement, de l'octet le plus faible vers l'octet le plus fort.

```
COPY(data:"\5A 32\")
HEXTONUM(data, ivar1)
HEXTONUM(data, ivar2, -2)
```

REMARQUE : en cas de remplacement hexadécimal, \0000\ termine une chaîne. Ainsi, « xxxx\0000\yyyy » devient « xxxx ».

Contenu des variables de sortie :

```
ivar1 = 23090
ivar2 = 12890
```

IF

La commande IF compare deux valeurs.

- Si le résultat de l'instruction IF() est true, les commandes d'analyse placées après IF() et jusqu'à l'instruction ELSE() ou ENDIF() suivante, sont exécutées.
- Si le résultat de l'instruction IF() est false, les commandes d'analyse placées après l'instruction ELSE() jusqu'à ENDIF() sont exécutées.
- Si aucune instruction ELSE() n'est utilisée, aucune commande d'analyse n'est exécutée entre les instructions IF() et ENDIF() lorsque le résultat de l'instruction IF() est false.
- Bien que vous puissiez utiliser tous les types de données des deux côtés de l'instruction de comparaison IF(), vous ne pouvez comparer que des valeurs de même type entre elles (numérique avec numérique, chaîne avec chaîne par exemple).
- L'opérateur de l'instruction de comparaison IF() peut être le suivant : <, =, >, <=, >=, <>, &, + ou ^. N'utilisez pas l'opérateur logique NON (^) en association avec une variable chaîne. Une erreur de syntaxe serait générée.

La comparaison directe avec un nombre négatif est impossible. Pour cela, utilisez l'une des méthodes suivantes :

- Utilisez la fonction d'analyse COMPARE.
- Effectuez une comparaison indirecte comme suit :

```
SET(i_compare_val=-10)
IF(ivar > i_compare_val)
ALERT("ivar is greater than -10")
ENDIF()
```

Format

```
IF(<expr>)
Where:
expr ::= var
        | (<expr>)
```

```
| ^ <expr>
```

Où <expr> doit retourner un entier ou une valeur flottante.

```
| <expr> <|=|>|<=|>=|<>|&|+ <expr>
```

Où les deux <expr> doivent retourner une valeur du même type.

Types de données

Argument	Type	Description
données1	variable (ENTRÉE)	Données à comparer à données2. Si données2 n'est pas utilisé, l'instruction devient logique (0 = false, tout le reste = true).
opérateur logique	< = > <= >= <> & + ^	Inférieur à Égal à Supérieur à Inférieur ou égal à Supérieur ou égal à Différent de ET logique OU logique NON logique
données2	tous (ENTRÉE) [FACULTATIF]	Données à comparer à données1. Elles doivent être du même type que ces dernières.
…	mêmes informations que précédemment	Utilisez jusqu'à 200 paramètres individuels pour créer des expressions logiques complexes.

Par exemple :

```
IF(s = "test" & i_count < 5)
script(test)
ELSE()
IF((i <= i_num) + (i_count <> 10) &
(i_page))page("111")
ENDIF()
ENDIF()
```

INC

La commande INC incrémente les variables numériques de 1. Lorsque vous utilisez cette commande, vous devez indiquer une variable entière ou flottante.

Format

```
INC(i_counter)
```

Types de données

Argument	Type	Description
i_counter	variable numérique (numvar) (ENTRÉE/ SORTIE)	Variable numérique à incrémenter de 1.

Par exemple :

```
SET(icounter = 0)
INC(icounter)
INC(icounter)
```

Résultat :

```
icounter = 2
```

INDICATOR

La commande INDICATOR envoie des messages d'indication à Sentinel. Les messages contiennent du texte à afficher sur l'indicateur spécifié dans Sentinel.

Format

```
INDICATOR(name, value)
```

REMARQUE : dans les versions antérieures à v4.0, la commande INDICATOR disposait d'arguments supplémentaires qui ne sont plus utilisés. Pour des raisons de compatibilité avec les anciens collecteurs, ces arguments portent l'étiquette « Not Used » (non utilisé) dans la fenêtre Wizard Command Editor (Éditeur de commandes de Wizard).

Types de données

Argument	Type	Description
name	chaîne (ENTRÉE)	Nom de l'indicateur.
value	chaîne (ENTRÉE)	Texte de l'indicateur à afficher dans la console Sentinel. Par exemple : `IMPRIMANTE ALLUMÉE`

Par exemple :

```
INDICATOR("memory", "5 MB")
INDICATOR(name, value)
```

REMARQUE : le nom de l'indicateur dans la commande d'analyse doit correspondre au nom de l'indicateur dans Sentinel. Dans le cas contraire, l'indicateur n'est pas mis à jour dans la console Sentinel.

INFO_CLEARTAGS

Cette fonction réinitialise à zéro (ou efface, dans le cas de chaînes) toutes les variables appartenant à l'ensemble de blocs d'informations auquel fait référence l'identificateur. Utilisez la commande INFO_CONSTANTTAGS pour éviter que cette opération ne porte sur un sous-ensemble de ces balises.

Format

```
INFO_CLEARTAGS(<IN handle>)
```

Types de données

Argument	Type	Description
IN handle	chaîne (ENTRÉE)	Type de bloc d'informations.

INFO_CLOSE

Cette commande est utilisée pour fermer une session de bloc d'informations. Lors de l'appel de cette commande, tout bloc d'informations non envoyé est tout d'abord envoyé comme il le serait avec la commande INFO_SEND. La commande envoie ensuite un message de fermeture de la session de bloc d'informations en définissant l'attribut EOD (End Of Data) de l'élément infos sur « true ». Une fois le message de fermeture envoyé, le numéro du segment (segnum) est incrémenté de un.

Format

```
INFO_CLOSE(<IN handle>)
```

Types de données

Argument	Type	Description
IN handle	chaîne (ENTRÉE)	Type de bloc d'informations.

INFO_CONSTANTTAGS

Utilisez cette commande pour indiquer les balises à conserver lors de l'appel de la commande INFO_CLEARTAGS. Transmettez plusieurs noms de balises ou aucun afin de créer l'ensemble de balises constantes. Plusieurs appels de cette fonction réinitialisent la liste des balises constantes.

Format

```
INFO_CONSTANTTAGS(<IN handle>, [<IN tag name>, …])
```

Types de données

Argument	Type	Description
IN handle	chaîne (ENTRÉE)	Type du bloc d'informations.
IN tag name	chaîne (ENTRÉE)	Nom auquel se référer pour IN handle.

INFO_CREATE

Cette commande crée un ensemble de blocs d'informations. Vous devez indiquer un identificateur (que vous utiliserez dans toutes les autres commandes en rapport avec cet ensemble de blocs d'informations). Vous devez également indiquer un type. Il s'agit d'une chaîne de votre choix qui doit néanmoins suivre un format précis (voir la commande INFO_SEND).

Si vous appelez INFO_CREATE sur un identificateur déjà existant, son contenu est supprimé, comme si vous utilisiez un nouvel identificateur. Vous devrez appeler de nouveau INFO_SETTAG et INFO_CONSTANTTAGS.

Format

```
INFO_CREATE(<OUT handle>,<IN type>)
```

Types de données

Argument	Type	Description
OUT handle	chaîne (SORTIE)	Nom associé à IN type.
IN type	chaîne (ENTRÉE)	Type de bloc d'informations.

INFO_DUMP

Cette commande conserve l'état actuel de l'ensemble de blocs d'informations dans une variable chaîne. Elle a été incluse afin de simplifier les opérations de test, mais peut également servir à réutiliser les ensembles de blocs d'informations ou à les enregistrer dans un fichier texte ou tout autre type de fichier de votre choix. Elle ne possède pas l'effet négatif de la commande INFO_SEND dans la mesure où elle n'efface pas l'état actuel.

Format

```
INFO_DUMP(<IN handle>, <OUT string-variable>)
```

Types de données

Argument	Type	Description
IN handle	chaîne (ENTRÉE)	Type du bloc d'informations.
OUT string-variable	chaîne (SORTIE)	variable de chaîne en rapport avec IN handle

INFO_PUSH

Cette commande balise les valeurs actuelles de toutes les balises (via leurs variables associées) et les place à la fin de la liste des blocs d'informations auxquels fait référence un identificateur.
Les blocs continuent de s'accumuler dans l'ensemble jusqu'à ce qu'ils en soient supprimés par le biais des commandes INFO_CREATE, INFO_SEND ou INFO_CLOSE. Pour INFO_CREATE, aucune action n'est effectuée. Pour INFO_SEND, les blocs d'informations sont envoyés au Gestionnaire des collecteurs. Pour INFO_CLOSE, les blocs d'informations sont envoyés au Gestionnaire des collecteurs et un message de fermeture de blocs d'informations (EndOfData ou EOD) est envoyé.

Format

```
INFO_PUSH(<IN handle>)
```

Types de données

Argument	Type	Description
IN handle	chaîne (ENTRÉE)	Type de bloc d'informations.

INFO_SEND

Cette commande envoie l'ensemble actuel de blocs d'informations sur le canal de communication spécifié par le type utilisé dans la commande INFO_CREATE, ajouté au mot « infoblock. », point inclus. Ainsi, si le type est « vulnérabilité », le nom du canal sur lequel est envoyé le message se nomme « infoblock.vulnérabilité ».

En outre, cette commande efface l'ensemble actuel de blocs d'informations et incrémente le numéro du segment (segnum) de un.

Format

```
INFO_SEND(<IN handle>)
```

Types de données

Argument	Type	Description
IN handle	chaîne (ENTRÉE)	Type de bloc d'informations.

INFO_SETTAG

Cette commande lie une variable de script au nom d'un attribut. Lors de l'appel de INFO_PUSH (voir INFO_PUSH), toutes les variables liées à cette commande sont définies en tant qu'attributs dans une entrée du bloc.

Format

```
INFO_SETTAG(<IN handle, IN tag name, IN variable)
```

Types de données

Argument	Type	Description
IN handle	chaîne (ENTRÉE)	Type du bloc d'informations.
IN tag name	chaîne (ENTRÉE)	Type du nom de la balise.
IN variable	chaîne (ENTRÉE)	Type de la variable.

Balises des blocs d'informations relatifs à la vulnérabilité

Le tableau suivant répertorie les balises valides des blocs d'informations sur la vulnérabilité associées à la commande INFO_SETTAG. Les balises indiquées comme étant obligatoires doivent être définies de sorte que le bloc d'informations puisse être stocké en tant que vulnérabilité. Même si le bloc n'est pas stocké en tant que vulnérabilité, les balises marquées comme étant constantes en seront extraites. Si une des balises définies ne figure pas dans la liste suivante, l'interface dorsale des vulnérabilités l'ignore.

Nom de la balise	Explication	Type	Constante	Obligatoire
ScannerInstance	Nom donné à l'instance du scanner par l'utilisateur. Défini habituellement dans les paramètres du collecteur.	Chaîne	X	
ProductName	Nom du scanner.	Chaîne	X	
ProductVersion	Version du scanner.	Chaîne	X	
ScannerType	Type du scanner.	Chaîne	X	
Vendor	Nom du fournisseur du scanner.	Chaîne	X	

Nom de la balise	Explication	Type	Constante	Obligatoire
ScanType	PARTIEL ou COMPLET.	Chaîne	X	
ScanStartDate	Heure à laquelle a débuté l'analyse.	Chaîne		
ScanEndDate	Heure à laquelle s'est terminée l'analyse.	Chaîne		
IP	IP de la ressource.	Chaîne		X
HostName	Nom d'hôte de la ressource.	Chaîne		
Location	Emplacement de la ressource.	Chaîne		
Department	Service de la ressource.	Chaîne		
BusinessSystem	Système professionnel de la ressource.	Chaîne		
OperationalEnvironment	Environnement d'exploitation de la ressource.	Chaîne		
Regulation	Régulation de la ressource.	Chaîne		
RegulationRating	Taux de régulation de la ressource.	Chaîne		
Criticality	Degré de sévérité de la ressource [1 – 25]	Nombre		
VulnModule	Module utilisé pour détecter la vulnérabilité.	Chaîne		
PortNumber	Numéro de port lié à la vulnérabilité.	Nombre		
PortName	Nom du port lié à la vulnérabilité.	Chaîne		
NetworkProtocol	Protocole réseau lié à la vulnérabilité.	Nombre		
ApplicationProtocol	Protocole d'application lié à la vulnérabilité.	Chaîne		
AssignedVulnSeverity	Degré de gravité attribué lié à la vulnérabilité.	Nombre		
ComputedVulnSeverity	Degré de gravité calculé lié à la vulnérabilité.	Nombre		
VulnDescription	Description de la vulnérabilité.	Chaîne		
VulnSolution	Solution de la vulnérabilité.	Chaîne		
VulnSummary	Solution de la vulnérabilité.	Chaîne		

Nom de la balise	Explication	Type	Constante	Obligatoire
VulnCrossRefs	Liste de codes liés à la vulnérabilité.	Chaîne		
DetectedOs	Système d'exploitation détecté lors de la découverte de la vulnérabilité.	Chaîne		
DetectedOsVersion	Version du système d'exploitation détectée lors de la découverte de la vulnérabilité.	Chaîne		
ScannedApp	Application détectée lors de la découverte de la vulnérabilité.	Chaîne		
ScannedAppVersion	Version de l'application détectée lors de la découverte de la vulnérabilité.	Chaîne		
VulnUserName	Nom d'utilisateur de la vulnérabilité.	Chaîne		
VulnUserDomain	Domaine de l'utilisateur lié à la vulnérabilité.	Chaîne		
VulnTaxonomy	Taxinomie de la vulnérabilité.	Chaîne		
ScannerClassification	Classification de la vulnérabilité indiquée par le scanner.	Chaîne		
ExtendedInformation	Informations développées à stocker avec la vulnérabilité.	Chaîne		
VulnName	Nom de la vulnérabilité indiqué par le scanner.	Chaîne		

Exemple des commandes INFO_*

Sentinel regroupe les analyses sur la vulnérabilité en blocs plus petits (sessions de blocs d'informations) plus faciles à traiter. Une session contient plusieurs ensembles de blocs d'informations, chacun doté d'un numéro de segment croissant (segnum) suivi d'un message de fermeture. On fait référence à une instance d'une session de bloc d'informations par son ID global unique. À chaque appel de la commande INFO_SEND, un ensemble de blocs d'informations accompagné des valeurs actuellement « empilées » et du numéro de segment actuel (segnum) est envoyé. Immédiatement après cette opération, le numéro du segment (segnum) est incrémenté de un. La commande INFO_SEND est appelée pour chaque lot de données, puis la commande INFO_CLOSE afin de fermer la session de bloc d'informations. Le message de fermeture consiste en un ensemble de bloc d'informations doté de l'attribut EOD défini sur « true ».

Par exemple :

```
INFO_CREATE(h_vuln,"vulnerability")
INFO_SETTAG(h_vuln,"ALPHA", s_alpha)
INFO_SETTAG(h_vuln,"BETA", i_beta)
INFO_SETTAG(h_vuln,"GAMMA", s_gamma)
INFO_SETTAG(h_vuln,"DELTA", i_delta)
INFO_SETTAG(h_vuln,"^1E*P$S I(L)O.N--", f_epsilon)
INFO_CONSTANTTAGS(h_vuln,"GAMMA","DELTA","^1E*P$S
I(L)O.N--")
SET(i_beta=12345)
SET(i_delta=123456789)
SET(f_epsilon=1.234)
COPY(s_alpha:"a is for apple")
COPY(s_gamma:"c is for coffee")
INFO_PUSH(h_vuln)
INFO_CLEARTAGS(h_vuln)
INFO_PUSH(h_vuln)
INFO_DUMP(h_vuln, s_simulate)
INFO_SEND(h_vuln)
SET(i_beta=6789)
SET(i_delta=987654321)
SET(f_epsilon=3.1415926)
COPY(s_alpha:"a is for acorn")
COPY(s_gamma:"c is for carrot")
INFO_PUSH(h_vuln)
INFO_SEND(h_vuln)
INFO_CLOSE(h_vuln)
```

Résultats :

```
<?xml version="1.0" encoding="UTF-8"?>
<infos id="B008961E00CB1026B8F000065BBD13AB"
type="vulnerability" segnum=”0” version=”4.2.0.0”
EOD=”false”>
<info ALPHA="a is for apple" BETA="12345"
DELTA="123456789" GAMMA="c is for coffee"
_1EPSILON="1.234"/>
<info ALPHA="" BETA="0" DELTA="123456789" GAMMA="c is
for coffee" _1EPSILON="1.234"/>
</infos>
<?xml version="1.0" encoding="UTF-8"?>
```

```
<infos id="B008961E00CB1026B8F000065BBD13AB"
type="vulnerability" segnum=”1” version=”4.2.0.0”
EOD=”false”>
<info ALPHA="a is for acorn" BETA="6789"
DELTA="987654321" GAMMA="c is for carrot"
_1EPSILON="3.1415926"/>
</infos>
<?xml version="1.0" encoding="UTF-8"?>
<infos id="B008961E00CB1026B8F000065BBD13AB"
type="vulnerability" segnum=”2” version=”4.2.0.0”
EOD=”true”>
</infos>
```

IPTONUM

La commande IPTONUM convertit une chaîne représentant une adresse IPv4 en un nombre entier et place ce dernier dans une variable entière. Cette fonction ne prend en charge que les adresses IPv4. Toute adresse IPv4 hors plage valide donne un résultat incorrect.

Format

```
IPTONUM(ip_address, i_integer, i_valid)
```

Types de données

Argument	Type	Description
ip_address	svar(ENTRÉE)	Adresse IPv4 (chaîne).
i_integer	numérique(SORTIE)	La chaîne d'adresse IPv4 est convertie en un entier. Le résultat est placé dans cette variable.
i_invalid	ivar(SORTIE) [FACULTATIF]	La valeur 0 signifie que l'adresse IP n'est pas valide. La valeur 1 que l'adresse IP est valide.

Par exemple :

Dans l'exemple suivant, l'adresse IPv4 « 10.10.10.255 » est convertie en un nombre entier. i_valid est défini sur 1, ce qui implique que le résultat est valide.

```
IPTONUM("10.10.10.255", i_y, i_valid)
```

Contenu de la variable de sortie :

```
i_y = 168430335
i_valid = 1
```

Dans l'exemple suivant, l'adresse IPv4 non valide « 10.10.10.258 » est convertie en un nombre entier 0. i_valid est défini sur 0, ce qui implique que le résultat n'est pas valide.

```
IPTONUM("10.10.10.258", i_y, i_valid)
```

Contenu de la variable de sortie :

```
i_y = 0
```

```
i_valid = 0
```

La commande NUMTOIP convertit un nombre en une adresse IP. Voir NUMTOIP pour plus d'informations.

LENGTH ou LENGTH-OPTION2

La commande LENGTH détermine une variable numérique à partir de la longueur en octets d'une variable chaîne (sans compter le zéro final).

> **REMARQUE :** au sein de l'éditeur plein écran du Générateur de collecteurs, les commandes LENGTH et LENGTH-OPTION2 sont répertoriées en tant que commandes distinctes. Il s'agit en fait d'une seule et même commande. Elles ne font que décrire différentes variantes de la commande. Si vous deviez utiliser la commande LENGTH-OPTION2 dans l'éditeur de texte, vous entreriez LENGTH.

Format

```
LENGTH(i_length, s_variable)
```

Types de données

Argument	Type	Description
s_variable	chaîne (ENTRÉE)	Chaîne (généralement une variable chaîne) sur laquelle porte le calcul de la longueur.
i_length	variable numérique (numvar) (SORTIE)	Longueur de la variable chaîne, s_variable, placée dans cette variable numérique.

Par exemple :

```
LENGTH(i_length, source)
LENGTH(i_num_bytes, "It makes no sense to do this, as
we know the string whose length we are checking")
```

Résultats :

```
i_num_bytes = 80
```

LOOKUP

La commande LOOKUP fait correspondre les données trouvées dans le tampon de réception ou une chaîne avec les chaînes d'un fichier de clés de recherche donné.

Si un enregistrement correspond octet pour octet, les commandes d'analyse de l'enregistrement du fichier de clés de recherche sont exécutées.

Si le premier paramètre spécifié est une chaîne dans la commande LOOKUP, la commande s'en sert lors de la recherche dans le fichier de clés.

Cette commande comprend cinq arguments ou paramètres.

- compare : si ce paramètre est une valeur numérique, ce nombre d'octets (la valeur numérique) des données issues du tampon de réception, en commençant à partir de la position du pointeur Rx Buffer, constitue la chaîne à comparer avec les chaînes du fichier de clés de recherche.
- lookup name : ce paramètre indique le nom du fichier de clés de recherche en fonction du répertoire WORKBENCH_HOME.
- imatch : une variable entière facultative que vous pouvez spécifier. Elle retourne le statut de la commande LOOKUP (0=aucune correspondance trouvée, 1=correspondance trouvée).
- parameter file : un paramètre facultatif correspondant au nom du fichier de paramètres à utiliser en dehors du fichier par défaut. Le nom par défaut est <Collecteur>.par. Ce nom de fichier ne doit pas comporter le suffixe .par.
- column name : un paramètre facultatif correspondant à la colonne du fichier de paramètres dans laquelle rechercher les valeurs. Son nom par défaut est le nom du modèle. Si vous spécifiez ce paramètre, vous devez également indiquer un fichier de paramètres.

Format

```
LOOKUP(compare, lookup filename [, imatch] [,
[parameter filename] [, column name]])
```

Types de données

Argument	Type	Description
compare	chaîne (ENTRÉE) ou numérique (ENTRÉE)	Données à comparer aux champs du fichier de clés de recherche. La comparaison se fait octet par octet. Le nombre d'octets du tampon de réception (en fonction de la position du pointeur Rx Buffer actuelle) à comparer avec les champs du fichier de clés de recherche. La comparaison se fait octet par octet. **REMARQUE :** cette opération ne fonctionne que si rxbuff a été défini dans le tampon de réception.
lookup filename	chaîne (ENTRÉE)	Nom du fichier de clés de recherche.
imatch	variable numérique (numvar) (SORTIE) [FACULTATIF]	Correspondance trouvée. 0=Non 1=Oui
parameter filename	chaîne (ENTRÉE)	Nom du fichier de paramètres. Valeur par défaut : Collector.par
column name	chaîne (ENTRÉE)	Colonne à utiliser dans le fichier des paramètres. Par défaut : `Nom du collecteur`

Par exemple :

```
LOOKUP(data, filename, imatch)
```

Dans l'exemple suivant, le nom de fichier key_01 est déterminé en fonction du nom figurant dans le fichier des paramètres, et non celui du fichier de clés de recherche.

```
LOOKUP(s_variable, {key_01})
LOOKUP(s_variable, {key_01}, imatch, "Send One Alert",
"GeoElements")
```

Si des définitions de paramètre existent dans le fichier de recherche, il faut les rechercher dans la colonne GeoElements du fichier de paramètres Send One Alert.

NEGSEARCH

La commande NEGSEARCH effectue une recherche vers l'arrière dans le tampon de réception. Cette commande comprend deux paramètres.

- search : la recherche débute au niveau de la position actuelle du pointeur Rx Buffer et se poursuit vers l'arrière jusqu'à ce que la chaîne recherchée soit trouvée, ou jusqu'à ce que la recherche atteigne le début du tampon de réception. Si la recherche aboutit, le pointeur Rx Buffer est mis à jour pour indiquer le premier octet de la chaîne recherchée. Dans le cas contraire, le pointeur Rx Buffer reste à sa position actuelle.
- ifound : un paramètre facultatif. Il s'agit d'une variable entière définie sur 1 si la recherche aboutit et sur zéro si la chaîne recherchée est introuvable.

Format

```
NEGSEARCH(search[, ifound])
```

Types de données

Argument	Type	Description
search	chaîne (ENTRÉE)	Chaîne recherchée dans le tampon de réception, en commençant à partir de la position actuelle du pointeur Rx Buffer vers l'arrière.
ifound	variable numérique (numvar) (SORTIE) (FACULTATIF)	Retourne un résultat en fonction du succès ou de l'échec de la recherche. 0=échec 1=succès

Par exemple :

```
NEGSEARCH("MINOR ALARM")
NEGSEARCH(search_string)
```

Dans les exemples suivants, la recherche porte sur un retour chariot et un saut de ligne :

```
NEGSEARCH("\0d0a\")
NEGSEARCH(data, ifound)
```

Autre exemple :

Dans l'exemple, la lettre soulignée indique la position actuelle du pointeur Rx Buffer.

REMARQUE : en cas de remplacement hexadécimal, \0000\ termine une chaîne. Ainsi, « xxxx\0000\yyyy » devient « xxxx ».

```
Rx Buffer = "Minor Alarm Radio A"
NEGSEARCH("Ala")
```

Résultat :

```
Rx Buffer = "Minor Alarm Radio A"
```

NUMTOHEX

La commande NUMTOHEX convertit une valeur numérique en données hexadécimales et place les octets hexadécimaux obtenus (jusqu'à 4 octets) dans une chaîne.

Format

```
NUMTOHEX(i_decimal, hex_data)
```

Types de données

Argument	Type	Description
i_decimal	numérique (ENTRÉE)	Valeur entière à convertir en données hexadécimales.
hex_data	svar (SORTIE)	Chaîne de 1 à 4 octets représentant les octets hexadécimaux obtenus à partir de la valeur numérique, i_decimal.

Par exemple :

Dans l'exemple suivant, le nombre décimal 16777215 est converti en données hexadécimales.

```
SET(i_decimal = 16777215)
NUMTOHEX(i_decimal, shex)
```

Contenu de la variable de sortie :

```
shex = "\ff ff ff\"
```

NUMTOIP

La commande NUMTOIP convertit une valeur numérique en une adresse IPv4 et place cette dernière dans une chaîne.

Format

```
NUMTOIP(i_integer, ip_address)
```

Types de données

Argument	Type	Description
i_integer	numérique(ENTRÉE)	Valeur entière à convertir en une adresse IPv4.
ip_address	svar(SORTIE)	Adresse IPv4 (chaîne).

Par exemple :

Dans l'exemple suivant, le nombre décimal 16777215 est converti en une adresse IPv4.

```
SET(i_integer = 167772161)
NUMTOIP(i_integer, s)
```

Contenu de la variable de sortie :

```
s = "10.0.0.1"
```

La commande IPTONUM effectue l'opération inverse en convertissant une adresse IP en un nombre. Voir IPTONUM pour plus d'informations.

PARSER_ATTACHVARIABLE

La commande PARSER_ATTACHVARIABLE permet d'associer le nom dans une paire nom-valeur à une variable target_variable.

Dans la plupart des cas, il est conseillé de créer un analyseur et d'associer une variable lors de l'initialisation en dehors de la boucle. Vous pouvez ensuite réutiliser cet analyseur dans la boucle d'analyse.

Pour plus d'informations sur les commandes d'analyse associées, voir les commandes PARSER_CREATEBASIC et PARSER_PARSESTRING.

Analyseur NVP (Name-value Pair, paire nom-valeur)

L'extrait de code suivant montre l'analyseur NVP :

```
PARSER_CREATEBASIC (h_nvp, "nvp", "separator==",
"entry_separator= ", "value_quotes=/"",
value_quotes_optional=yes")
PARSER_ATTACHVARIABLE (h_nvp,"this",s_this)
PARSER_ATTACHVARIABLE (h_nvp,"me",s_me)
PARSER_ATTACHVARIABLE (h_nvp,"hello",s_hello)
```

```
PARSER_PARSESTRING (h_nvp, "this=/”that/” me=/"you =
them/" hello=/”goodbye/”")
```

Paramètres

Les paramètres suivants sont reconnus lorsqu'ils apparaissent sous le format suivant :

```
"<paramètre>=<valeur>"
```

<paramètre> correspond à l'un des éléments cités ci-dessous, et <valeur> à une valeur appropriée pour ce paramètre.

- separator : le caractère que vous utilisez pour séparer le nom de la valeur.
- entry_separator : le caractère que vous utilisez pour séparer une paire nom-valeur de la paire suivante.
- name_quotes : le caractère que vous utilisez pour encadrer le nom (“ ou ‘, par exemple).
- value_quotes : le caractère que vous utilisez pour encadrer la valeur.
- name_quoted : défini sur oui pour que l'analyseur NVP prenne en compte l'option name_quotes.
- value_quoted : défini sur oui pour que l'analyseur NVP prenne en compte l'option value_quotes.
- name_quotes_optional : défini sur oui pour que le nom soit encadré de guillemets. Dans ce cas et si les guillemets sont omis, un espace facultatif suivi du caractère separator sont placés à la fin du nom.
- value_quotes_optional : défini sur oui pour que la valeur soit encadrée de guillemets.

Dans ce cas et si les guillemets sont omis, un espace facultatif suivi du caractère entry_separator sont placés à la fin de la valeur.

Format

```
PARSER_ATTACHVARIABLE(<parser_handle>, <name>,
<target_variable>)
```

Types de données

Argument	Type	Description
parser_handle	variable chaîne (ENTRÉE)	Variable d'identificateur de l'analyseur créé.
name	chaîne (ENTRÉE)	Nom de la paire nom-valeur.
target_variable	toute variable (SORTIE)	Variable à définir avec la valeur associée au nom de la paire nom-valeur.

L'exemple suivant porte sur l'analyseur du point de contrôle.

```
COLLECTOR SETUP STATE:
PARSER_CREATEBASIC(h_nvp,"nvp", "separator==",
"entry_separator= ", "value_quotes=/"",
"value_quotes_optional=yes")
PARSER_ATTACHVARIABLE(h_nvp,"action", s_EVT)
PARSER_ATTACHVARIABLE(h_nvp,"d_port", s_DP)
```

```
PARSER_ATTACHVARIABLE(h_nvp,"proto", s_P)
PARSER_ATTACHVARIABLE(h_nvp,"src", s_SIP)
PARSER_ATTACHVARIABLE(h_nvp,"dst", s_DIP

PARSE STATE:
PARSER_PARSESTRING(h_nvp,s_RXBufferString)
```

PARSER_CREATEBASIC

La commande PARSER_CREATEBASIC définit un analyseur et l'associe à un identificateur parser_handle. Pour plus d'informations, voir la section Analyseur NVP (Name-value Pair, paire nom-valeur) de la commande PARSER_ATTACHVARIABLE.

Dans la plupart des cas, il est conseillé de créer un analyseur et d'associer une variable lors de l'initialisation en dehors de la boucle. Vous pouvez ensuite réutiliser cet analyseur dans la boucle d'analyse.

Pour plus d'informations sur une autre commande d'analyse connexe, reportez-vous à la commande PARSER_PARSESTRING.

Format

```
PARSER_CREATEBASIC(<parser_handle>, <parser_name>, [,
<nvp> [, ...]])
```

Types de données

Argument	Type	Description
parser_handle	variable chaîne (SORTIE)	Variable qui fera désormais référence à l'analyseur.
parser_name	chaîne (ENTRÉE)	Nom de type chaîne de l'analyseur simple que vous créez. **REMARQUE :** à ce stade, seul nvp est reconnu.
nvp	chaîne (ENTRÉE) (FACULTATIF)	Paire nom-valeur. Zéro ou plusieurs chaînes contenant le nom d'une propriété, suivies du signe égal, puis d'une valeur. Les paramètres reconnus sont déterminés par l'argument parser_name choisi. **REMARQUE** : lorsque le nom de l'analyseur est défini sur nvp, vous devez utiliser les arguments suivants : "separator==" "entry_separator= " "value_quotes=/"" "value_quotes_optional=yes"

Argument	Type	Description
nvp1	chaîne (ENTRÉE) (FACULTATIF)	Paire nom-valeur 1.
nvp2	chaîne (ENTRÉE) (FACULTATIF)	Paire nom-valeur 2.
…	chaîne (ENTRÉE) (FACULTATIF)	Autres paires nom-valeur.

Pour avoir un exemple, reportez-vous à la section relative à l'exemple de l'analyseur du point de contrôle de la commande PARSER_ATTACHVARIABLE, située sous le tableau Type de données.

PARSER_NEXT

La commande PARSER_NEXT avance l'analyseur jusqu'à la position suivante dans la chaîne d'analyse en complétant les variables définies par la commande PARSER_ATTACHVARIABLE.

Format

```
PARSER_NEXT(<parser_handle>, <success_flag>)
```

Type de données

Argument	Type	Description
parser_handle	chaîne variable (ENTRÉE)	Variable d'identificateur de l'analyseur créé.
success_flag	variable numérique (numvar) (ENTRÉE)	0: échec de l'analyse 1: succès de l'analyse

PARSER_PARSESTRING

La commande PARSER_PARSESTRING traite l'argument string_to_parse à l'aide de l'analyseur créé référencé par l'argument parser_handle. De cette manière, vous pouvez construire n'importe quelle chaîne arbitraire pour l'analyse, au lieu de faire appel à une source de flux ou à la mémoire tampon de réception.

Pour plus d'informations, reportez-vous aux commandes PARSER_ATTACHVARIABLE et PARSER_CREATEBASIC.

Vous pouvez utiliser la variable réservée s_RXBufferString en tant qu'argument string_to_parse après l'état de réception pour analyser la saisie du script. Pour plus d'informations, voir la section Analyseur NVP (Name-value Pair, paire nom-valeur) de la commande PARSER_ATTACHVARIABLE.

Format

```
PARSER_PARSESTRING(<parser_handle>, <string_to_parse>)
```

Types de données

Argument	Type	Description
parser_handle	variable chaîne (ENTRÉE)	Variable d'identificateur de l'analyseur créé.
string_to_parse	variable (ENTRÉE)	Unique chaîne qui sera traitée par cet analyseur.

Pour avoir un exemple, reportez-vous à la section relative à l'exemple de l'analyseur du point de contrôle de la commande PARSER_ATTACHVARIABLE, située sous le tableau Type de données.

PAUSE

La commande PAUSE permet de suspendre immédiatement le script en cours pendant « n » secondes. Cette commande fonctionne entre les instructions d'une d'analyse et entre les différents états. Elle est utile pour définir des cycles d'interrogation ou pour garantir une fréquence raisonnable des interrogations (lors des interrogations d'un fichier journal de base de données par exemple).

Au cours de l'analyse, vous pouvez spécifier plusieurs commandes PAUSE.

Format

```
PAUSE(iseconds)
```

Argument	Type	Description
iseconds	numérique (ENTRÉE)	Durée de l'interruption en secondes avant de passer à l'état suivant.

Par exemple :

```
PAUSE(10)
PAUSE(iseconds)
```

Ou

```
IF(slowing=true)
PAUSE(50)
ENDIF( )
```

POPUP

La commande POPUP affiche
le contenu d'une chaîne à l'écran dans une fenêtre de texte contextuelle.

Format

```
POPUP(data [, title])
```

Types de données

Argument	Type	Description
data	chaîne (ENTRÉE)	Données de type chaîne à afficher dans la fenêtre contextuelle.
title	chaîne (ENTRÉE) [FACULTATIF]	Chaîne à utiliser comme titre de la fenêtre contextuelle (par défaut = “Popup DATA”).

Par exemple :

```
POPUP(data)
POPUP("Hello World", "Title String")
POPUP(data, title)
```

PRINTF

La commande PRINTF copie les données formatées dans une variable chaîne (svar). Il s'agit d'une commande d'analyse avancée. Si vous êtes peu familier du langage de commande d'analyse, utilisez plutôt les commandes COPY et APPEND jusqu'à ce que vous soyez familiarisé avec ce langage.

Lors de l'utilisation de cette commande :

- Indiquez une variable svar comme chaîne de destination.
- Indiquez la chaîne format.
- Indiquez tout paramètre supplémentaire facultatif à analyser en fonction de la chaîne format.

Chaîne format

Pour utiliser des données hexadécimales dans la chaîne format, appliquez la convention suivante :

```
\HX HX HX\
```

Pour inclure un saut de ligne à la fin de cette chaîne, cette dernière doit ressembler à ceci :

```
Chaîne format\0a\
```

Pour un retour chariot : \0d0a\. Par exemple :

```
PRINTF(message,"Voltage is %lf \0d0a\",f_volts)
```

Pour une tabulation : \09\. Par exemple :

```
PRINTF(message,"Voltage = \09\ %lf",f_volts)
```

Format

```
PRINTF(dest, format [, <paramList>])
```

où :

```
<paramList> ::= var [, <paramList>]
```

Types de données

Argument	Type	Description
dest	svar (SORTIE)	Variable chaîne de destination dans laquelle placer la chaîne formatée.
format	chaîne (ENTRÉE)	Format de la chaîne à copier dans la variable chaîne de destination. Similaire au format de la commande C printf. Par exemple, « Looping %d in %s » (voir Caractères % du format de sortie).
parm1	tous (ENTRÉE) [FACULTATIF]	Tous les types de données à l'exception des tableaux. Doit correspondre à la chaîne format.
parm2	tous (ENTRÉE) [FACULTATIF]	Tous les types de données à l'exception des tableaux. Doit correspondre à la chaîne format.
…	tous (ENTRÉE) [FACULTATIF]	Tous les types de données à l'exception des tableaux. Doit correspondre à la chaîne format.

Format

```
Caractères % du format de sortie
```

Caractère	Type	Format de sortie
%d	entier	Entier décimal signé.
%le	flottant	Valeur signée au format [-]d.dddd e [signe]ddd ...où d correspond à un seul chiffre décimal, dddd un ou plusieurs chiffres décimaux, ddd trois chiffres décimaux et signe le signe + ou -.
%lf	flottant	Valeur signée au format [-]dddd.dddd ...où dddd représente un ou plusieurs chiffres décimaux. Le nombre de chiffres précédant le point décimal dépend de la grandeur du nombre et le nombre de chiffres suivant ce même point dépend de la précision à atteindre.

Caractère	Type	Format de sortie
%lg	flottant	Valeur signée écrite au format f ou e, en fonction de celui qui correspond le mieux à la valeur et à la précision données. Le format e n'est utilisé que lorsque l'exposant de la valeur est inférieur à -4 ou supérieur ou égal à l'argument de précision. Les zéros de fin sont tronqués et le point décimal s'affiche uniquement si un ou plusieurs chiffres le suivent.
%s	chaîne	Écrit une variable chaîne.

Affichage des chiffres liés à la précision

Par défaut, la commande PRINTF affiche un nombre à virgule flottante avec une précision de six chiffres. Cette précision par défaut s'applique également aux nombres en double précision.

Pour afficher des chiffres supplémentaires, indiquez une valeur pour le champ de précision dans la spécification du format PRINTF() :

```
%[<width>][.<precision>] type>
```

Par exemple :

```
PRINTF(dest, "%2.3lf", fvar)
```

Donnerait la sortie : 22.012, correspondant à 2 positions à gauche du point décimal et à 3 positions à droite du point décimal.

Les exemples suivants montrent comment transmettre des variables chaînes et entières.

```
PRINTF(dest,format_string) PRINTF(mystring,
"val of matrix[%d][%d] = %s",
index_x, index_y, matrix[index_x][index_y])
PRINTF(dest,"Looping %d in state %s",iloop,state)
PRINTF(dest,"Formatted %s Data into
%s","string","dest")
```

L'exemple suivant montre comment transmettre une variable flottante à une chaîne.

```
PRINTF(message,"Voltage is %lf",f_volts)
```

Pour imprimer des nombres à virgule flottante, utilisez %lf ou %le.

REGEXPREPLACE

La commande REGEXPREPLACE recherche des chaînes et les remplace, à l'aide d'expressions régulières. Lorsqu'une chaîne est trouvée, elle est remplacée par la chaîne regexpreplace.
La commande REGEXPREPLACE procède à un remplacement global et non uniquement au remplacement de la première occurrence.

Format

```
REGEXPREPLACE(dest_string, search, replace)
```

Types de données

Argument	Type	Description
dest_string	svar (ENTRÉE/ SORTIE)	Variable chaîne qui comporte des octets à remplacer.
search	chaîne (ENTRÉE) ou svar (ENTRÉE/ SORTIE)	Chaîne de recherche à remplacer.
replace	chaîne (ENTRÉE) Ou svar (ENTRÉE/ SORTIE)	Chaîne de remplacement. Elle peut être de longueur zéro pour indiquer une chaîne null.

Par exemple :

```
COPY(string:"The 1st time")
REGEXREPLACE(string, "1st", "2nd")
```

Résultat :

```
string = "The 2nd time"
```

REMARQUE : dans cet exemple, vous pouvez utiliser une expression régulière pour remplacer la chaîne

```
“1st”.
```

Pour remplacer par une chaîne null

```
COPY(string:"The 1st time")
REGEXPREPLACE(string, "1st", "")
```

Résultat :

```
string="The time"
```

Pour plus d'informations sur les expressions régulières et le jeu de caractères portable, voir la section relative aux expressions régulières.

Sentinel utilise une bibliothèque d'expressions régulières compatible avec la norme POSIX (Portable Operating System Interface for UNIX). POSIX est un ensemble de normes IEEE et ISO qui garantit la compatibilité entre les systèmes d'exploitation POSIX englobant la plupart des variétés d'UNIX.

REGEXPSEARCH, REGEXPSEARCH_EXPLICIT ou REGEXPSEARCH_STRING

La commande REGEXPSEARCH effectue une recherche vers l'avant dans le tampon de réception (Rx Buffer) ou dans la variable chaîne d'entrée désignée, à l'aide d'expressions régulières. Elle prend également en charge les groupes d'expressions.

REMARQUE : au sein de l'éditeur plein écran du Générateur de collecteurs, les commandes REGEXPSEARCH, REGEXPSEARCH_EXPLICIT ou REGEXPSEARCH_STRING sont répertoriées en tant que commandes distinctes. Il s'agit en fait d'une seule et même commande. Elles sont indiquées pour décrire différentes variantes de la même commande. Si vous deviez utiliser REGEXPSEARCH_EXPLICIT ou REGEXPSEARCH_STRING dans l'éditeur de texte, vous entreriez REGEXPSEARCH.

Tampon de réception

La recherche dans le tampon de réception fonctionne comme suit :

- La recherche débute au niveau de la position actuelle du pointeur Rx Buffer et se poursuit vers l'avant jusqu'à ce que la chaîne recherchée soit trouvée, ou jusqu'à ce que la recherche atteigne la fin du tampon de réception.
- Si la recherche aboutit, le pointeur Rx Buffer est mis à jour pour indiquer le premier octet de la chaîne recherchée. Cette position est conservée quels que soient les états, à moins d'un changement explicite demandé par la commande RESET.
- Si la recherche n'aboutit pas, le pointeur Rx Buffer reste à sa position actuelle.

Lorsque vous utilisez cette commande pour effectuer une recherche dans le tampon de réception, le deuxième paramètre facultatif est une variable entière définie sur 1 si la recherche aboutit, ou sur 0 si la recherche échoue.

Variable chaîne

Les variables chaînes ne prennent pas en charge le pointeur d'analyse, la dynamique est donc différente lors de la recherche dans une variable chaîne. Le modèle d'expression régulière correspondra à une partie ou à l'intégralité de la chaîne d'entrée. S'il est configuré avec des groupes d'expressions, il est possible de stocker le contenu de la chaîne d'entréeb correspondant aux groupes d'expressions dans les variables de sortie. Il existe deux options de sortie pour les groupes d'expressions. La première consiste à remplir la liste des variables dans l'ordre des groupes d'expressions, et l'autre à désigner un tableau de chaînes.

Si l'expression régulière correspond à l'entrée (variable chaîne), une liste désignée de variables ou le tableau de sortie est défini avec les valeurs du groupe, et la variable recherchée est définie sur le nombre de groupes incrémenté de un ou sur zéro en cas d'échec de correspondance.

Lorsque la sortie des valeurs du groupe doit être un tableau de chaînes, le premier élément indexé avec 0 contient la chaîne recherchée. La chaîne recherchée contient le contenu correspondant à l'expression régulière dans son intégralité, indépendamment des groupes d'expressions. Ainsi, le contenu du premier groupe d'expressions est stocké dans la position indexée avec 1 dans le tableau. Lors d'un tour de boucle dans le tableau de sortie, la valeur i_Found_Tokens donne toujours le nombre total de groupes incrémenté de un, car elle compense le fait que le premier élément correspond à la chaîne recherchée. Dans une boucle

for, la condition d'arrêt de la boucle qui est réalisée lorsque la valeur est inférieure à la valeur i_Found_Tokens fonctionne toujours, mais vous devrez probablement commencer votre index à « 1 » au lieu de « 0 ».

Lorsque les valeurs de groupe doivent être stockées dans une liste de variables de sortie au lieu d'un tableau, la commande est à même de réaliser des conversions de types. Bien que la chaîne d'entrée soit de type chaîne, ses composants peuvent être de type numérique. Si ces numéraux doivent être considérés comme des valeurs entières ou à virgule flottante, le fait de désigner les variables de sortie dans le type approprié entraîne une conversion.

Correspondance REGEX simple

Expression	Description
.	Tout caractère
\d	Tout chiffre
\w	Tout caractère alphanumérique
\s	Tout espace blanc
+	1 fois ou plus que la valeur précédente
*	0 fois ou plus que la valeur précédente

Format

Pour le tampon de réception :

```
REGEXPSEARCH(search[, ifound])
```

Pour une variable chaîne :

```
REGEXPSEARCH(Input_String, s_Regular_Exp_Pattern,
i_Found_Tokens[, s_Output_Results[]])
REGEXPSEARCH(s_Input_String, s_Regular_Exp_Pattern,
i_Found_Tokens, s_Match[, var1, var2, ...)]
```

Types de données

Argument	Type	Description
s_Input_String	Chaîne ou variable chaîne (ENTRÉE) [FACULTATIF]	Chaîne ou variable chaîne à rechercher lors de la correspondance regex spécifiée dans la commande regex.
s_Regular_Exp_Pattern	Chaîne (ENTRÉE)	Chaîne à rechercher dans le tampon de réception (à partir de la position du pointeur Rx Buffer vers l'avant), un littéral de chaîne d'entrée, ou une variable chaîne d'entrée.

Argument	Type	Description
i_Found_Tokens	variable numérique (numvar) (SORTIE) [FACULTATIF]	Retourne un résultat en fonction du succès ou de l'échec de la recherche. 0: le modèle d'expression régulière n'a pas de correspondance. 1: le modèle correspond, mais aucun groupe d'expressions n'est désigné. 2: le modèle correspond avec 1 groupe d'expressions désigné. N+1 : le modèle correspond avec N groupes d'expressions désignés. **REMARQUE :** la variable I_found_tokens peut servir de test, car la valeur sera différente de zéro en cas de correspondance avec l'expression régulière.
s_Match	Chaîne (SORTIE) [CONDITIONNEL]	Cet argument n'est rempli qu'en cas de correspondance. Il doit être indiqué lorsqu'une liste de variables de sortie de groupes d'expressions est utilisée. Lorsque les valeurs de groupe sont stockées dans un tableau de sortie, s_Match N'est PAS un paramètre valide.
Liste de variables OU s_Output_Results[]	Tout type possible (SORTIE) [FACULTATIF] OU Tableau de chaînes (SORTIE) [FACULTATIF]	Liste des variables dans laquelle placer les valeurs de groupe. L'affectation des valeurs s'effectue dans l'ordre des valeurs de groupe désignées lorsque des règles de priorité sont appliquées.

Dans les exemples suivants, la recherche porte sur un retour chariot et un saut de ligne dans le tampon de réception :

```
REGEXPSEARCH("\0d0a\")
```

Dans l'exemple suivant, la recherche porte sur le mot « alarm » dans le tampon de réception :

```
REGEXPSEARCH("alarm")
```

REMARQUE : en cas de remplacement hexadécimal, \0000\ termine une chaîne. Ainsi, « xxxx\0000\yyyy » devient « xxxx ».

Voici un exemple détaillé de la recherche d'un modèle dans une valeur de chaîne littérale :

```
REGEXPSEARCH("2003 Jan 15 13:34:20",
"(/\d+)/\s+(/\w+)/\s+(/\d+)/\s+(/\d+):(/\d+):(/\d+)",
i_Success, s_Match, s_Year, s_Month, s_Day, s_Hour,
s_Minute, s_Second)
```

où,

```
i_Success = 7
s_Match = 2003 Jan 15 13:34:20
s_Year = 2003
s_Month = Jan
s_Day = 15
s_Hour = 13
s_Minute = 34
s_Second = 20
```

Pour plus d'informations sur les expressions régulières et le jeu de caractères portable, voir la section relative aux expressions régulières du chapitre 2.

Sentinel utilise une bibliothèque d'expressions régulières compatible avec la norme POSIX (Portable Operating System Interface for UNIX). POSIX est un ensemble de normes IEEE et ISO qui garantit la compatibilité entre les systèmes d'exploitation POSIX englobant la plupart des variétés d'UNIX.

REPLACE

La commande REPLACE recherche et remplace des chaînes.

Lorsqu'une chaîne est trouvée, elle est remplacée par la chaîne de remplacement. La commande REPLACE procède à un remplacement global et non uniquement au remplacement de la première occurrence.

Format

```
REPLACE(dest_string, search, replace)
```

Types de données

Argument	Type	Description
dest_string	svar (ENTRÉE/ SORTIE)	Variable chaîne qui comporte des octets à remplacer.
search	chaîne (ENTRÉE)	Chaîne de recherche à remplacer.
replace	chaîne (ENTRÉE)	Chaîne de remplacement.

Par exemple :

```
COPY(string:"The 1st time")
REPLACE(string, "1st", "2nd")
```

Résultat :

```
string = "The 2nd time"
```

REMARQUE : dans cet exemple, vous pouvez utiliser une expression régulière pour remplacer la chaîne “1st”.

RESET

La commande RESET réinitialise le pointeur Rx Buffer sur zéro.

Format

```
RESET()
```

Dans l'exemple, le symbole ^ indique la position du pointeur Rx Buffer.

```
rxbuff = "abcdefg"
                ^
RESET()
```

Résultat :

```
"abcdefg"
 ^
```

RXBUFF

La commande RXBUFF écrase les données du tampon de réception avec le contenu d'une variable chaîne ou d'une chaîne entre guillemets. Le contenu du tampon de réception est immédiatement modifié et le pointeur Rx Buffer est réinitialisé sur zéro.

Format

```
RXBUFF(s_data)
```

Types de données

Argument	Type	Description
s_data	chaîne (ENTRÉE)	Chaîne de données à écrire dans le tampon de réception. Elle remplace immédiatement l'ancien contenu du tampon de réception.

Par exemple :

Dans l'exemple suivant, la commande FILER lit un fichier appelé alert.data et place son contenu dans une variable chaîne nommée s_data. Cet exemple se base sur l'hypothèse suivante :

```
alert.data: "Minor Alarm Xterminal A"
```

Ensuite, la commande RXBUFF place les données dans le tampon de réception, exactement comme si ces données provenaient d'un port.

```
FILER("alert.data", s_data)
RXBUFF(s_data)
//copies data from Rx BUFFER into S_Alarm_Priority,
stopping before the string "Alarm")
COPY(S_Alarm_Priority:," Alarm")
```

Résultat :

```
S_Alarm_Priority= "Minor"
```

SEARCH

La commande SEARCH recherche une chaîne vers l'avant dans le tampon de réception (Rx Buffer).

La recherche se déroule comme suit :

- La recherche débute au niveau de la position actuelle du pointeur Rx Buffer et se poursuit vers l'avant jusqu'à ce que la chaîne recherchée soit trouvée, ou jusqu'à ce que la recherche atteigne la fin du tampon de réception.
- Si la recherche aboutit, le pointeur Rx Buffer est mis à jour pour indiquer le premier octet de la chaîne recherchée. Cette position est conservée quels que soient les états, à moins d'un changement explicite demandé par la commande RESET.
- Si la recherche n'aboutit pas, le pointeur Rx Buffer reste à sa position actuelle.

Lorsque vous utilisez cette commande, le deuxième paramètre facultatif est une variable entière définie sur 1 si la recherche aboutit, et sur 0 si elle échoue.

Format

```
SEARCH(search[, ifound])
```

Types de données

Argument	Type	Description
search	chaîne (ENTRÉE)	Chaîne à rechercher dans le tampon de réception, en commençant à partir de la position actuelle du pointeur Rx Buffer vers l'avant.
ifound	variable numérique (numvar) (SORTIE) [FACULTATIF]	Retourne un résultat en fonction du succès ou de l'échec de la recherche. 0= échec 1= succès

Par exemple :

Dans les exemples suivants, la recherche porte sur un retour chariot et un saut de ligne :

```
SEARCH("\0d0a\")
SEARCH(data, ifound)
```

Dans l'exemple suivant, la recherche porte sur le mot « alarm » :

```
SEARCH("alarm")
```

REMARQUE : en cas de remplacement hexadécimal, \0000\ termine une chaîne. Ainsi, « xxxx\0000\yyyy » devient « xxxx ».

SET

La commande SET évalue une expression mathématique et met à jour une valeur numérique (numvar) avec le résultat de l'évaluation.

Lors de l'utilisation de cette commande :

- Indiquez une variable numérique de destination, suivie du signe égal et de toute combinaison des caractères ( ) - + * /, numéraux et variables numériques.
- Vous devez spécifier au moins une valeur numérique à droite du signe égal.
- Vous pouvez utiliser autant de parenthèses que nécessaire.
- Tous les arguments sont convertis en une valeur flottante. Le résultat est converti dans le type (entier ou flottant) de la variable numérique de destination.
- Vous pouvez saisir jusqu'à 98 entrées après le signe égal, dont : (,), *, /, +, -, tout nombre et toute variable numérique.
- Lorsque les opérations sont de même niveau, elles sont évaluées de gauche à droite. L'ordre est décrit dans le tableau ci-dessous.

Niveau 1	:	()	Par exemple : parenthèses
Niveau 2	:	*/	Par exemple : multiplication, division
Niveau 3	:	+ -	Par exemple : addition, soustraction

Format

```
SET(idest = <expr>) ou SET(fdest = <expr>)
```

Où :

```
set_command ::= SET(<idest>=<expr>) |
SET(<fdest>=<expr>)
expr ::= (<expr>)
         | expr ( '+' | '-' | '*' | '/' ) expr
         | ivar | fvar | number
```

Type de données

Argument	Type	Description
idest	variable numérique (numvar) (SORTIE)	Variable numérique (fvar ou ivar) dans laquelle est enregistrée la valeur.
inum1	numérique (ENTRÉE)	Variable fvar, ivar ou un nombre.
inum2	numérique (ENTRÉE) [FACULTATIF]	Variable fvar, ivar ou un nombre.
inum3	numérique (ENTRÉE) [FACULTATIF]	Variable fvar, ivar ou un nombre.
…	numérique (ENTRÉE) [FACULTATIF]	Variable fvar, ivar ou un nombre.

Par exemple :

```
SET(idest=inum1)
SET(i_loop=10)
SET(idest=inum1+inum2)
SET(idest=(inum1+inum2) * inum3)
SET(i_counter=i_counter+1)
SET(i_val = (ivar)*(ivar/3) + 15/fvar - (5 +
20/iloop))
```

SETBYTES

La commande SETBYTES vous permet de définir des octets d'une variable chaîne sur une valeur particulière, transmise soit en tant qu'entier, soit en tant que chaîne. Si un entier est transmis, la plage des valeurs correcte est comprise entre 0 et 255. Si c'est une chaîne, elle est placée au niveau de la position de l'index dans la variable chaîne de destination.

Format

```
SETBYTES(dest_string, index, replace)
```

Types de données

Argument	Type	Description
dest_string	svar (ENTRÉE/ SORTIE)	Variable chaîne qui comporte des octets à remplacer.
index	numérique (ENTRÉE)	Index (le premier octet commençant à 0) dans dest_string au niveau duquel seront placées les valeurs de remplacement.

Argument	Type	Description
replace	chaîne (ENTRÉE) Ou entier (ENTRÉE)	Octets qui seront écrits dans dest_string. La valeur à définir pour l'octet #n de l'index dans la chaîne de destination.

Par exemple :

```
COPY(string:"Bandwidth Util. = 22%")
SETBYTES(string, 18, "44")
```

Contenu des variables de sortie :

```
string = "Bandwidth Util. = 44%"
```

SETCONFIG

Cette commande permet de définir une propriété système. Vous pouvez ensuite récupérer ce paramétrage avec la commande GETCONFIG. Ces commandes permettent de définir des propriétés système et de récupérer les valeurs actuelles des propriétés système susceptibles de changer de manière périodique, comme un fichier journal qui est renommé quotidiennement avec la date du jour.

Les propriétés système disponibles sont les suivantes :

Propriété système	Exemple(s)
▪ System.OS.Family	Solaris et Windows
▪ System.OS.Name	Windows 2000
▪ System.OS.Version.Major	5
▪ System.OS.Version.Minor	0
▪ System.Net.Hostname	ESECServer
▪ System.Net.IP_List	liste des adresses IP de cet hôte séparées par un point-virgule, comme « 172.163.3.45;172.45.2.1 ».

Voir également la commande GETCONFIG.

Cette commande comprend deux paramètres obligatoires.

- Le premier paramètre définit l'option de configuration (FileConnector.InputFile ou FileConnector.OutputFile).
- Le deuxième définit la valeur de configuration.

Format

```
SETCONFIG(Config Option, Value)
```

Types de données

Argument	Type	Description
Config Option	chaîne (ENTRÉE)	Nom de la variable de configuration à définir. Fichier en entrée = “FileConnector.InputFile” Fichier de sortie = “FileConnector.OutputFile”
Value	chaîne svar (ENTRÉE)	Paramètre de configuration.

Par exemple :

```
SETCONFIG(“FileConnector.InputFile”, s_inputfilename)
SETCONFIG(“FileConnector.OutputFile”,
s_outputfilename)
```

Contenu des variables de sortie :

```
“C:/\test.dat”
```

SHELL

La commande SHELL exécute
une commande ou un script de shell.

Format

```
SHELL(command [, wait_parameter][,
wait_return_status])
```

Types de données

Argument	Type	Description
command	chaîne (ENTRÉE)	Chemin et nom du fichier de la commande à exécuter. Par défaut, la variable d'environnement PATH est utilisée.
wait/no_wait	variable numérique (numvar) [FACULTATIF]	Permet à la commande SHELL d'attendre (ou non) l'exécution complète du programme lancé avant de poursuivre. 0 = pas d'attente 1 = attend la fin du programme

Argument	Type	Description
return_status	variable numérique (numvar) [FACULTATIF]	Valeur numérique lorsque l'option d'attente est utilisée. SUCCÈS = 1 ÉCHEC = 0

Dans l'exemple suivant, un fichier de traitement par lots PC ou un script de shell UNIX est initié :

```
SHELL("device_poll")
```

L'exemple suivant lance le Bloc-notes :

```
SHELL("c:/\winnt/\system32/\notepad.exe")
```

L'exemple suivant permet d'attendre la fin de l'exécution de la commande d'horloge :

```
SHELL("clock",1)
```

L'exemple suivant permet d'attendre la fin de l'exécution d'un fichier de traitement par lots PC ou d'un script de shell UNIX, puis de renvoyer le résultat :

```
SHELL("device_poll",1,i_ret)
```

L'exemple suivant permet d'exécuter le processus d'horloge sans attendre qu'il soit terminé :

```
SHELL("clock",0)
```

SKIP

La commande SKIP ajoute un nombre à la valeur du pointeur Rx Buffer.

Il peut s'agir d'un nombre positif ou négatif. Si la position du pointeur obtenue est inférieure à zéro, le pointeur Rx Buffer est défini sur zéro. Si elle va au-delà du tampon de réception, le pointeur est défini de façon à pointer vers le dernier octet du tampon.

Format

```
SKIP([+ | -] iskip_amount)
```

Types de données

Argument	Type	Description
iskip_amount	numérique (ENTRÉE)	Nombre d'octets correspondant au déplacement du pointeur.

Par exemple :

```
SKIP(iskip_amount)
SKIP(+iskip_amount)
SKIP(-iskip_amount)
SKIP(5)
SKIP(-1)
```

Les exemples suivants montrent la position du pointeur Rx Buffer après l'exécution d'une commande skip :

```
aaaaaa bbbbb c d ee
      ^

SKIP(-2)
aaaaaa bbbbb c d ee
    ^

SKIP(-1)
aaaaaa bbbbb c d ee
     ^

SKIP(0)
aaaaaa bbbbb c d ee
      ^

SKIP(1)
aaaaaa bbbbb c d ee
       ^
SKIP(2)
aaaaaa bbbbb c d ee
        ^

SKIP(3)
aaaaaa bbbbb c d ee
         ^

SKIP(4)
aaaaaa bbbbb c d ee
          ^

SKIP(8)
aaaaaa bbbbb c d ee
              ^
```

SKIPWORD

La commande SKIPWORD modifie le pointeur Rx Buffer de sorte qu'il pointe vers le début d'un mot.

Pour cette commande, toute séquence d'octets imprimables consécutifs séparée par au moins un octet non imprimable est considérée comme un mot. Les octets imprimables relèvent du codage ASCII et ASCII-0-255 étendu (d'après ISO 8859-1).

À l'aide de valeurs positives ou négatives, le pointeur Rx Buffer se déplace dans le tampon de réception jusqu'au premier octet imprimable ou jusqu'à l'octet imprimable suivant.

Le pointeur ne peut se déplacer au-delà de la fin du tampon de réception ni en deçà du début, et ce même si la commande SKIPWORD le demande.

La valeur zéro n'entraîne pas de changement pour le pointeur Rx Buffer. La commande SKIPWORD considère tous les caractères inférieurs à 33 et entre 126 et 161 comme des espaces blancs.

Format

```
SKIPWORD([+ | -] iwords)
```

Types de données

Argument	Type	Description
iwords	numérique (ENTRÉE)	Nombre de mots définissant le déplacement du pointeur Rx Buffer dans le tampon de réception.

Par exemple :

```
SKIPWORD(iwords)
SKIPWORD(3)
SKIPWORD(+iwords)
SKIPWORD(-iwords)
SKIPWORD(-4)
```

Les exemples suivants montrent la position du pointeur Rx Buffer après l'exécution d'une commande SKIPWORD :

```
aaaaaa bbbbb c d ee
      ^

SKIPWORD(-2)
aaaaaa bbbbb c d ee
^

SKIPWORD(-1)
aaaaaa bbbbb c d ee
^
```

```
SKIPWORD(0)
aaaaaa bbbbb c d ee
      ^

SKIPWORD(1)
aaaaaa bbbbb c d ee
       ^

SKIPWORD(2)
aaaaaa bbbbb c d ee
            ^

SKIPWORD(3)
aaaaaa bbbbb c d ee
              ^

SKIPWORD(4)
aaaaaa bbbbb c d ee
                ^

SKIPWORD(5)
aaaaaa bbbbb c d ee
                 ^
```

SOCKETW

La commande SOCKETW exécute des opérations non exclusives (socket réseau utilisé dans les flux d'octets) d'ouverture, de connexion et d'écriture de données dans un socket (port IP et TCP) avant de fermer le socket. Elle peut éventuellement retourner le statut de la tentative d'écriture dans le socket.

Format

```
SOCKETW(address, i_port, data [, istat])
```

Types de données

Argument	Type	Description
address	chaîne (ENTRÉE)	Adresse IP du socket.
i_port	numérique (ENTRÉE)	Numéro de port TCP du socket.
data	chaîne (ENTRÉE)	Chaîne de données à écrire dans le socket.

Argument	Type	Description
istat	variable numérique (numvar) (SORTIE)	Statut facultatif éventuellement retourné. istat = Nombre d'octets écrits ; > 0 (SUCCÈS) istat = 0 (ÉCHEC)

Exemples :

```
SOCKETW("192.168.15.25", 5051, "Data Write Socket")
SOCKETW("192.168.15.25", i_port, "Data to Socket\0d\")
SOCKETW(s_ip_address, i_port, "\54AF0D0B91\",
i_status)
SOCKETW(s_ip_address, i_port, "\54AF0D0B91\",
f_status)
SOCKETW(s_ip_address, 6004, "\54AF0D0B91\", f_status)
SOCKETW(s_ip_address, 6004,sdata, f_status)
```

STONUM

La commande STONUM (chaîne vers nombre) convertit une variable chaîne (svar) en une variable numérique (numvar).

ATTENTION : les variables chaînes autres que les représentations sous forme de chaîne d'une valeur entière ou flottante peuvent donner des résultats imprévisibles. Toutes les valeurs entières sont limitées à 2147483647 ; toute valeur supérieure est tronquée (2147483647).

Format

```
STONUM(string, ivar)
```

Types de données

Argument	Type	Description
inum	variable numérique (numvar) (SORTIE)	Variable numérique dans laquelle est enregistré le nombre (fvar ou ivar).
chaîne	chaîne (ENTRÉE)	Représentation d'un nombre sous forme de chaîne (par exemple : “306”).

Par exemple :

```
STONUM(source, idest)
STONUM(string_number, ivar)
STONUM("6512", ivar)
```

STRIP ou STRIP-ASCII-RANGE


La commande STRIP supprime toutes les occurrences d'une chaîne ou d'une plage de valeurs ASCII de la variable svar. La commande STRIP effectue toujours plusieurs passages jusqu'à ce que la chaîne à supprimer ou la plage de valeurs ASCII soient introuvables dans la variable chaîne de destination.

Lorsque vous utilisez cette commande, indiquez la variable chaîne à partir de laquelle supprimer les caractères. Les autres paramètres peuvent être une chaîne ou les valeurs de début et de fin d'une plage numérique.

> **REMARQUE :** au sein de l'éditeur plein écran du Générateur de collecteurs, les commandes STRIP et STRIP-ASCII-RANGE sont répertoriées en tant que commandes distinctes. Il s'agit en fait d'une seule et même commande. Elles sont indiquées pour décrire différentes variantes de la même commande. Si vous deviez utiliser la commande STRIP-ASCII-RANGE dans l'éditeur de texte, vous entreriez STRIP.

Format

```
STRIP(dest, strip)
STRIP(dest, start ASCII range, stop ASCII range)
```

Types de données

Argument	Type	Description
dest	svar (ENTRÉE/ SORTIE)	Variable chaîne contenant les données à supprimer en fonction du deuxième argument.
strip ou start ASCII range	chaîne ou numérique (ENTRÉE)	Chaîne ou valeur ASCII de début à supprimer de la chaîne de destination (dest).
stop ASCII range	numérique (ENTRÉE [facultatif])	Valeur ASCII de fin. **REMARQUE** : si la valeur ASCII de début est spécifiée, vous devez également indiquer ce paramètre.

Les exemples suivants impliquent plusieurs passages pour la suppression.

```
COPY(test:"THHELLOE")
STRIP(test, "HELLO")
```

Après exécution de la commande STRIP(), la variable test prend la valeur THE.

```
COPY(test2:"ABCDDEDDDFGDDH")
STRIP(test2, "D")
```

Après exécution de la commande STRIP(), la variable test2 prend la valeur ABCEFGH.

```
COPY(test3:"ABCDDEDDDFGDDH")
STRIP(test3, 68, 69)
```

Après exécution de la commande STRIP(), la variable test3 prend la valeur ABCFGH.

TBOSSETCOMMAND

La commande TBOSSETCOMMAND construit un paquet de commande TBOS à 3 octets à transmettre à un périphérique à l'aide du protocole TBOS.

Les numéros de commande et d'affichage TBOS ainsi que le type de commande permettent de placer le bon paquet TBOS (3 octets) dans la variable chaîne de sortie. Le format du paquet TBOS créé à l'aide de cette commande d'analyse est décrit dans les tableaux ci-dessous relatifs aux requêtes de commandes distantes.

Caractère 1		
Numéro(s) de bit	**Valeur**	**Signification**
8 7	0 1	Code d'opération : 01 = Requête de commande distante (caractère 1)
6 5 4	MSB LSB	Numéro d'affichage : 000 = No. 1 001 = No. 2 ... 111 = No. 7
3	0	Aucune signification
2 1	MSB LSB	Type : 00 = momentané 01 = verrouillé 10 = déverrouillé

Caractère 2		
Numéro(s) de bit	**Valeur**	**Signification**
8 7	1 0	Code d'opération : 10 = Requête de commande distante (caractère 2)
6 5 4 3 2 1	MSB LSB	Numéro de commande distante : 000000 = No. 1 000001 = No. 2 ... 111111 = No. 63

Caractère 3		
Numéro(s) de bit	**Valeur**	**Signification**

Caractère 3		
Numéro(s) de bit	**Valeur**	**Signification**
8 7 6 5 4 3 2 1	1 1 0 0 1 1 0 0	Écho du caractère : La réponse à la commande distante est l'écho de cet octet sur le port.

Format

```
TBOSSETCOMMAND(cmd_bytes, idisp_num, icmd_num, type)
```

Types de données

Argument	Type	Description
cmd_bytes	svar (SORTIE)	Octets de données hexadécimales (3 octets au total) qui seront placés dans cette variable chaîne et susceptibles d'être transmis au périphérique TBOS dans la zone Next State Transmit (Transmission de l'état suivant).
idisp_num	numérique (ENTRÉE)	Numéro d'affichage TBOS (ou adresse) du périphérique (1 - 8). **REMARQUE :** les plages valides pour ce paramètre vont de 1 à 8 uniquement ; pour toute autre valeur, la sortie (cmd_bytes) est définie sur des zéros, « \00 00 00\ ».
i_cmd_num	numérique (ENTRÉE)	Numéro de commande TBOS (1 à 64). **REMARQUE :** les plages valides pour ce paramètre vont de 1 à 64 uniquement ; pour toute autre valeur, la sortie (cmd_bytes) est définie sur des zéros, « \00 00 00\ ».

Argument	Type	Description
type	numérique (ENTRÉE) Ou chaîne (ENTRÉE)	Type de commande TBOS (0 à 2) : 0 = momentané 1 = verrouillé 2 = déverrouillé **REMARQUE :** les plages valides pour ce paramètre vont de 0 à 2 uniquement ; pour toute autre valeur, le type est défini par défaut sur 0 = momentané. Type de commande TBOS au format chaîne. « momentary » ou « m » = momentané « latch » ou « l » = verrouillé « unlatch » ou « u » = déverrouillé La distinction majuscules/minuscules n'est pas faite pour cette chaîne.

Par exemple :

```
TBOSSETCOMMAND(string_cmd_bytes, 1, 1, 0)
TBOSSETCOMMAND(s_bytes, 1, 1, "latch")
TBOSSETCOMMAND(s_bytes, i_display, i_cmd_num, "U")
TBOSSETCOMMAND(s_bytes, i_display, i_cmd_num, 2)
TBOSSETCOMMAND(s_bytes, 1, 1, "momentary")
TBOSSETCOMMAND(s_bytes, 1, 1, "latch")
```

Pensez à vérifier si la sortie cmd_bytes est définie sur « \00 00 00\ » afin de contrôler la présence éventuelle d'erreurs liées à des saisies hors plage. Par exemple :

```
TBOSSETCOMMAND(cmd_bytes, i_display, i_cmd_num, "M")
IF(cmd_bytes = "\00 00 00\") /* INPUTS OUT OF RANGE */
...
ENDIF()
```

L'exemple suivant permet de créer une commande TBOS avec le numéro d'affichage 5, le numéro de commande 33 et le type déverrouillé.

```
TBOSSETCOMMAND(sbytes, 5, 33, 2)
```

Contenu des variables de sortie :

```
sbytes = "\ba0 cc\"
```

TBOSSETREQUEST

La commande TBOSSETREQUEST construit un paquet de requête TBOS à 1 octet susceptible d'être transmis à un périphérique à l'aide du protocole TBOS. Les numéros de requête et d'affichage TBOS permettent de placer le bon paquet de requête TBOS (1 octet) dans la variable chaîne de sortie. Le format du paquet TBOS créé à l'aide de cette commande d'analyse est décrit dans les tableaux ci-dessous relatifs aux requêtes et réponses d'analyse des caractères.

Caractère 1 : requête d'analyse de caractères		
Numéro(s) de bit	**Valeur**	**Signification**
8 7	0 0	Code d'opération : 00 = Requête d'analyse de caractères
6 5 4	MSB LSB	N° d'affichage : 000 = No. 1 001 = No. 2 ... 111 = No. 3
3 2 1	MSB LSB	Type : 000 = No. 1 001 = No. 2 ... 111 = No. 8

Caractère 1 : réponse à l'analyse de caractères		
Numéro(s) de bit	**Valeur**	**Signification**
8 7 6 5 4 3 2 1	MSB LSB	Chacun des bits de cet octet de réponse possède une signification particulière en fonction du numéro de caractère envoyé (1-8) et du numéro d'affichage envoyé relatif au protocole du périphérique (1-8).

Format

```
TBOSSETREQUEST(cmd_bytes, idisp_num, irequest_num)
```

Types de données

Argument	**Type**	**Description**
cmd_bytes	svar (SORTIE)	L'octet de données hexadécimales est placé dans cette variable chaîne et est susceptible d'être transmis au périphérique TBOS dans la zone Next State Transmit (Transmission de l'état suivant).

Argument	Type	Description
idisp_num	numérique (ENTRÉE)	Numéro d'affichage TBOS (ou adresse) du périphérique (1 - 8). **REMARQUE :** les plages valides pour ce paramètre vont de 1 à 8 uniquement ; pour toute autre valeur, la sortie (cmd_bytes) est définie sur zéro, « \00\ ».
irequest_num	numérique (ENTRÉE)	Numéro d'analyse TBOS (1 - 8). **REMARQUE :** les plages valides pour ce paramètre vont de 1 à 8 uniquement ; pour toute autre valeur, la sortie (cmd_bytes) est définie sur zéro, « \00\ ».

Par exemple :

```
TBOSSETREQUEST(string_request_byte, 1, 1)
TBOSSETREQUEST(s_byte, idisp_num, i_scan_number)
```

L'exemple suivant permet de créer une requête d'analyse de caractères TBOS avec le numéro d'affichage 2 et le numéro de requête 1.

```
TBOSSETREQUEST(sbytes, 2, 1)
```

Contenu des variables de sortie :

```
sbytes = "\08\"
```

TIME

La commande TIME copie l'heure actuelle (au format HH-MM-SS) dans une variable chaîne, ivar ou fvar.

Format

```
TIME(dest)
```

Types de données

Argument	Type	Description
dest	svar (SORTIE)	La représentation au format chaîne de l'heure est placée dans cette variable chaîne (par exemple : «23-11-55»).
	variable numérique (numvar) (SORTIE)	Le nombre de secondes écoulées depuis le 1er janvier 1970 à 00:00:00 UTC est placé dans cette variable numérique (fvar par exemple).

Par exemple :

```
TIME(time_of_day)
TIME(i_num_seconds)
TIME(f_num_seconds)
```

REMARQUE : si vous utilisez une variable fvar, l'heure retournée sera précise à la microseconde près.

TOKENIZE

La commande TOKENIZE copie tous les composants d'une chaîne situés entre délimiteurs dans un tableau de chaînes. Cela peut se révéler utile lorsque vous copiez des données délimitées dans un script à exécuter ensuite à la demande.

Chaque caractère de la chaîne est considéré comme un séparateur potentiel d'éléments. Par exemple, si vous utilisez le séparateur « THE END », ce n'est pas la chaîne dans son intégralité qui sera considérée comme le délimiteur potentiel, mais chacun des caractères qui la compose :

```
"T"
"H"
"E"
"E"
"N"
"D"
```

Format

```
TOKENIZE(data, delimiter, tokens[], itokens)
```

Types de données

Argument	Type	Description
data	svar (ENTRÉE)	Données délimitées (par exemple : « xterm|subres|33|50 »).
delimiter	chaîne (ENTRÉE)	Séparateur(s) des différents éléments.
token	tableau (SORTIE)	Tableau des éléments tels que figurant dans les données en entrée de la chaîne délimitée.
itokens	variable numérique (numvar) (SORTIE)	Nombre d'éléments placés dans le tableau de chaînes.

Par exemple :

```
COPY(data:"This|Data|Is|Tokenized")
TOKENIZE(data, "|",tokens[], inumtokens)
```

Contenu des variables de sortie :

```
inumtokens = 4
tokens[0]= "This"
tokens[1]= "Data"
tokens[2]= "Is"
tokens[3]= "Tokenized"
```

Dans l'exemple suivant, les données transmises au script sont les suivantes :

```
"There#are|several*fields|in*this#string".
```

Trois séparateurs d'éléments différents sont utilisés : #, | et *.

Contenu des variables de sortie :

```
i_tokens = 7
messages[0] = "There"
messages[1] = "are"
messages[2] = "several"
messages[3] = "fields"
messages[4] = "in"
messages[5] = "this"
messages[6] = "string"
```

Dans l'exemple suivant, les données du tampon de réception sont les suivantes :

```
"Firewall Alarm - Major;Denial of Service Alarm -
Major;"
COPY(rxbuff:)
TOKENIZE(rxbuff,";",msgs[],i_msgs)
```

Contenu des variables de sortie :

```
i_msgs = 2
msgs[0] = "Firewall Alarm - Major"
msgs[1] = "Denial of Service Alarm - Major"
```

TOLOWER

La commande TOLOWER convertit les caractères d'une variable chaîne en minuscules. La variable chaîne ainsi transmise par l'intermédiaire de cette commande ne contient que des minuscules.

Format

```
TOLOWER(stringvar)
```

Types de données

Argument	Type	Description
stringvar	chaîne (ENTRÉE/ SORTIE)	Variable chaîne contenant la chaîne à convertir en minuscules.

Par exemple :

```
s_var = "This Is Lower Case"
TOLOWER(s_var)
```

Résultat :

```
s_var = "this is lower case"
```

TOUPPER

La commande TOUPPER convertit les caractères d'une variable chaîne en majuscules. La variable chaîne ainsi transmise par l'intermédiaire de cette commande ne contient que des majuscules.

Format

```
TOUPPER(stringvar)
```

Types de données

Argument	Type	Description
stringvar	chaîne (ENTRÉE/ SORTIE)	Variable chaîne contenant la chaîne à convertir en majuscules.

Par exemple :

```
s_var = "This Is Upper Case"
toupper(s_var)
```

Résultat :

```
s_var = "THIS IS UPPER CASE"
```

TRANSLATE

La commande TRANSLATE charge un fichier de valeurs séparées par une virgule (.csv) en mémoire, permet d'y effectuer une recherche rapide sur l'entrée de clé et d'en extraire les données associées à cette clé.

La commande TRANSLATE est associée aux éléments suivants.

- Valeurs séparées par une virgule (CSV)
- Recherche de clés (casse indifférente)
- Statut de la recherche
- Variables de données

Fichier de valeurs séparées par une virgule (CSV)

Les fichiers .csv sont des chemins relatifs du répertoire de script d'un collecteur. Le Générateur de collecteurs ne prend pas en charge l'édition de ces fichiers. Novell recommande donc de procéder à leur génération depuis Microsoft Excel. Le nom du fichier peut être une chaîne ou une variable.

L'exemple suivant du fichier friends.csv montre le format d'un fichier csv :

```
key1,data1,data2,data3
Bob,blue,25,210
Alice,green,19,110
Pat,purple,36,145
```

Pour savoir si l'un de vos amis figure dans le fichier friends.csv, la commande TRANSLATE effectue une recherche comme suit :

```
TRANSLATE("Bob","friends.csv",i_found)
```

Ou

```
COPY(s_Name:"Bob")
TRANSLATE(s_Name,"friends.csv",i_found)
```

Recherche de clés (casse indifférente)

Le paramètre de clé peut être une chaîne ou une variable chaîne. Les variables ou nombres entiers sont également pris en charge. Lors du chargement du fichier csv dans la mémoire, la clé de chaque entrée est définie sur des minuscules. La clé de la commande TRANSLATE est également définie en interne sur la casse minuscule afin de permettre des recherches de clé sans tenir compte de la casse.

Si l'on reprend l'exemple du fichier csv vu précédemment :

```
TRANSLATE("boB", "friends.csv",i_found)
```

La commande trouverait également Bob dans le fichier csv.

Statut de la recherche

Le statut de la recherche est défini sur 1 si la clé figure dans le fichier csv, et sur zéro dans le cas contraire. Vous pouvez utiliser un fichier csv ne comportant que des entrées de clé avec la commande TRANSLATE uniquement dans le but de déterminer la présence d'une clé donnée dans ce fichier. Pour des raisons de sécurité, un fichier csv peut contenir une liste d'adresses IP hostiles connues ou des noms d'utilisateur valides avec des informations liées à la stratégie comme des autorisations d'accès ou des temps d'accès autorisés.

REMARQUE : les clés exprimant des plages ne sont pas prises en charge, par exemple : les plages d'adresses IP et de valeurs numériques.

Variables de données

Il est possible d'extraire des données associées à la clé que vous recherchez dans le fichier csv. Vous pouvez utiliser un certain nombre de variables de script pour indiquer dans quelles variables stocker ces données. Les variables chaînes, entières et flottantes sont prises en charge. Toutes les entrées de données sont stockées sous forme de chaînes et seront converties dans le type de la variable fournie par la commande TRANSLATE.

Si l'on reprend l'exemple du fichier friends.csv vu précédemment :

```
Bob,blue,25,210
Alice,green,19,110
Pat,purple,36,145
```

Vous pouvez obtenir les données associées suivantes :

```
TRANSLATE(s_friend, "friends.csv", i_found, s_color,
i_age, i_weight)
```

Où :

- Si s_friend contient Alice, i_found est égal à 1, s_color à green, i_age à 19 et i_weight à 110.
- Si l'entrée de clé est introuvable, les variables demeurent telles quelles (s_color, i_age, i_weight).
- Si l'entrée pour Alice était la suivante :

  ```
  Alice,green,19,
  ```

  La même commande TRANSLATE donnerait le résultat suivant : la variable i_weight serait effacée (0 pour les entiers, 0.0 pour les valeurs flottantes et "" pour les chaînes) ; s_color serait green et i_age 19.
- Si l'entrée pour Alice était la suivante :

  ```
  Alice,green,,thin,Ford
  ```

  La même commande TRANSLATE donnerait le résultat suivant : la variable i_age serait effacée et thin serait converti en un entier (0) et placé dans la variable i_weight ; s_color serait green et Ford serait ignoré.
- Si l'entrée pour Alice était la suivante :

  ```
  Alice,25,19,110
  ```

  La même commande TRANSLATE donnerait le résultat suivant : s_color serait 25, i_age 19 et i_weight 110.

Format

```
TRANSLATE(<key>, <csv_file>, <found_status> [,
<variable>, ...])
```

Types de données

Argument	Type	Description
key		Clé à rechercher dans le fichier csv.
csv_file		Nom du fichier csv.
found_status		La variable entière est définie sur 1 si la clé figure dans le fichier csv, ou sur zéro dans le cas contraire.
variable		La liste des variables dans lesquelles placer les données associées à la clé.

TRIM

Cette commande supprime tous
les blancs (espaces vides) situés aux deux extrémités d'une chaîne, et remplace
les espaces multiples au sein des chaînes par un seul espace. Les blancs incluent
les caractères suivants :

- <tabulation>
- <retour chariot>
- <nouvelle ligne>
- <tabulation verticale>
- <saut de page>
- <espace>

Format

```
TRIM(svar)
```

Types de données

Argument	Type	Description
chaîne	svar (ENTRÉE)	Chaîne dans laquelle supprimer les espaces. Le résultat est stocké dans la variable d'entrée.

Par exemple :

```
COPY(s_var:" Hello    World  "
TRIM(s_var)
```

Contenu des variables de sortie :

```
s_var = " Hello World "
```

WHILE

La commande WHILE permet de mettre en boucle un flux de contrôle.

La commande WHILE fonctionne comme suit :

- Si le résultat de l'instruction WHILE() est true, les commandes d'analyse placées après WHILE() et avant l'instruction ENDWHILE() suivante, sont exécutées.
- Si le résultat de WHILE() est false, aucune des commandes situées entre les instructions WHILE() et ENDWHILE() n'est exécutée.

Bien que vous puissiez utiliser tous les types de données des deux côtés de l'opérateur d'une instruction WHILE(), vous ne pouvez comparer que des valeurs de même type entre elles (numérique avec numérique, chaîne avec chaîne par exemple).

L'opérateur de l'instruction WHILE() peut être l'un des caractères suivants : <, =, >, <=, >=, <>, &, +, ou ^.

ATTENTION : n'utilisez pas l'opérateur logique NON (^) en association avec une variable chaîne. Une erreur de syntaxe serait générée.

La comparaison directe avec un nombre négatif est impossible. Pour cela, utilisez l'une des méthodes suivantes :

- Utilisez la fonction d'analyse COMPARE.
- Effectuez une comparaison indirecte comme suit :

```
SET(i_compare_val=-10)
WHILE(ivar >i_compare_val)
SET(ivar=ivar-1)
ENDWHILE()
```

Format

```
WHILE(<expr>)
```

Où :

```
expr ::= var
       | (<expr>)
       | ^ <expr>
```

Où <expr> doit retourner un entier ou une valeur flottante.

```
       | <expr> <|=|>|<=|>=|<>|&|+ <expr>
```

Où les deux <expr> doivent retourner une valeur du même type.

Types de données

Argument	Type	Description
données1	tous (ENTRÉE)	Données à comparer à données2. Si données2 n'est pas utilisé, l'instruction devient logique (0 = false, tout le reste = true).
opérateur logique	< = > <= >= <> & + ^	Inférieur à Égal à Supérieur à Inférieur ou égal à Supérieur ou égal à Différent de ET logique OU logique NON logique
données2	tous (ENTRÉE) [FACULTATIF]	Données à comparer à données1. Elles doivent être du même type que ces dernières.
…	mêmes informations que précédemment	Utilisez jusqu'à 200 paramètres individuels pour créer des expressions logiques complexes.

Par exemple :

```
WHILE(i<3)
SET(i=i+1)
ALERT("Still in loop")
ENDWHILE()
ALERT("Exited loop")
```

4 Fonctions administratives de Sentinel Wizard

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

Ce chapitre s'adresse à l'administrateur système du module Wizard. Il décrit les différentes fonctions administratives que l'administrateur doit effectuer et fournit des informations relatives aux processus d'arrière-plan de Wizard.

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

Utilitaires et applications Wizard

Wizard est constitué d'une interface utilisateur, le Générateur de collecteurs, et de plusieurs autres utilitaires fonctionnant avec ce générateur pour les opérations de surveillance réseau.

Générateur de collecteurs

L'interface utilisateur de Wizard est le Générateur de collecteurs. Ce dernier permet à l'utilisateur de configurer les collecteurs sur le réseau, ainsi que les ports et les scripts qui sont utilisés pour communiquer avec les hôtes. Le Générateur de collecteurs fonctionne uniquement sous Windows.

REMARQUE : si un problème d'affichage des fenêtres Wizard survient après déplacement de la fenêtre par glisser-déplacer, il faut vérifier les paramètres d'affichage dans le panneau de configuration de Microsoft Windows. Dans l'onglet Effects (Effets), désélectionnez la case à cocher Show window contents while dragging (Afficher le contenu des fenêtres pendant leur déplacement).

Port

Dans le module Wizard, les ports permettent au collecteur de localiser les données d'événement de sécurité sur le réseau, car ils fournissent l'adresse IP de la source ainsi que d'autres informations (périphérique de sécurité [routeur, IDS, commutateur, etc.]). Chaque ligne de la table de configuration exécute un script de collecteur par source d'événement.

Gestionnaire des collecteurs

Le Gestionnaire des collecteurs démarre et arrête les processus de port.

Moteur du collecteur

Le moteur du collecteur traite la logique de modèle pour chaque port. Un moteur de collecteur est exécuté sur chaque port actif.

popup.exe

L'utilitaire d'exécution popup.exe est utilisé par le moteur du collecteur pour le traitement des commandes d'analyse contextuelles ou d'affichage.

popup.cfg

Le fichier de configuration popup.cfg est un fichier facultatif servant à contrôler les timeouts des commandes d'analyse contextuelles et d'affichage. Si vous ne disposez pas d'un fichier popup.cfg, aucun timeout ne s'applique aux commandes d'analyse contextuelles et d'affichage.

Pour définir un timeout à appliquer à la commande d'affichage, entrez l'instruction suivante :

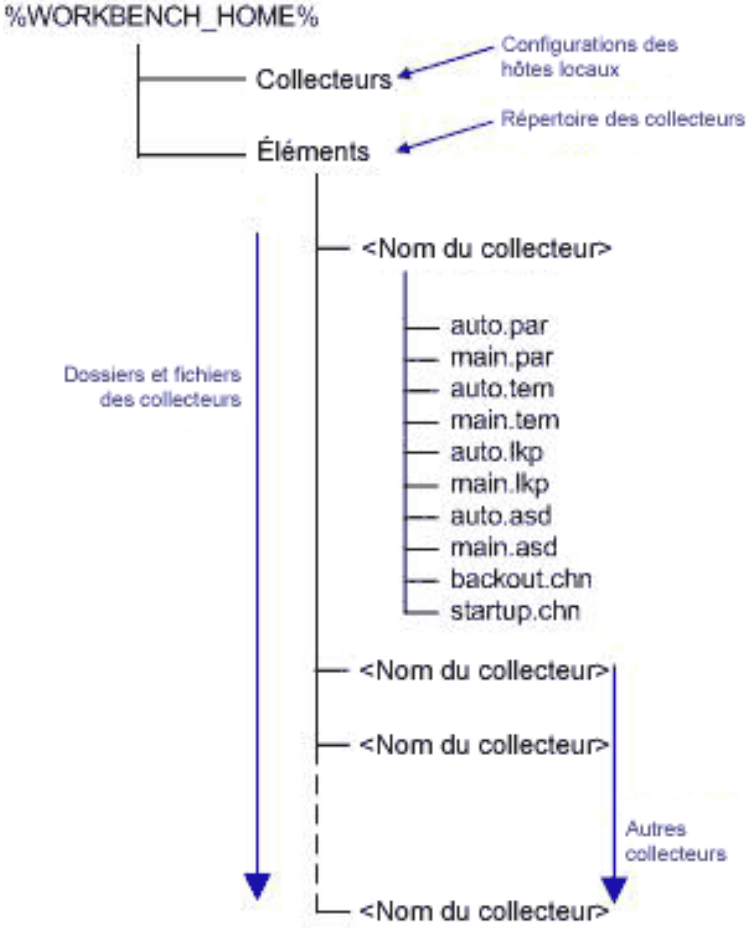
```
displaytimeout <true/false>.
```

Le timeout d'affichage est défini sur 20 secondes.

Pour définir un timeout à appliquer à la commande contextuelle, entrez l'instruction suivante :

```
timeout <timeout in seconds>.
```

Structure du répertoire Wizard



Légende

Collecteurs	Fichiers de configuration des ports (hôtes Wizard)
Éléments	Fichiers du collecteur
.par	Fichiers de paramètres
.tem	Fichiers de modèle
.lkp	Fichiers de recherche
.asd	Fichiers de description de l'état des éléments actifs
backout.chn	Fichiers de script pour le retour à l'état antérieur
startup.chn	Fichiers de script pour le démarrage

5 Balises META de Wizard et de Sentinel

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

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

Les balises META stockent les métadonnées. Les métadonnées sont des informations sur les données, des noms de variables prédéfinies pour les métadonnées. Par exemple, l'IP source d'une attaque est stocké dans la métabalise SourceIP. Les noms de produit sont stockés dans la balise META ProductName. Les données utilisées pour renseigner les balises META sont soit extraites des données de journal de périphérique soit définies dans le cadre du traitement du collecteur.

Pour accéder à la configuration de l'événement et à la fonction d'assignation du Gestionnaire des données Sentinel, cliquez sur l'onglet Événements.

REMARQUE : dans le langage de règle de corrélation RuleLg de format libre, lorsqu'une étiquette est précédée d'un « e », comme e.crt, celle-ci se rapporte à des événements actuels. Si une étiquette est précédée d'un « w », comme w.crt, celle-ci se rapporte à des événements historiques.

La valeur indiquée dans la colonne Variable du collecteur est le nom de la variable de collecteur à définir pour renseigner la balise META correspondante. Pour plus d'informations sur les commandes d'analyse, voir le chapitre 3 et la documentation relative aux collecteurs spécifiques situés dans

```
%ESEC_HOME%\wizard\elements\<nom du collecteur>\docs.
```

REMARQUE : dans le tableau ci-dessous, les étiquettes et les balises META sont utilisées dans le centre de contrôle Sentinel. Les variables de collecteur sont utilisées dans l'analyse du collecteur. Toutes les balises META n'ont pas de variable de collecteur correspondante.

Les types spécifiés dans la colonne Type possèdent les propriétés suivantes :

- chaîne : limitée à 255 caractères (sauf indication contraire).
- entier : entier signé de 32 bits.
- UUID : chaîne hexadécimale de 36 caractères (avec des tirets) ou 32 caractères (sans tirets) dans le format XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX (par exemple, - 6A5349DA-7CBF-1028-9795-000BCDFFF482).
- date : la variable de collecteur peut être définie avec une date en tant que nombre de millisecondes depuis le 1er janvier 1970 00:00:00 GMT. Lorsqu'elles sont affichées dans le centre de contrôle Sentinel, les balises META de type date sont affichées dans un format de date normal.
- IPv4 : adresse IP en notation décimale séparée par des points (par exemple, – xxx.xxx.xxx.xxx).

Étiquette	Balise META	Type	Description	Variable de collecteur
CorrelatedEventUuids	ceu	chaîne	Liste d'UUID d'événement associés à cet événement corrélé. S'appliquent uniquement pour les événements corrélés.	
Criticality	crt	entier	Sévérité de l'actif identifié dans cet événement.	s_CRIT
Ct1 à Ct2 (Réservée aux clients)	ct1 à ct2	chaîne	Réservée à l'utilisation par des clients pour des données spécifiques du client (Chaîne).	s_CT1 et s_CT2
Ct3 (Réservée aux clients)	ct3	entier	Réservée à l'utilisation par des clients pour des données spécifiques du client (Nombre).	s_CT3
CustomerVar1 à CustomerVar10	cv1 à cv10	entier	Réservée à l'utilisation par des clients pour des données spécifiques du client (Nombre).	s_CV1 à s_CV10
CustomerVar11 à CustomerVar20	cv11 à cv20	date	Réservée à l'utilisation par des clients pour des données spécifiques du client (Date).	s_CV11 à s_CV20
CustomerVar21 à CustomerVar29	cv21 à cv29	chaîne	Réservée à l'utilisation par des clients pour des données spécifiques du client (Chaîne).	s_CV21 à s_CV29
CustomerVar30 à CustomerVar34	cv30 à cv34	chaîne	Réservée à l'utilisation par des clients pour des données spécifiques du client (Chaîne). Peut prendre en charge des chaînes d'une longueur maximale de 4000 caractères.	s_CV30 à s_CV34
CustomerVar35 à CustomerVar89	cv35 à cv89	chaîne	Réservée à l'utilisation par des clients pour des données spécifiques du client (Chaîne).	s_CV35 à s_CV89
SARBOX	cv90	chaîne	Données spécifiques de Sarbanes Oxley.	s_CV90
HIPAA	cv91	chaîne	Données spécifiques de HIPAA (Health Insurance Portability and Accountability Act).	s_CV91
GLBA	cv92	chaîne	Données spécifiques de GLBA (Gramm-Leach-Bliley Act).	s_CV92

Étiquette	Balise META	Type	Description	Variable de collecteur
FISMA	cv93	chaîne	Données spécifiques de FISMA (Federal Information Security Management Act).	s_CV93
NISPOM	cv94	chaîne	Données spécifiques de NISPOM (National Industrial Security Program Operating Manual).	s_CV94
SIPCountry	cv95	chaîne	Pays de l'IP source.	s_CV95
DIPCountry	cv96	chaîne	Pays de l'IP de destination.	s_CV96
CustomerVar97 à CustomerVar100	cv97 à cv100	chaîne	Réservée à l'utilisation par des clients pour des données spécifiques du client (Chaîne).	s_CV97 à s_CV100
DateTime	dt	date	Date et heure normalisées de l'événement, fournies par le collecteur.	
DestinationHostName	dhn	chaîne	Nom d'hôte de destination vers lequel l'événement a été ciblé.	s_DHN
DestinationIP	dip	IPv4	Adresse IP de destination vers lequel l'événement a été ciblé.	s_DIP
DestinationPort	dp	chaîne (32)	Port de destination vers lequel l'événement a été ciblé.	s_DP
DestinationUserName	dun	chaîne	Nom d'utilisateur de destination sur lequel une action a été tentée. Exemple : tentatives de réinitialiser le mot de passe de racine.	s_DUN
EventID	id	UUID	Identificateur unique de cet événement.	
EventTime	et	chaîne	Heure normalisée de l'événement indiquée par le capteur et analysée dans le format suivant : A-M-J-H:M:S~AMPM24~TZ.	s_ET
EventName	evt	chaîne	Nom descriptif de l'événement indiqué (ou fourni) par le capteur. Exemple « Analyse des ports ».	s_EVT

Étiquette	Balise META	Type	Description	Variable de collecteur
ExtendedInformation	ei	chaîne (1000)	Stocke des informations supplémentaires collectée par le collecteur. Les valeurs incluses dans cette variable sont séparées par des points-virgules (;). Exemple : domaine pour un ID ou des noms de fichier.	s_EI
FileName	fn	chaîne (1000)	Nom du programme exécuté ou du fichier accédé, modifié ou affecté. Exemple : nom d'un fichier infecté par un virus ou d'un programme détecté par un IDS.	s_FN
Message	msg	chaîne (4000)	Texte de message en forme libre pour l'événement.	s_BM
Protocol	prot	chaîne	Protocole réseau de l'événement.	s_P
ProductName	pn	chaîne	Indique le type, le nom de code produit et de fournisseur du capteur à partir duquel l'événement a été généré. Exemple : Check Point FireWall=CPFW.	s_PN
ReporterName	rn	chaîne	Nom d'hôte ou adresse IP du périphérique vers lequel ou laquelle un événement a été consigné où partir duquel ou de laquelle l'événement est envoyé.	s_RN
ReservedVar1 à ReservedVar10	rv1 à rv10	entier	Réservée par Novell pour l'expansion (Nombre).	s_RV1 à s_RV10
ReservedVar11 à ReservedVar20	rv11 à rv20	date	Réservée par Novell pour l'expansion (Date).	s_RV11 à s_RV20
ReservedVar21 à ReservedVar25	rv21 à rv25	UUID	Réservée par Novell pour l'expansion (UUID).	s_RV21 à s_RV25
ControlPack	rv26	chaîne	Niveau 1 de catégorisation de contrôle Sentinel	s_RV26
ControlMonitor	rv27	chaîne	Niveau 2 de catégorisation de contrôle Sentinel	s_RV27
ReservedVar28	rv28	chaîne	Réservée par Novell pour l'expansion (Chaîne).	s_RV28

Étiquette	Balise META	Type	Description	Variable de collecteur
SourceIPCountry	rv29	chaîne	Pays de l'adresse IP source.	s_RV29
AttackID	rv30	chaîne	ID d'attaque normalisé (ID d'attaque de l'assistant)	s_RV30
DeviceName	rv31	chaîne	Nom du périphérique de sécurité	s_RV31
DeviceCategory	rv32	chaîne	Catégorie de périphérique (AV, DB, ESEC, FW, IDS, OS). AV : antivirus DB : base de donnée ESEC : événement système FW : pare-feu IDS : détection d'intrusion OS : système d'exploitation	s_RV32
EventContext	rv33	chaîne	Contexte d'événement (niveau de menace).	s_RV33
SourceThreatLevel	rv34	chaîne	Niveau de menace source.	s_RV34
SourceUserContext	rv35	chaîne	Contexte d'utilisateur source.	s_RV35
DataContext	rv36	chaîne	Contexte de données.	s_RV36
SourceFunction	rv37	chaîne	Fonction source.	s_RV37
SourceOperationalContext	rv38	chaîne	Contexte opérationnel source.	s_RV38
MSSPCustomerName	rv39	chaîne	Nom de client MSSP.	s_RV39
ReservedVar40 à ReservedVar43	rv40 à rv43	chaîne	Réservée par Novell pour l'expansion (Chaîne).	s_RV40 à s_RV43
DestinationThreatLevel	rv44	chaîne	Niveau de menace de destination.	s_RV44
DestinationUserContext	rv45	chaîne	Contexte utilisateur de destination.	s_RV45
VirusStatus	rv46	chaîne	Statut du virus.	s_RV46
DestinationFunction	rv47	chaîne	Fonction de destination.	s_RV47
DestinationOperationalContext	rv48	chaîne	Contexte opérationnel de destination.	s_RV48
ReservedVar49	rv49	chaîne	Réservée par Novell pour l'expansion (Chaîne).	s_RV49
eSecTaxonomyLevel1	rv50	chaîne	Catégorisation de code d'événement Sentinel - niveau 1.	s_RV50
eSecTaxonomyLevel2	rv51	chaîne	Catégorisation de code d'événement Sentinel - niveau 2.	s_RV51
eSecTaxonomyLevel3	rv52	chaîne	Catégorisation de code d'événement Sentinel - niveau 3.	s_RV52

Étiquette	Balise META	Type	Description	Variable de collecteur
eSecTaxonomyLevel4	rv53	chaîne	Catégorisation de code d'événement Sentinel - niveau 4.	s_RV53
ReservedVar54 à ReservedVar55	rv54 à rv55	chaîne	Réservée par Novell pour l'expansion (Chaîne).	s_RV54 à s_RV55
SourceAssetName	rv56	chaîne	Source (Gestion des ressources) – Nom de l'actif	s_RV56
SourceMacAddress	rv57	chaîne	Source (Gestion des ressources) – Adresse Mac	s_RV57
SourceNetworkIdentity	rv58	chaîne	Source (Gestion des ressources) – Identité du réseau	s_RV58
SourceAssetCategory	rv59	chaîne	Source (Gestion des ressources) – Catégorie d'actif	s_RV59
SourceEnvironmentIdentity	rv60	chaîne	Source (Gestion des ressources) – Identité d'environnement	s_RV60
SourceAssetValue	rv61	chaîne	Source (Gestion des ressources) - Valeur de l'actif	s_RV61
SourceCriticality	rv62	chaîne	Source (Gestion des ressources) - Sévérité	s_RV62
SourceSensitivity	rv63	chaîne	Source (Gestion des ressources) - Sensibilité	s_RV63
SourceBuilding	rv64	chaîne	Source (Gestion des ressources) - Bâtiment	s_RV64
SourceRoom	rv65	chaîne	Source (Gestion des ressources) – Pièce	s_RV65
SourceRackNumber	rv66	chaîne	Source (Gestion des ressources) – Numéro de rack	s_RV66
SourceCity	rv67	chaîne	Source (Gestion des ressources) – Ville	s_RV67
SourceState	rv68	chaîne	Source (Gestion des ressources) – État	s_RV68
SourceCountry	rv69	chaîne	Source (Gestion des ressources) - Pays	s_RV69
SourceZipCode	rv70	chaîne	Source (Gestion des ressources) – Code postal	s_RV70
SourceAssetOwner	rv71	chaîne	Source (Gestion des ressources) – Propriétaire de l'actif	s_RV71

Étiquette	Balise META	Type	Description	Variable de collecteur
SourceAssetMaintainer	rv72	chaîne	Source (Gestion des ressources) – Gestionnaire de l'entretien des ressources	s_RV72
SourceBusinessUnit	rv73	chaîne	Source (Gestion des ressources) – Division stratégique	s_RV73
SourceLineOfBusiness	rv74	chaîne	Source (Gestion des ressources) – Secteur d'activité	s_RV74
SourceDivision	rv75	chaîne	Source (Gestion des ressources) - Division	s_RV75
SourceDepartment	rv76	chaîne	Source (Gestion des ressources) - Service	s_RV76
SourceAssetId	rv77	chaîne	Source (Gestion des ressources) – ID d'actif source	s_RV77
DestinationAssetName	rv78	chaîne	Destination (Gestion des ressources) – Nom de l'actif	s_RV78
DestinationMacAddress	rv79	chaîne	Destination (Gestion des ressources) – Adresse Mac	s_RV79
DestinationNetworkIdentity	rv80	chaîne	Destination (Gestion des ressources) – Identité de réseau	s_RV80
DestinationAssetCategory	rv81	chaîne	Destination (Gestion des ressources) – Catégorie d'actif	s_RV81
DestinationEnvironmentIdentity	rv82	chaîne	Destination (Gestion des ressources) – Identité d'environnement	s_RV82
DestinationAssetValue	rv83	chaîne	Destination (Gestion des ressources) – Valeur de l'actif	s_RV83
DestinationCriticality	rv84	chaîne	Destination (Gestion des ressources) - Sévérité	s_RV84
DestinationSensitivity	rv85	chaîne	Destination (Gestion des ressources) - Sensibilité	s_RV85
DestinationBuilding	rv86	chaîne	Destination (Gestion des ressources) - Bâtiment	s_RV86
DestinationRoom	rv87	chaîne	Destination (Gestion des ressources) - Pièce	s_RV87
DestinationRackNumber	rv88	chaîne	Destination (Gestion des ressources) – Numéro de rack	s_RV88
DestinationCity	rv89	chaîne	Destination (Gestion des ressources) - Ville	s_RV89

Étiquette	Balise META	Type	Description	Variable de collecteur
DestinationState	rv90	chaîne	Destination (Gestion des ressources) - État	s_RV90
DestinationCountry	rv91	chaîne	Destination (Gestion des ressources) - Pays	s_RV91
DestinationZipCode	rv92	chaîne	Destination (Gestion des ressources) – Code postal	s_RV92
DestinationAssetOwner	rv93	chaîne	Destination (Gestion des ressources) – Propriétaire de l'actif	s_RV93
DestinationAssetMaintainer	rv94	chaîne	Destination (Gestion des ressources) – Gestionnaire de l'entretien des ressources	s_RV94
DestinationBusinessUnit	rv95	chaîne	Destination (Gestion des ressources) – Division stratégique	s_RV95
DestinationLineOfBusiness	rv96	chaîne	Destination (Gestion des ressources) – Secteur d'activité	s_RV96
DestinationDivision	rv97	chaîne	Destination (Gestion des ressources) - Division	s_RV97
DestinationDepartment	rv98	chaîne	Destination (Gestion des ressources) - Service	s_RV98
DestinationAssetId	rv99	chaîne	Destination (Gestion des ressources) – ID d'actif de destination	s_RV99
ReservedVar100	rv100	chaîne	Réservée par Novell pour l'expansion (Chaîne).	s_RV100
Resource	res	chaîne	Nom de la ressource.	s_Res
DeviceAttackName	rt1	chaîne	À utiliser avec l'assistant. Nom d'attaque provenant du périphérique de sécurité.	s_RT1
Rt2	rt2	chaîne	Renseignée par le nom de règle de corrélation lorsqu'une règle de corrélation génère un événement.	s_RT2
Rt3	rt3	entier	Réservée par Novell pour l'expansion (Nombre).	s_RT3
SourceHostName	shn	chaîne	Nom d'hôte source à partir duquel l'événement s'est produit.	s_SHN
SourceID	src	UUID	Identificateur unique du processus Sentinel qui a produit cet événement.	
SourceIP	sip	IPv4	Adresse IP source à partir de laquelle l'événement s'est produit.	s_SIP

Étiquette	Balise META	Type	Description	Variable de collecteur
SensorName	sn	chaîne	Nom du « détecteur ultime » de l'événement lors de sa réception dans les données brutes. Exemple, « FW1 » pour un pare-feu.	s_SN
Severity	sev	entier	Sévérité normalisée de l'événement (0 à 5).	i_Severity
SourcePort	sp	chaîne (32)	Port source à partir duquel l'événement a été généré.	s_SP
SensorType	st	chaîne (5)	Indicateur composé d'un seul caractère désignant le type de capteur (N, H, I, O, P, V, C, W). C : corrélation H : basé sur l'hôte I : interne (événement système) N : basé sur le réseau O : Autre P : performance (événement système) V : Antivirus W : Liste de surveillance	s_ST
SourceUserName	sun	chaîne	Nom d'utilisateur source utilisé pour initier un événement. Exemple, « jdupond » durant une tentative de « su ».	s_SUN
SubResource	sres	chaîne	Nom de la sous-ressource.	s_SubRes
Vulnerability	vul	entier	Vulnérabilité de l'actif identifié dans cet événement.	s_VULN
WizardAgent	agent	chaîne (64)	Collecteur Sentinel qui a généré l'événement. Pour les événements système, le collecteur sera Performance ou Internal.	
WizardPort	port	chaîne (64)	Description de port du collecteur Sentinel.	

6 Autorisations utilisateur relatives au centre de contrôle Sentinel

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

Les autorisations utilisateur sont réparties comme suit :

- Général
  - Filtres publics
  - Filtres privés
  - Actions d'intégration
- Vues actives
  - Eléments du menu
  - Affichage des récapitulatifs
- iTRAC
  - Gestion des modèles
  - Gestion des processus
- Incidents
- Gestion des collecteurs
- Analyse
- Advisor
- Administration
  - Corrélation
  - Statistiques DAS
  - Informations du fichier d'événements
  - Vues du serveur
  - Filtres globaux
  - Gestion des rôles iTRAC
  - Configuration du menu
  - Gestion des utilisateurs
  - Gestion des sessions d'utilisateur

Utilisateurs par défaut

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.

Général

Nom de l'autorisation	Description
Save Workspace (Enregistrement de l'espace de travail)	Permet à l'utilisateur d'enregistrer ses préférences. Si cette autorisation n'est pas disponible, l'utilisateur ne sera pas invité à enregistrer les modifications effectuées dans les préférences au moment de se déconnecter ou de quitter le centre de contrôle Sentinel.
Column Management (Gestion de colonnes)	Permet à l'utilisateur de gérer les colonnes dans les tables des vues actives.
Instantané	Permet à l'utilisateur de prendre des instantanés des tables des vues actives.

Général : filtres publics

Nom de l'autorisation	Description
Create Public Filters (Création de filtres publics)	Permet à l'utilisateur de créer un filtre dont l'ID de propriétaire est PUBLIC. Si l'utilisateur ne dispose pas de cette autorisation, la valeur PUBLIC n'apparaît pas dans la liste des ID de propriétaire pour lesquels il peut créer un filtre.
Modify Public Filters (Modification de filtres publics)	Permet à l'utilisateur de modifier un filtre public.
Delete Public Filters (Suppression de filtres publics)	Permet à l'utilisateur de supprimer un filtre public.

Général : filtres privés

Nom de l'autorisation	Description
Create Private Filters (Création de filtres privés)	Permet à l'utilisateur de créer des filtres privés pour lui-même ou pour d'autres utilisateurs.
Modify Private Filters (Modification de filtres privés)	Permet à l'utilisateur de modifier ses propres filtres privés ainsi que ceux créés par d'autres utilisateurs.
Delete Private Filters (Suppression de filtres privés)	Permet à l'utilisateur de supprimer ses propres filtres privés ainsi que ceux créés par d'autres utilisateurs.
View/Use Private Filters (Affichage/utilisation de filtres privés)	Permet à l'utilisateur d'afficher ses propres filtres privés ainsi que ceux créés par d'autres utilisateurs.

Général : actions d'intégration

Nom de l'autorisation	Description
Send to HP Open View (Envoi à HP Open View)	Permet à l'utilisateur d'envoyer des événements, un incident et des objets associés à HP OVO (HP Open View Operations).
Send Event to HP Service Desk (Envoi d'événements à HP Service Desk)	Permet à l'utilisateur d'envoyer des événements, un incident et des objets associés à HP Service Desk.
Send to Remedy Help Desk (Envoi vers Remedy Help Desk)	Permet à l'utilisateur d'envoyer des événements, un incident et des objets associés à Remedy Help Desk (BMC).

Active Views

Nom de l'autorisation	Description
View Active View Tab (Affichage de l'onglet Active Views)	Permet à l'utilisateur d'afficher et d'utiliser l'onglet Active Views, le menu et les fonctions associées à cet onglet.

Active Views : éléments de menu

Nom de l'autorisation	Description
Use Assigned Menu Items (Utilisation des éléments de menu assignés)	Permet à l'utilisateur d'utiliser des éléments de menu assignés dans la table des événements de la vue active (clic avec le bouton droit sur le menu).
Add to Existing Incident (Ajout à l'incident existant)	Permet à l'utilisateur d'ajouter des événements à des incidents existants à l'aide de la table des événements de la vue active (clic avec le bouton droit sur le menu).
Remove from Incident (Suppression d'événements d'un incident existant)	Permet à l'utilisateur de supprimer des événements d'incidents existants à l'aide de la table des événements de la vue active (clic avec le bouton droit sur le menu).
Email Events (Envoi d'événements par courrier électronique)	Permet à l'utilisateur d'envoyer par courrier électronique des événements à l'aide de la table des événements de la vue active (clic avec le bouton droit sur le menu).
View Advisor Attack Data (Affichage des données d'attaque du dispositif Advisor)	Permet à l'utilisateur d'afficher le flux de données Advisor relatives aux attaques.
View Vulnerability (Affichage des données de vulnérabilité)	Permet à l'utilisateur d'afficher le résultat d'une analyse Nessus.

Active Views : affichage des récapitulatifs

Nom de l'autorisation	Description
Use/View Summary Displays (Utilisation/affichage des récapitulatifs)	Permet à l'utilisateur d'accéder aux graphiques de la vue active.

iTRAC

Nom de l'autorisation	Description
View iTRAC Tab (Affichage de l'onglet iTRAC)	Permet à l'utilisateur d'afficher et d'utiliser l'onglet iTRAC, le menu et les fonctions associées à cet onglet.
Activity Management (Gestion des activités)	Permet à l'utilisateur d'accéder au Gestionnaire d'activités.

Gestion des modèles

Nom de l'autorisation	Description
View/Use Template Manager (Affichage/utilisation du Gestionnaire de modèles)	Permet à l'utilisateur d'accéder au Gestionnaire de modèles.
Create/Modify Templates (Création/modification de modèles)	Permet à l'utilisateur de créer et de modifier des modèles.

Gestion des processus

Nom de l'autorisation	Description
View/Use Process Manager (Affichage/utilisation du Gestionnaire de processus)	Permet à l'utilisateur d'accéder au Gestionnaire d'affichage des processus.
Control Processes (Contrôle des processus)	Permet à l'utilisateur d'utiliser le Gestionnaire d'affichage des processus.

Incidents

Nom de l'autorisation	Description
View Incidents Tab (Affichage de l'onglet Incidents)	Permet à l'utilisateur d'afficher et d'utiliser l'onglet Incidents, le menu et les fonctions associées à cet onglet.
Incident Administration (Administration des incidents)	Permet à l'utilisateur de modifier un incident.
View Incident(s) (Affichage des incidents)	Permet à l'utilisateur d'afficher les détails relatifs à un incident. Sans cette autorisation, la fenêtre Détails de l'incident ne s'affiche pas lorsque l'utilisateur double-clique sur un incident dans le navigateur ou dans l'onglet Incident des cas.

Nom de l'autorisation	Description
Create Incident(s) (Création d'incidents)	Permet à l'utilisateur de créer des incidents dans le menu Événement qui s'affiche lorsqu'il clique sur un événement avec le bouton droit de la souris.
Modify Incident(s) (Modification d'incidents)	Permet à l'utilisateur de modifier un incident dans la fenêtre Détails de l'incident.
Delete Incident(s) (Suppression d'incidents)	Permet à l'utilisateur de supprimer des incidents.
Assign Incident(s) (Assignation d'incidents)	Permet à l'utilisateur d'assigner un incident dans la fenêtre de création et de modification d'un incident.
Email Incidents (Envoi d'incidents par courrier électronique)	Permet à l'utilisateur d'envoyer par courrier électronique les incidents importants.
Incident Actions (Opérations d'incident)	Permet à l'utilisateur d'activer ou de désactiver la configuration ou l'exécution des opérations d'incidents.

Gestion des collecteurs

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

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

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

Analyse

Nom de l'autorisation	Description
View Analysis Tab (Affichage de l'onglet Analysis)	Permet à l'utilisateur d'afficher et d'utiliser l'onglet View Analysis (Affichage de l'analyse), le menu et les fonctions associées à l'onglet View System Overview (Affichage des informations du système).

Advisor

Nom de l'autorisation	Description
View Advisor Tab (Affichage de l'onglet Advisor)	Permet à l'utilisateur d'afficher et d'utiliser l'onglet View Advisor (Affichage de l'Advisor), le menu et les fonctions associées à cet onglet.

Administration

Nom de l'autorisation	Description
View Administration Tab (Affichage de l'onglet Administration)	Permet à l'utilisateur d'afficher et d'utiliser l'onglet View Administration (Affichage de l'Administration), le menu et les fonctions associées à cet onglet.

Administration : corrélation

Nom de l'autorisation	Description
Use/View Correlation Engine Manager (Utilisation/affichage du Gestionnaire de moteurs de corrélation)	Permet à l'utilisateur d'afficher et d'utiliser le moteur de corrélation.
Use/View Correlation Rules (Utilisation/affichage des règles de corrélation)	Permet à l'utilisateur de démarrer ou de mettre fin à l'exécution de règles de corrélation.

Administration : filtres globaux

Nom de l'autorisation	Description
View/Use Global Filters (Affichage/utilisation de filtres globaux)	Permet à l'utilisateur d'accéder à la fenêtre Configuration du filtre global.
Modify Global Filters (Modification de filtres globaux)	Permet à l'utilisateur de modifier la configuration des filtres globaux. **REMARQUE :** pour accéder à cette fonction, l'utilisateur doit également disposer de l'autorisation d'affichage et d'utilisation des filtres globaux.

Administration : configuration du menu

Nom de l'autorisation	Description
Configuration du menu	Permet à l'utilisateur d'accéder à la fenêtre Configuration du menu et d'ajouter des options qui s'affichent dans le menu Événement lorsque l'utilisateur clique avec le bouton droit sur un événement.

Administration : statistiques DAS

Nom de l'autorisation	Description
Statistiques DAS	Permet à l'utilisateur d'afficher les activités DAS (fichiers DAS_Binary et DAS_Query).

Administration : informations du fichier d'événements

Nom de l'autorisation	Description
Informations du fichier d'événements	Permet à l'utilisateur d'afficher le statut des fichiers d'événements.

Administration : vues du serveur

Nom de l'autorisation	Description
View Servers (Affichage des serveurs)	Permet à l'utilisateur de surveiller le statut de tous les processus.
Control Servers (Contrôle des serveurs)	Permet à l'utilisateur de démarrer, de redémarrer ou d'arrêter les processus.

Administration : gestion des utilisateurs

Nom de l'autorisation	Description
Use/View User Account (Utilisation/affichage des comptes d'utilisateur)	Permet à l'utilisateur d'utiliser et d'afficher les comptes des utilisateurs.
Create User Account (Création d'un compte d'utilisateur)	Permet à l'utilisateur de créer un compte d'utilisateur. **REMARQUE :** pour accéder à cette fonction, l'utilisateur doit également disposer de l'autorisation d'affichage et d'utilisation des comptes d'utilisateur.
Modify Existing User Account (Modification d'un compte d'utilisateur existant)	Permet à l'utilisateur de modifier un compte d'utilisateur existant. **REMARQUE :** pour accéder à cette fonction, l'utilisateur doit également disposer de l'autorisation d'affichage et d'utilisation des comptes d'utilisateur.

Nom de l'autorisation	Description
Delete User Account (Suppression d'un compte d'utilisateur)	Permet à l'utilisateur de supprimer un compte d'utilisateur existant. **REMARQUE :** pour accéder à cette fonction, l'utilisateur doit également disposer de l'autorisation d'affichage et d'utilisation des comptes d'utilisateur.

Administration : gestion des sessions d'utilisateur

Nom de l'autorisation	Description
User Session Management (Gestion des sessions d'utilisateur)	Permet à l'utilisateur d'afficher, de verrouiller et de fermer des sessions d'utilisateur actives (connexions au centre de contrôle Sentinel).

Administration : gestion des rôles iTRAC

Nom de l'autorisation	Description
iTRAC Role Management (Gestion des rôles iTRAC)	Permet à l'utilisateur d'afficher et d'utiliser le Gestionnaire de rôles dans l'onglet Admin.

7 Moteur de corrélation Sentinel

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

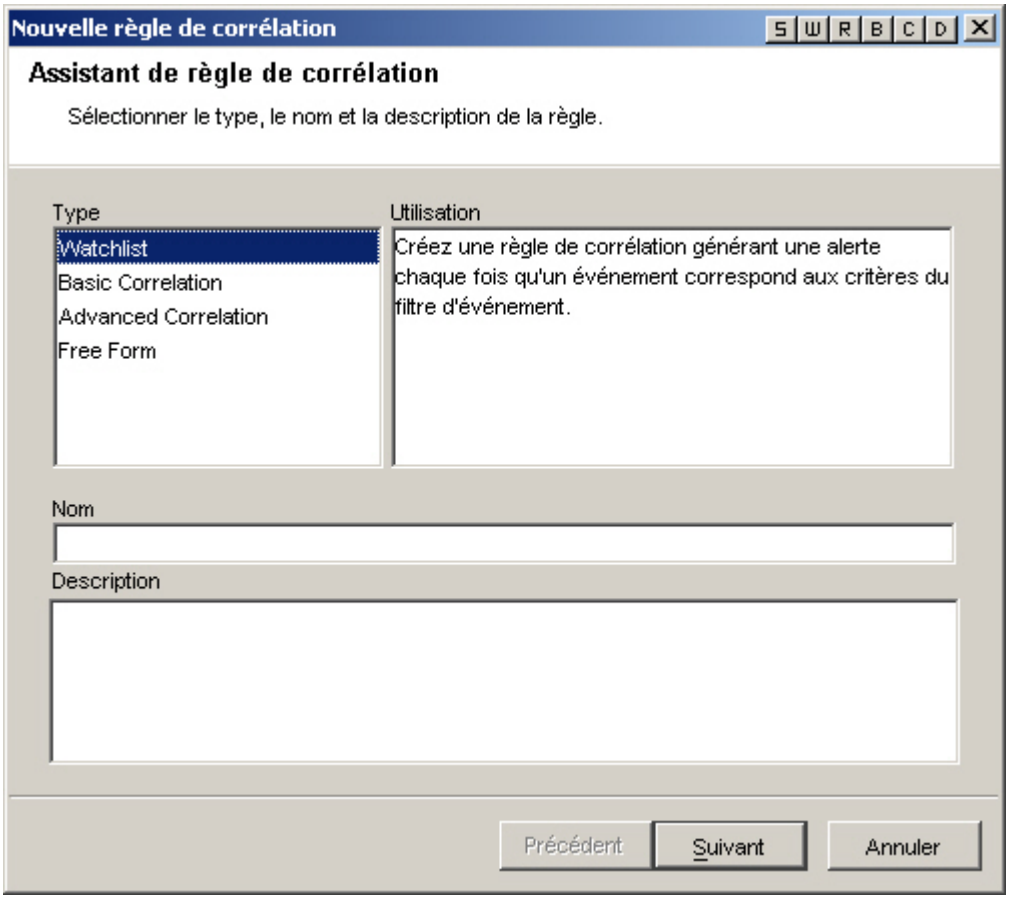
Le moteur de corrélation Sentinel est une application multithread résidant en mémoire. Le traitement multithread permet au moteur de corrélation de tirer profit d'une configuration matérielle multiprocesseur telle qu'un ensemble de machines SMP (symmetric multiprocessing).

Le moteur de corrélation est conçu pour recevoir des données provenant de périphériques sécurisés, de périphériques réseau ou d'autres applications et pour rechercher des modèles, généralement dans un certain laps de temps. Ces modèles peuvent signaler des attaques, des intrusions, une utilisation incorrecte ou un échec. Lorsqu'un événement corrélé est généré, le champ Rt2 contient le nom de la règle de corrélation.

Le moteur de corrélation Sentinel permet un déploiement évolutif. Son architecture rend possible le déploiement d'un réseau distribué de moteurs de corrélation fonctionnant ensemble pour corréler des données importantes en temps réel et en toute sécurité : les événements de sécurité surveillés en temps réel, les résultats d'analyse de vulnérabilité pour les systèmes susceptibles d'être visés et les informations sur les actifs, qui indiquent l'importance relative des systèmes par rapport aux processus d'entreprise critiques ainsi que leur association à d'autres systèmes dans l'organisation.

Le moteur de corrélation Sentinel fonctionne à partir de règles. Vous pouvez diriger le processus du moteur de corrélation à l'aide de règles créées dans l'éditeur de règles du centre de contrôle Sentinel. Cet éditeur fonctionne à partir d'un ensemble d'assistants de règles de corrélation qui proposent plusieurs options de création de règles. Ces assistants sont les suivants :

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



Types des filtres de corrélation

Pour les assistants de règles Liste de surveillance, Corrélation de base et Corrélation avancée, il existe quatre types de filtre possibles. Ces types sont les suivants :

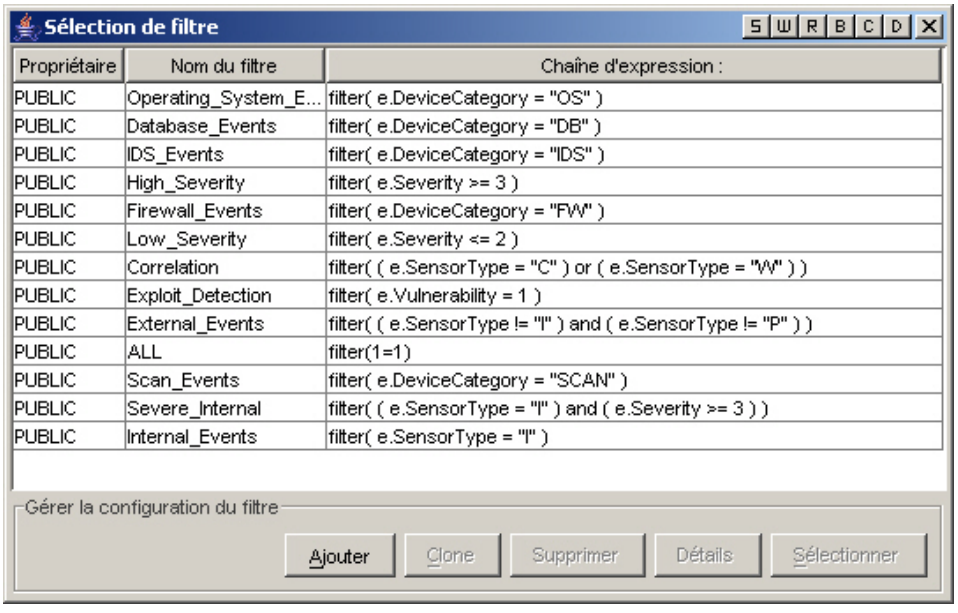
- Allow All (Tout autoriser) : type équivalent à l'exécution d'un filtre d'un niveau de gravité supérieur ou égal à zéro.
- Modèle : toute expression générique dont la syntaxe est similaire à celle d'une commande Grep. Règle capable de rechercher l'adresse IP source d'un pirate informatique et de vous avertir chaque fois que cette adresse IP est repérée dans un message d'événement.
- Gestionnaire de filtres : liste déroulante qui permet de sélectionner ou de créer un filtre.
- Générateur : permet de créer des critères d'inclusion ou d'exclusion d'événements en fonction d'opérateurs booléens.

Filtre de corrélation Pattern (Modèle)

Un filtre de corrélation Pattern (Modèle) se sert de toutes les expressions génériques qui respectent une syntaxe de type Grep. L'expression générique à utiliser pour la correspondance est obtenue par concaténation de toutes les balises META présentes pour chaque événement entrant. Par exemple, virusXYZ doit vérifier la présence de la chaîne virusXYZ dans toutes les balises META présentes dans chaque événement entrant.

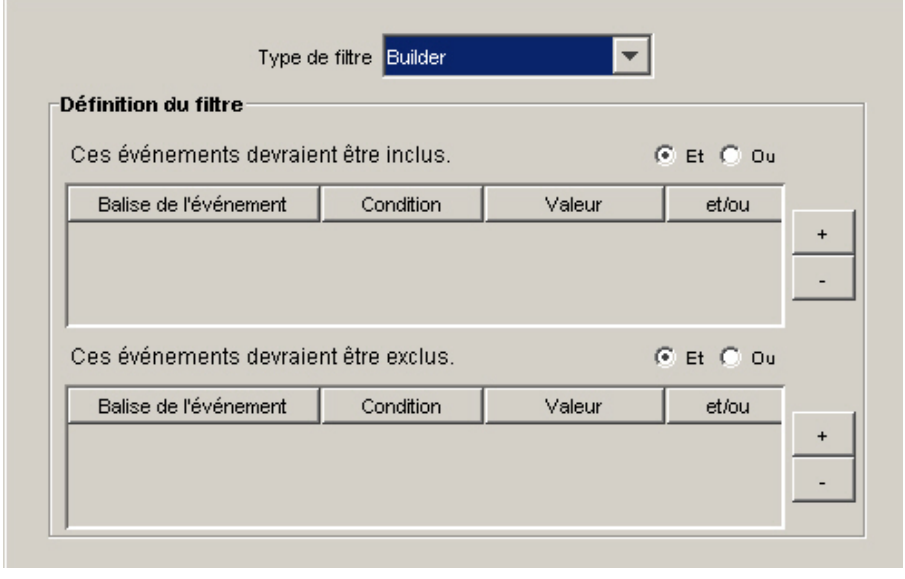
Filtre de corrélation Gestionnaire de filtres

Cette option vous permet de sélectionner un filtre existant ou de créer un filtre à utiliser dans votre corrélation à l'aide de la fenêtre Gestionnaire de filtres.



Filtre de corrélation Builder (Générateur)

Le filtre de corrélation Builder (Générateur) est composé de deux parties. La première concerne les critères d'inclusion pour déterminer les événements à inclure dans la correspondance des modèles, tandis que la deuxième est consacrée aux critères d'exclusion permettant de déterminer les événements à exclure de la correspondance.



- Événements à inclure dans la correspondance des modèles : utilisez le tableau ci-dessus pour indiquer les conditions qui vont déterminer les événements déclencheurs de la corrélation.
  - Balise de l'événement : la colonne Balise de l'événement contient une liste déroulante des différentes balises d'événement (ou balises META) en fonction desquelles une corrélation peut être établie.
  - Condition : la colonne Condition contient une liste déroulante d'opérateurs utilisés pour créer une condition de corrélation.
  - Valeur : lorsque les conditions =, !=, <, >, <= ou >= ont été sélectionnées, la colonne Valeur est constituée d'un ensemble de champs où vous pouvez entrer librement des valeurs. Si l'élément =balise META ou !=balise META est sélectionné dans la colonne Condition, la colonne Valeur contient une liste déroulante de balises META qu'il est possible de sélectionner. Vous pouvez entrer toute valeur qui respecte les conditions suivantes :
    - Aucune apostrophe ne peut être utilisée.
    - Les caractères génériques possibles sont l'astérisque (*) et le point (.). Ils peuvent apparaître à n'importe quel endroit de la chaîne si vous utilisez une expression rationnelle (regex).
    - Aucun caractère d'échappement ne peut être utilisé, ce qui signifie que les caractères génériques ne peuvent pas non plus faire l'objet d'un échappement.
  - et/ou : passez de l'opérateur logique « et » à l'opérateur logique « ou » en cliquant sur la case d'option correspondante. Lorsque plusieurs conditions sont indiquées dans ce tableau, les cases « et » et « ou » vous permettent de préciser si toutes les conditions doivent être remplies ou si seulement l'une de ces conditions doit être remplie. Sélectionnez « et » pour indiquer que toutes les conditions doivent être remplies. Sélectionnez « ou » pour indiquer qu'une seule des conditions doit être remplie.

  REMARQUE : cette sélection n'est valide que lorsque le tableau contient plusieurs lignes. Par défaut, l'opérateur logique sélectionné est celui qui s'applique à toutes les lignes du tableau, sauf la dernière. Il est impossible de combiner ces deux opérateurs logiques pour des lignes du même tableau.

  - Boutons +/- : le bouton + permet d'ajouter une ligne à la fin du tableau tandis que le bouton - permet de supprimer la ligne sélectionnée dans le tableau, quelle que soit sa position.
- Événements à exclure de la correspondance des modèles : utilisez le tableau présenté ci-avant pour indiquer les conditions qui vont déterminer les événements non-déclencheurs
  de la règle de corrélation.
  - Balise de l'événement : contient une liste déroulante des balises d'événement en fonction desquelles une corrélation peut être établie.
  - Condition : la colonne Condition contient une liste déroulante d'opérateurs utilisés pour créer une condition de corrélation.
  - Valeur : lorsque les conditions =, !=, <, >, <= ou >= ont été sélectionnées, la colonne Valeur est constituée d'un ensemble de champs où vous pouvez entrer librement des valeurs. Si l'élément =balise META ou !=balise META est sélectionné dans la colonne Condition, la colonne Valeur contient une liste déroulante de balises META qu'il est possible de sélectionner. Vous pouvez entrer toute valeur qui respecte les conditions suivantes :
    - Aucune apostrophe ne peut être utilisée.
    - Les caractères génériques possibles sont l'astérisque (*) et le point (.). Ils peuvent apparaître à n'importe quel endroit de la chaîne si vous utilisez une expression rationnelle (regex).

- Aucun caractère d'échappement ne peut être utilisé, ce qui signifie que les caractères génériques ne peuvent pas non plus faire l'objet d'un échappement.

- et/ou : passez de l'opérateur logique « et » à l'opérateur logique « ou » en cliquant sur la case d'option correspondante. Lorsque plusieurs conditions sont indiquées dans ce tableau, les cases « et » et « ou » vous permettent de préciser si toutes les conditions doivent être remplies ou si seulement l'une de ces conditions doit être remplie. Sélectionnez « et » pour indiquer que toutes les conditions doivent être remplies. Sélectionnez « ou » pour indiquer qu'une seule des conditions doit être remplie.

REMARQUE : cette sélection n'est valide que lorsque le tableau contient plusieurs lignes. Par défaut, l'opérateur logique sélectionné est celui qui s'applique à toutes les lignes du tableau, sauf la dernière. Il est impossible de combiner ces deux opérateurs logiques pour des lignes du même tableau.

- Boutons +/- : le bouton + permet d'ajouter une ligne à la fin du tableau tandis que le bouton - permet de supprimer la ligne sélectionnée dans le tableau, quelle que soit sa position.

Définition des règles de corrélation

Les assistants de règles de corrélation Liste de surveillance, Corrélation de base et Corrélation avancée vous permettent d'appliquer très rapidement un type de règle prédéfini en fonction de ce que vous souhaitez faire. Pour chaque type de règle, l'assistant correspondant traite la génération d'une règle de corrélation dans un langage de règle propre au moteur de corrélation. Chaque règle est créée dans la fenêtre Règles de corrélation qui s'ouvre à partir de l'onglet Admin.

Un assistant de règle de corrélation comprend un éditeur libre permettant d'utiliser le langage de définition de corrélation RuleLg pour ajouter la règle directement dans le langage du moteur de corrélation.

Liste de surveillance

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

- Allow All (Tout autoriser) : type équivalent à l'exécution d'un filtre d'un niveau de gravité supérieur ou égal à zéro.
- Modèle : toute expression générique dont la syntaxe est similaire à celle d'une commande Grep.
- Gestionnaire de filtres : liste déroulante qui permet de sélectionner ou de créer un filtre.
- Générateur : permet de créer des critères d'inclusion ou d'exclusion d'événements en fonction d'opérateurs booléens.

Pour plus d'informations, reportez-vous à la section Création d'une règle de liste de surveillance.

Corrélation de base

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

- Allow All (Tout autoriser) : type équivalent à l'exécution d'un filtre d'un niveau de gravité supérieur ou égal à zéro.
- Modèle : toute expression générique dont la syntaxe est similaire à celle d'une commande Grep.
- Gestionnaire de filtres : liste déroulante qui permet de sélectionner ou de créer un filtre.
- 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, tels qu'un système de détection d'intrusion ou un pare-feu.

Pour plus d'informations, reportez-vous à la section Création d'une règle de corrélation de base.

Corrélation avancée

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

- Allow All (Tout autoriser) : type équivalent à l'exécution d'un filtre d'un niveau de gravité supérieur ou égal à zéro.
- Modèle : toute expression générique dont la syntaxe est similaire à celle d'une commande Grep.
- Gestionnaire de filtres : liste déroulante qui permet de sélectionner ou de créer un filtre.
- Générateur : permet de créer des critères d'inclusion ou d'exclusion d'événements en fonction d'opérateurs booléens.

Cette règle de corrélation 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 évènements aux évènements 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).

Pour plus d'informations, reportez-vous à la section Création d'une règle de corrélation avancée.

Règle de corrélation RuleLg de format libre

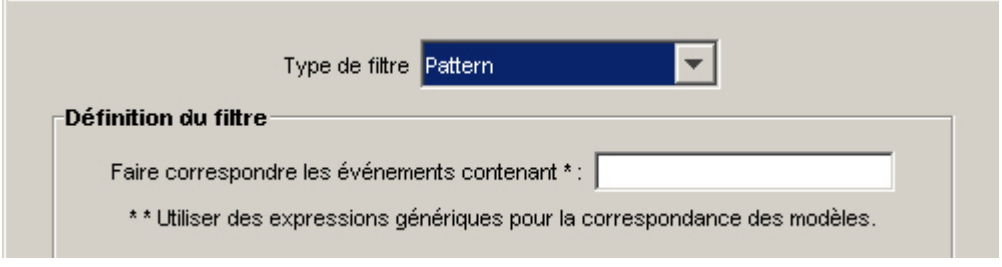
Le langage de définition de règle de corrélation RuleLg vous permet de définir entièrement les règles de corrélation. L'utilisation de ce type de règle de corrélation exige la connaissance préalable du langage RuleLg.

Pour plus d'informations, reportez-vous à la section Création d'une règle de corrélation RuleLg de format libre.

Création d'une règle de liste de surveillance

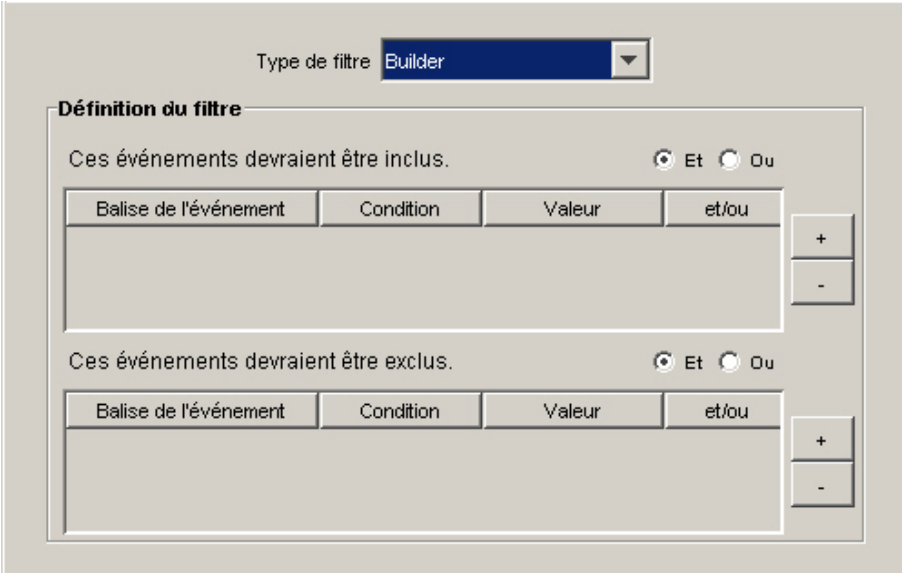
Créez une règle de liste de surveillance lorsque vous souhaitez indiquer au moteur de corrélation une chaîne à rechercher dans chaque évènement entrant. Pour créer une règle de liste de surveillance :

- Sélectionnez une règle de liste de surveillance dans la première fenêtre de l'assistant de règle de corrélation. Entrez les informations requises suivantes :
  - Nom de la règle : nom qui s'affiche dans la liste des règles. Nombre maximal de caractères autorisés : 255. Les points (.) ne sont pas autorisés. Les caractères ASCII du code étendu ne sont pas autorisés. Une distinction entre les majuscules et les minuscules est faite pour les noms de règles.
  - Description : bref descriptif de 1 024 caractères au maximum.
- Type du filtre :
  - Allow All (Tout autoriser) -
  - Pattern (Modèle) - Surveiller les événements contenant *



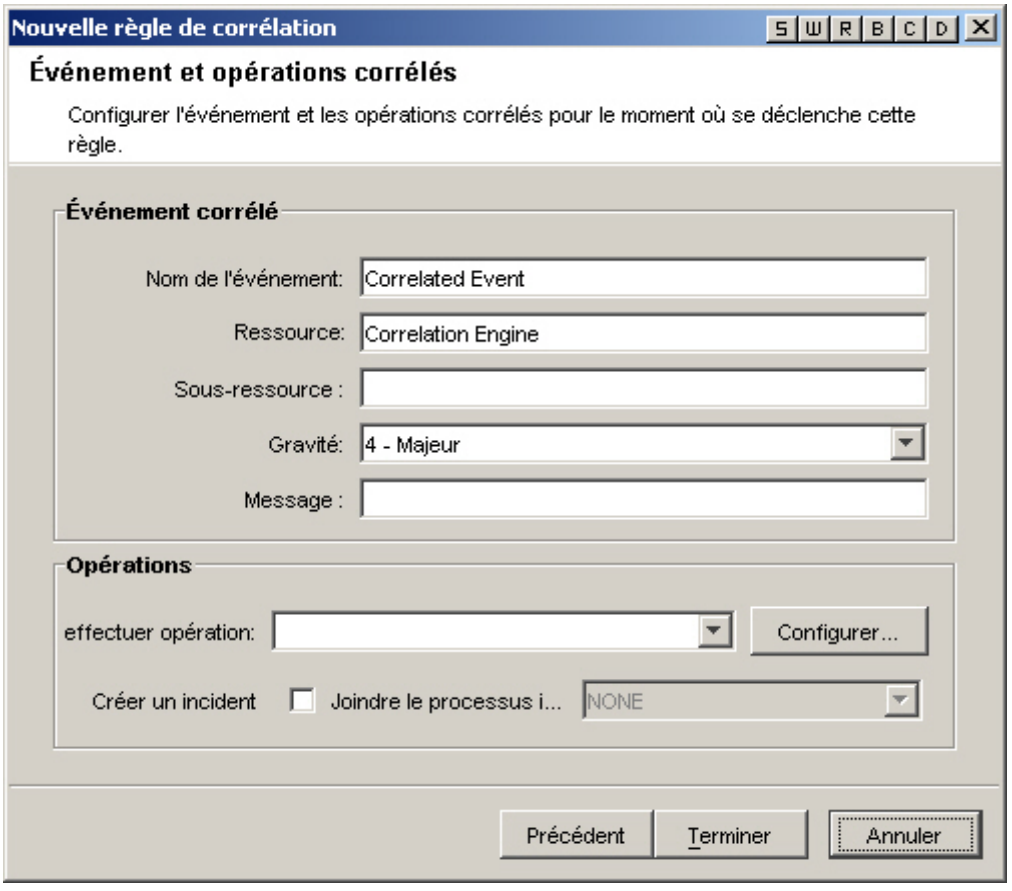
  - Gestionnaire de filtres - ({ownerid}:{Filter name}:<Nom du champ>

  - Builder (Générateur)

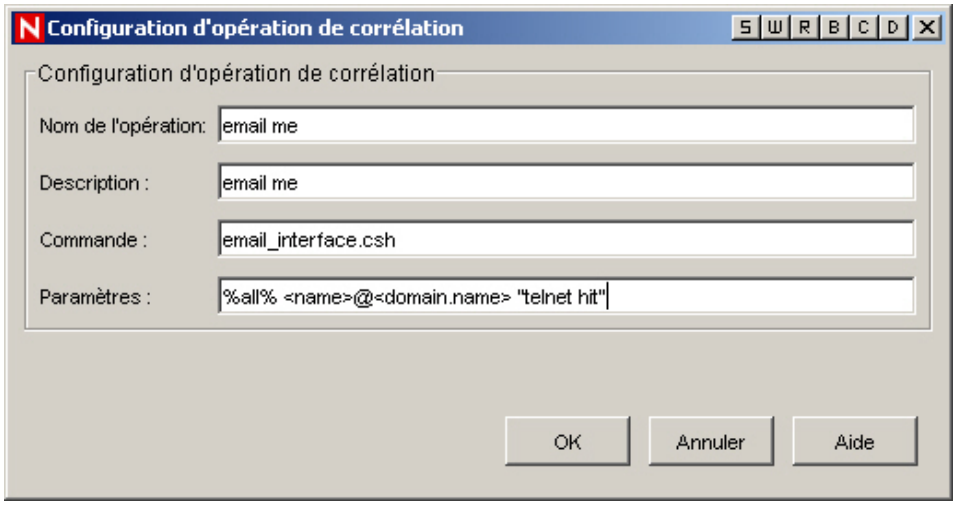


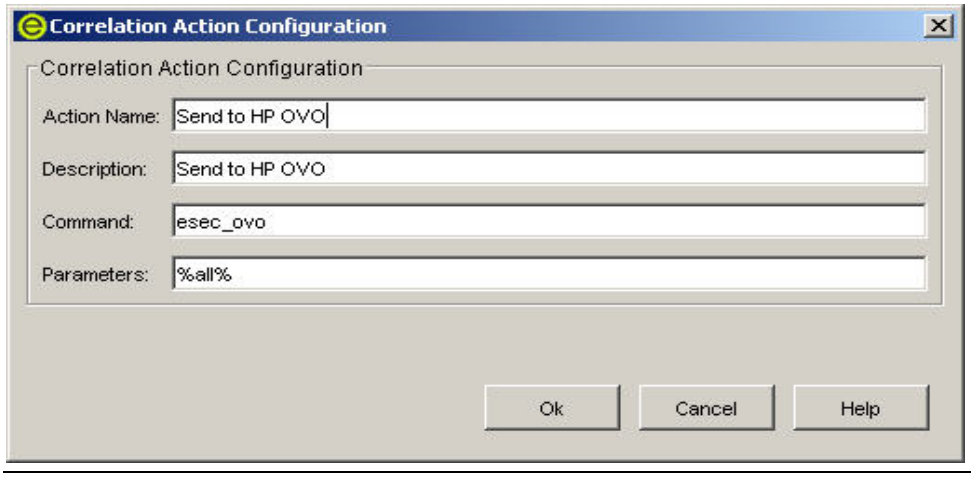
- Page Événements et opérations corrélés : cette fenêtre permet de définir l'action automatiquement appliquée lorsque des événements correspondent à la règle de corrélation concernée. Seul le niveau de gravité est obligatoire. Par défaut, il est défini sur 4.
  - Nom de l'événement : par défaut, le nom de l'événement est celui de l'événement corrélé. Il s'agit du nom textuel de l'événement corrélé.
  - Ressource : par défaut, moteur de corrélation Il s'agit du nom textuel de la ressource dans le système.
  - Sous-ressource : par défaut, <Aucun>. Cela vaut pour toutes les ressources contenant plusieurs sous-ressources.
  - Définir le niveau de gravité sur : la valeur par défaut est 4. Il s'agit du niveau de gravité attribué par défaut à l'événement. Les valeurs valides sont 0, 1, 2, 3, 4 (valeur par défaut) et 5. Une liste déroulante qui affiche tous les niveaux de gravité valides est disponible.
  - Texte de message personnalisé : la valeur par défaut est <Aucun>. Il s'agit du texte qui s'affiche en même temps que l'événement. Il sert à identifier la condition qui a déclenché la règle de liste de surveillance. Le nombre maximal de caractères autorisé est de 4 000. Le texte entré dans cette zone est placé devant celui de l'événement corrélé et séparé de lui par une barre verticale. Par exemple, si vous entrez le texte « Nouveau message », le message de corrélation apparaît sous la forme « Nouveau message|Trois instances de... ».
  - Effectuer l'opération (Oracle uniquement) : la valeur par défaut est <Aucun>. Il s'agit du nom d'un fichier exécutable qui démarre dès que la règle de liste de surveillance est déclenchée. Ce fichier doit se trouver dans le répertoire $ESEC_HOME/sentinel/exec et doit pouvoir être exécuté par l'utilisateur esecadm. Aucune validation n'est effectuée pour la valeur entrée dans cette zone de texte de format libre. Vous pouvez indiquer les balises META que vous souhaitez intégrer au fichier exécutable.

- Effectuer l'opération (MSSQL uniquement) : la valeur par défaut est <Aucun>. Il s'agit du nom d'un fichier exécutable qui démarre dès que la règle de liste de surveillance est déclenchée. Ce fichier doit se trouver dans le répertoire %ESEC_HOME%\sentinel\bin et doit pouvoir être exécuté par l'utilisateur esecadm. Aucune validation d'entrée n'est effectuée. Vous pouvez indiquer les balises META que vous souhaitez intégrer au fichier exécutable. Dans le premier des deux exemples suivants, la règle de corrélation entraîne l'envoi d'un courrier électronique. Dans le deuxième, la règle de corrélation entraîne l'envoi d'un événement à HP OVO (HP OpenView Operations).



La ligne de commande et celle des paramètres doivent être renseignées par des chaînes de caractères. Lors de l'analyse, les mêmes règles sont appliquées aux deux lignes, à savoir que la barre oblique inverse (\) constitue un caractère d'échappement. Elle permet d'utiliser les caractères suivants : \, % et ". Par exemple, la chaîne \%\"\\ équivaut à %"\. Si vous avez besoin d'une commande qui contient une barre oblique inverse, comme lorsque vous exécutez une commande Windows dans un sous-répertoire de sentinel\bin par exemple, il vous faut entrer deux barres obliques inverses pour chaque barre oblique de répertoire. Exemple : Pour exécuter un fichier traitement par lot nommé « run.bat » sous %esec_home%\sentinel\bin\ fichiers_par_lots\, il vous faut entrer fichiers_par_lots\\run.bat. Notez bien que tous les fichiers exécutables doivent se trouver sous %esec_home%\sentinel\bin\.





REMARQUE : pour plus d'informations sur les commandes et les paramètres, reportez-vous au « Chapitre 5 : Balises META de Wizard et de Sentinel » du guide des références utilisateur ainsi qu'à la section Sortie de corrélation du présent document.

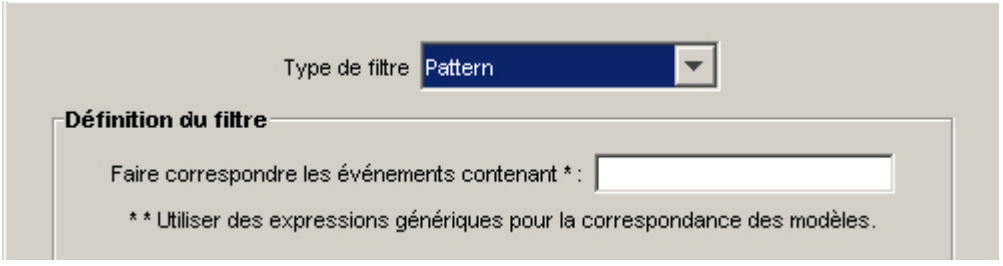
- Créer un incident : la création d'un incident fait partie des actions possibles pour un événement corrélé.
- Attacher le processus iTRAC : un processus iTrac peut être associé à un incident.

Création d'une règle de corrélation de base

Pour compter le nombre de fois que certaines conditions sont remplies sur une durée déterminée, vous pouvez créer une règle de corrélation de base. Les étapes de la procédure sont les suivantes :

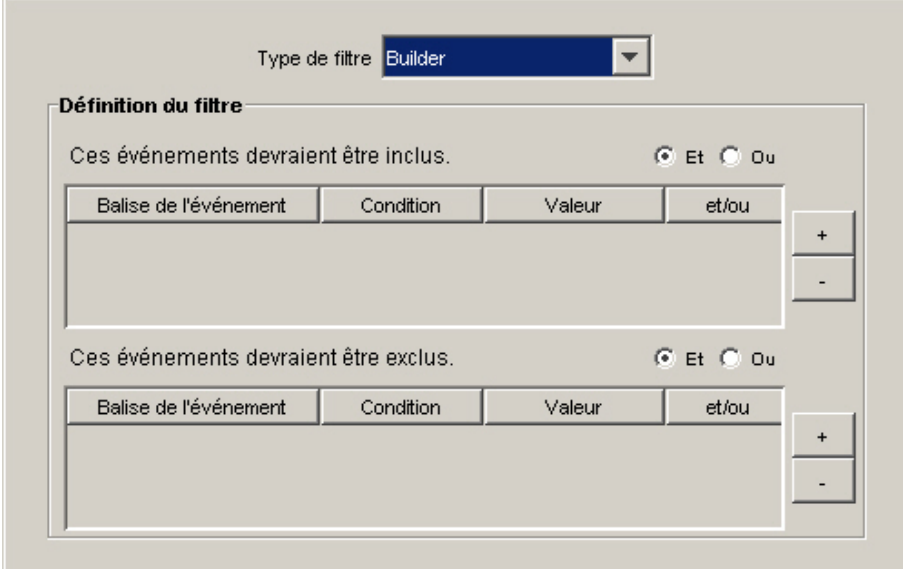
- Sélectionnez Basic Correlation Rule (Règle de corrélation de base) dans la première fenêtre de l'assistant de règle de corrélation. Entrez les informations requises suivantes :
  - Nom de la règle : nom qui s'affiche dans la liste des règles. Nombre maximal de caractères autorisés : 255. Les points (.) ne sont pas autorisés. Les caractères ASCII du code étendu ne sont pas autorisés. Une distinction entre les majuscules et les minuscules est faite pour les noms de règles.
  - Description : bref descriptif de 1 024 caractères au maximum.

- Type du filtre :
  - Allow All (Tout autoriser)
  - Pattern (Modèle)



  - Gestionnaire de filtres - ({ownerid}:{Filter name}:<Nom du champ>

  - Builder (Générateur)



- Seuil et critères de regroupement (moitié supérieure de la fenêtre) : Activer la règle : - Cette option vous permet d'entrer des critères de correspondance pour plusieurs événements entrant dans le système dans un certain laps de temps.
  - Lorsque la condition est remplie _fois : la valeur par défaut est 1. Il faut que la condition ait été détectée autant de fois que spécifié pour qu'une règle soit déclenchée. La valeur minimale à entrer pour ce seuil est 1.
  - dans (délai) : la valeur par défaut est 60 secondes. En indiquant une valeur pour cette option, la condition se retrouve liée à la période indiquée. Cette option est constituée à la fois d'une zone d'entrée de variable et d'une liste déroulante. Les options proposées par la liste déroulante sont les suivantes : secondes, minutes, heures et jours.

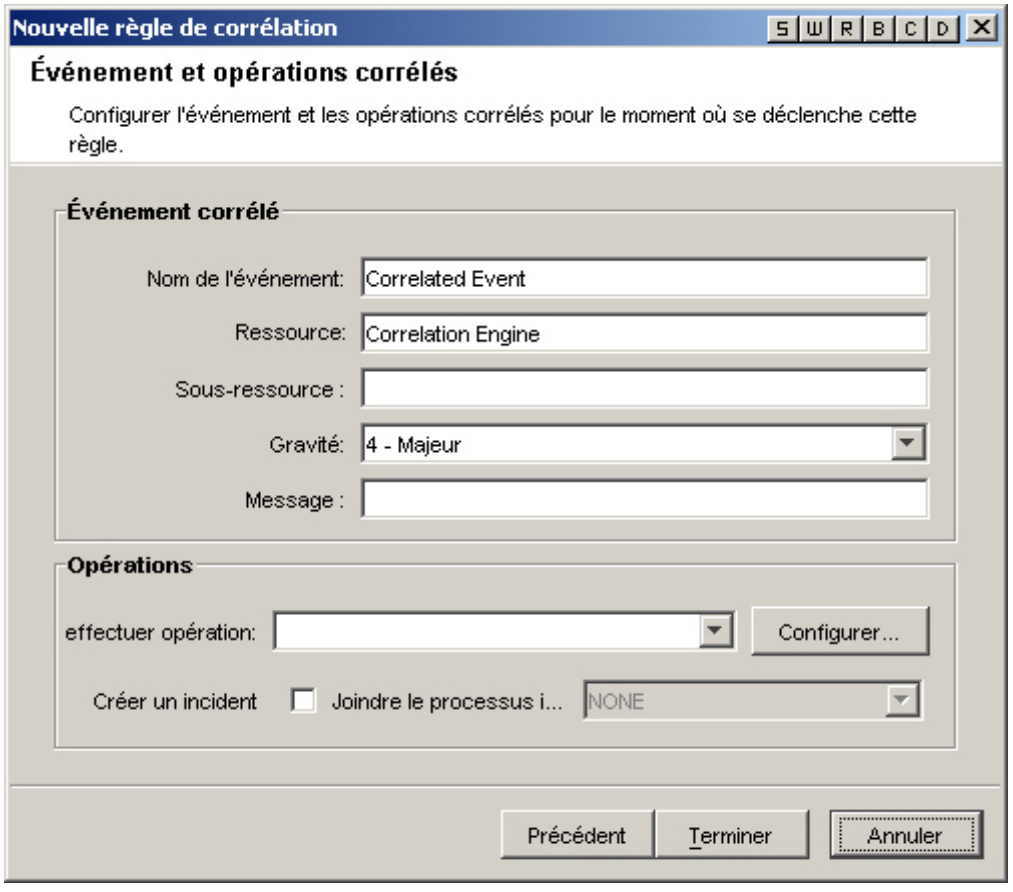
REMARQUE : lorsque la valeur indiquée est 0, la règle est déclenchée immédiatement. Pour une corrélation de base, l'événement se produit une seule fois lorsque le délai indiqué est de 0.

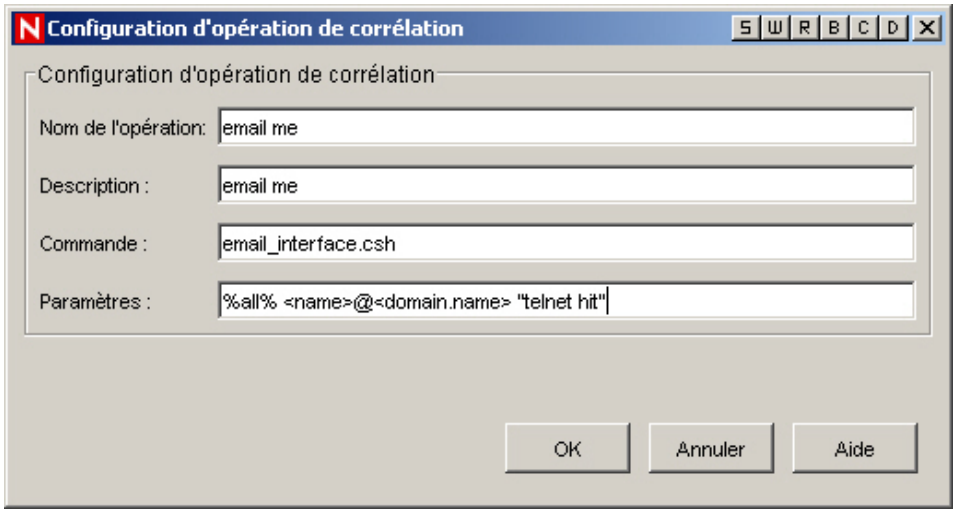
- Page Seuil et critères de regroupement (moitié inférieure de la fenêtre) : établit une corrélation en fonction de regroupements entre les balises META ci-après. Pour cela, sélectionnez les balises META à regrouper pour établir une corrélation. Les événements sont placés dans des groupes selon les balises META sélectionnées.

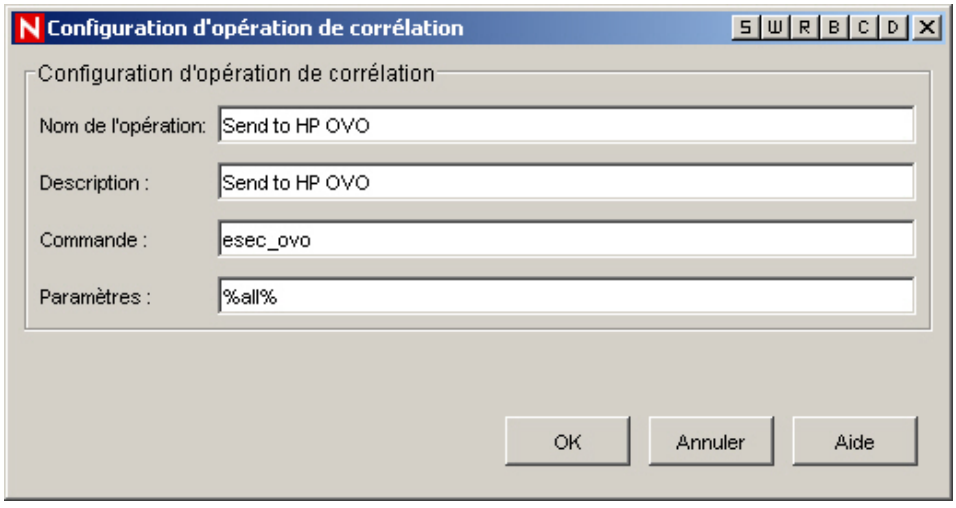
- Page Événements et opérations corrélés : cette fenêtre permet de définir l'action automatiquement appliquée lorsque des événements correspondent à la règle de corrélation concernée. Seul le niveau de gravité est obligatoire. Par défaut, il est défini sur 4.
  - Nom de l'événement : par défaut, le nom de l'événement est celui de l'événement corrélé. Il s'agit du nom textuel de l'événement corrélé.
  - Ressource : par défaut, moteur de corrélation Il s'agit du nom textuel de la ressource dans le système.
  - Sous-ressource : par défaut, <Aucun>. Cela vaut pour toutes les ressources contenant plusieurs sous-ressources.
  - Définir le niveau de gravité sur : la valeur par défaut est 4. Il s'agit du niveau de gravité attribué par défaut à l'événement. Les valeurs valides sont 0, 1, 2, 3, 4 (valeur par défaut) et 5. Une liste déroulante qui affiche tous les niveaux de gravité valides est disponible.
  - Texte de message personnalisé : la valeur par défaut est <Aucun>. Il s'agit du texte qui s'affiche en même temps que l'événement. Il sert à identifier la condition qui a déclenché la règle de liste de surveillance. Le nombre maximal de caractères autorisé

est de 4 000. Le texte entré dans cette zone est placé devant celui de l'événement corrélé et séparé de lui par une barre verticale. Par exemple, si vous entrez le texte « Nouveau message », le message de corrélation apparaît sous la forme « Nouveau message|Trois instances de... ».

- Exécuter cette commande (Oracle uniquement) : la valeur par défaut est <Aucun>. Il s'agit du nom d'un fichier exécutable qui démarre dès que la règle de liste de surveillance est déclenchée. Ce fichier doit se trouver dans le répertoire $ESEC_HOME/sentinel/exec et doit pouvoir être exécuté par l'utilisateur esecadm. Aucune validation n'est effectuée pour la valeur entrée dans cette zone de texte de format libre. Vous pouvez indiquer les balises META que vous souhaitez intégrer au fichier exécutable.
- Effectuer l'opération (MSSQL uniquement) : la valeur par défaut est <Aucun>. Il s'agit du nom d'un fichier exécutable qui démarre dès que la règle de liste de surveillance est déclenchée. Ce fichier doit se trouver dans le répertoire %ESEC_HOME%\sentinel\bin et doit pouvoir être exécuté par l'utilisateur esecadm. Aucune validation d'entrée n'est effectuée. Vous pouvez indiquer les balises META que vous souhaitez intégrer au fichier exécutable. Dans le premier des deux exemples suivants, la règle de corrélation entraîne l'envoi d'un courrier électronique. Dans le deuxième, la règle de corrélation entraîne l'envoi d'un événement à HP OVO (HP OpenView Operations).







REMARQUE : pour plus d'informations sur les commandes et les paramètres, reportez-vous au « Chapitre 5 : Balises META de Wizard et de Sentinel » du guide des références utilisateur ainsi qu'à la section Sortie de corrélation du présent document.

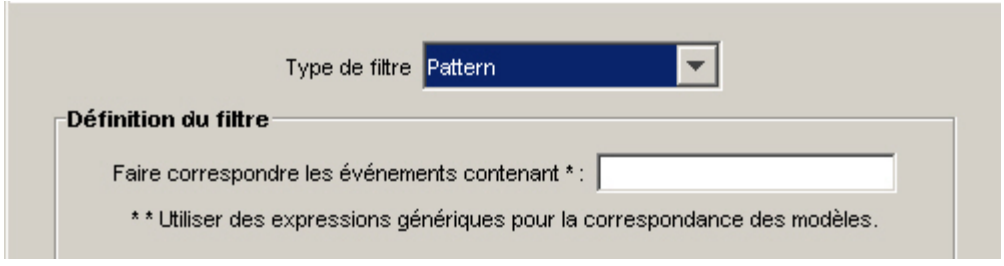
- Créer un incident : la création d'un incident fait partie des actions possibles pour un événement corrélé.
- Attacher le processus iTRAC : un processus iTrac peut être associé à un incident.

Création d'une règle de corrélation avancée

Une règle de corrélation avancée vous permet de créer des règles plus complexes, car vous pouvez ajouter une condition dans la fenêtre Critères supplémentaires, ce qui revient à ajouter un niveau logique de type « et » à la définition de la règle.

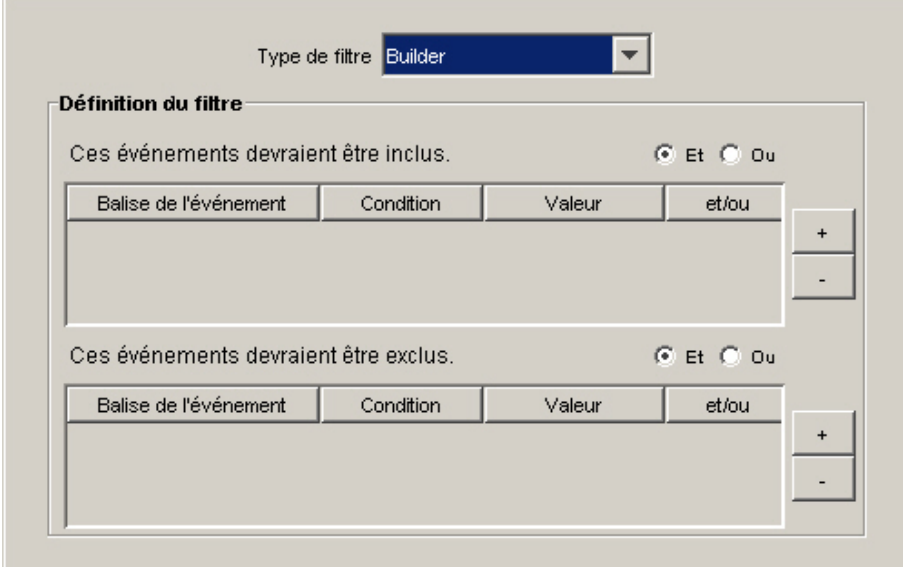
Pour compter le nombre de fois que certaines conditions sont remplies sur une durée déterminée ainsi que pour recevoir une alerte lorsque des événements remplissent également des critères impliqués dans des événements passés, vous pouvez créer une règle de corrélation avancée. Les étapes de la procédure sont les suivantes :

- Sélectionnez Advanced Correlation Rule (Règle de corrélation avancée) dans la première fenêtre de l'assistant de règle de corrélation. Entrez les informations requises suivantes :
  - Nom de la règle : nom qui s'affiche dans la liste des règles. Nombre maximal de caractères autorisés : 255. Les points (.) ne sont pas autorisés. Les caractères ASCII du code étendu ne sont pas autorisés. Une distinction entre les majuscules et les minuscules est faite pour les noms de règles.
  - Description : bref descriptif de 1 024 caractères au maximum.
- Type du filtre :
  - Allow All (Tout autoriser)
  - Pattern (Modèle)



  - Gestionnaire de filtres - ({ownerid}:{Filter name}:<Nom du champ>

  - Builder (Générateur)



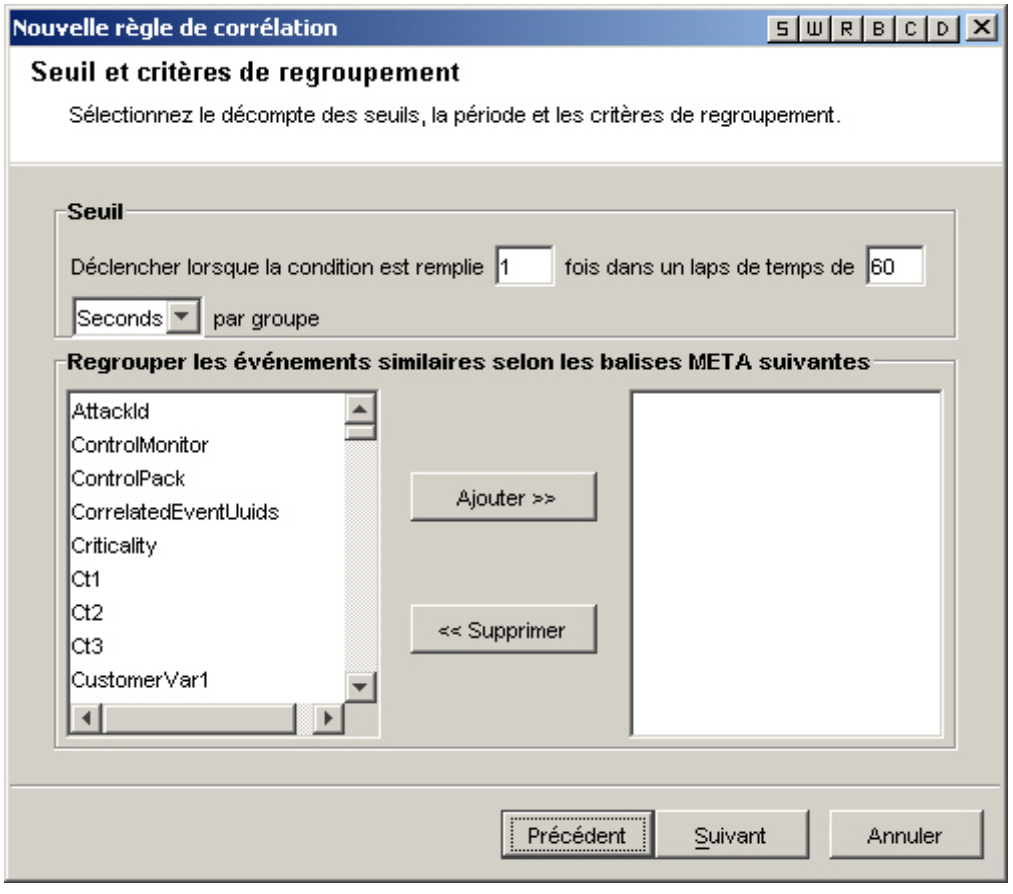
- Critères supplémentaires : cette option vous permet d'entrer des critères de correspondance pour plusieurs événements entrant dans le système dans un certain laps de temps.

La valeur par défaut est 60 secondes. Cette option est constituée à la fois d'une zone d'entrée de variable et d'une liste déroulante. Les options proposées par la liste déroulante sont les suivantes : secondes, minutes, heures et jours.

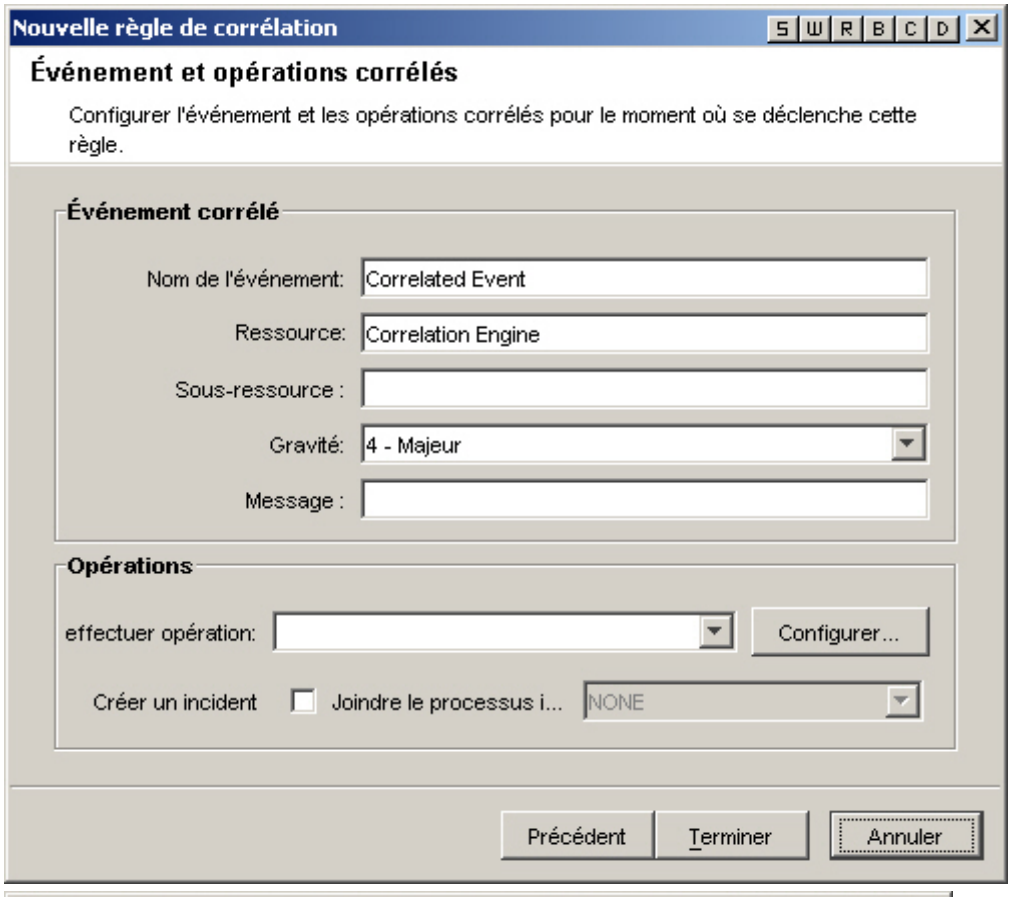
- Seuil et critères de regroupement (moitié supérieure de la fenêtre) : Activer la règle : - Cette option vous permet d'entrer des critères de correspondance pour plusieurs événements entrant dans le système dans un certain laps de temps.
  - Lorsque la condition est remplie _fois : la valeur par défaut est 1. Il faut que la condition ait été détectée autant de fois que spécifié pour qu'une règle soit déclenchée. La valeur minimale à entrer pour ce seuil est 1.
  - dans (délai) : la valeur par défaut est 60 secondes. En indiquant une valeur pour cette option, la condition se retrouve liée à la période indiquée. Cette option est constituée à la fois d'une zone d'entrée de variable et d'une liste déroulante. Les options proposées par la liste déroulante sont les suivantes : secondes, minutes, heures et jours.

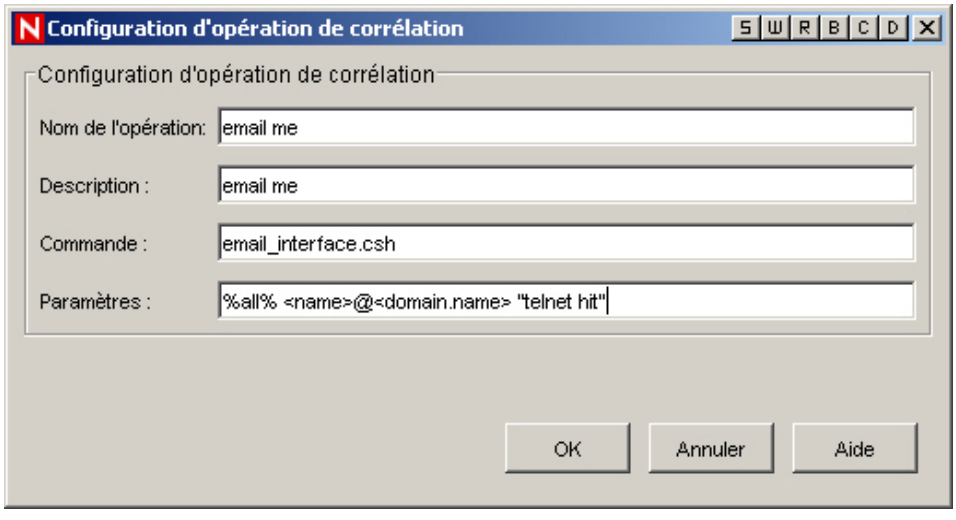
REMARQUE : lorsque la valeur indiquée est 0, la règle est déclenchée immédiatement. Pour une corrélation de base, l'événement se produit une seule fois lorsque le délai indiqué est de 0.

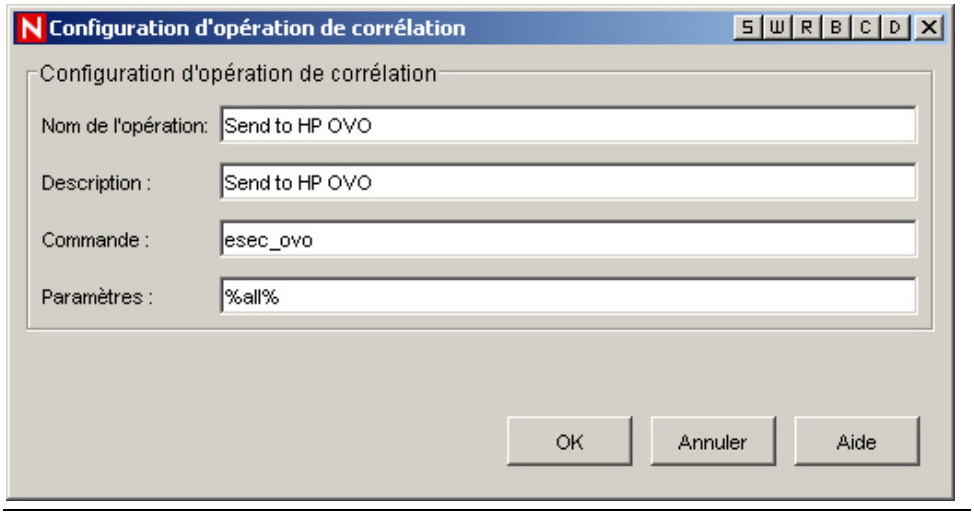
- Page Seuil et critères de regroupement (moitié inférieure de la fenêtre) : établit une corrélation en fonction de regroupements entre les balises META ci-après. Pour cela, sélectionnez les balises META à regrouper pour établir une corrélation. Les événements sont placés dans des groupes selon les balises META sélectionnées.



- Page Événements et opérations corrélés : cette fenêtre permet de définir l'action automatiquement appliquée lorsque des événements correspondent à la règle de corrélation concernée. Seul le niveau de gravité est obligatoire. Par défaut, il est défini sur 4.
  - Nom de l'événement : par défaut, le nom de l'événement est celui de l'événement corrélé. Il s'agit du nom textuel de l'événement corrélé.
  - Ressource : par défaut, moteur de corrélation Il s'agit du nom textuel de la ressource dans le système.
  - Sous-ressource : par défaut, <Aucun>. Cela vaut pour toutes les ressources contenant plusieurs sous-ressources.
  - Définir le niveau de gravité sur : la valeur par défaut est 4. Il s'agit du niveau de gravité attribué par défaut à l'événement. Les valeurs valides sont 0, 1, 2, 3, 4 (valeur par défaut) et 5. Une liste déroulante qui affiche tous les niveaux de gravité valides est disponible.
  - Texte de message personnalisé : la valeur par défaut est <Aucun>. Il s'agit du texte qui s'affiche en même temps que l'événement. Il sert à identifier la condition qui a déclenché la règle de liste de surveillance. Le nombre maximal de caractères autorisé est de 4 000. Le texte entré dans cette zone est placé devant celui de l'événement corrélé et séparé de lui par une barre verticale. Par exemple, si vous entrez le texte « Nouveau message », le message de corrélation apparaît sous la forme « Nouveau message|Trois instances de... ».
  - Exécuter cette commande (Oracle uniquement) : la valeur par défaut est <Aucun>. Il s'agit du nom d'un fichier exécutable qui démarre dès que la règle de liste de surveillance est déclenchée. Ce fichier doit se trouver dans le répertoire $ESEC_HOME/sentinel/exec et doit pouvoir être exécuté par l'utilisateur esecadm. Aucune validation n'est effectuée pour la valeur entrée dans cette zone de texte de format libre. Vous pouvez indiquer les balises META que vous souhaitez intégrer au fichier exécutable.
  - Effectuer l'opération (MSSQL uniquement) : la valeur par défaut est <Aucun>. Il s'agit du nom d'un fichier exécutable qui démarre dès que la règle de liste de surveillance est déclenchée. Ce fichier doit se trouver dans le répertoire %ESEC_HOME%\sentinel\bin et doit pouvoir être exécuté par l'utilisateur esecadm. Aucune validation d'entrée n'est effectuée. Vous pouvez indiquer les balises META que vous souhaitez intégrer au fichier exécutable. Dans le premier des deux exemples suivants, la règle de corrélation entraîne l'envoi d'un courrier électronique. Dans le deuxième, la règle de corrélation entraîne l'envoi d'un événement à HP OVO (HP OpenView Operations).


Nouvelle règle de corrélation
Événement et opérations corrélés
Configurer l'événement et les opérations corrélés pour le moment où se déclenche cette règle.
Événement corrélé
Nom de l'événement: Correlated Event
Ressource: Correlation Engine
Sous-ressource :
Gravité: 4 - Majeur
Message :
Opérations
effectuer opération:
Configurer...
Créer un incident
Joindre le processus i...
NONE
Précédent
Terminer
Annuler


Configuration d'opération de corrélation
Configuration d'opération de corrélation
Nom de l'opération: email me
Description : email me
Commande : email_interface.csh
Paramètres : %all% <name>@<domain.name> "telnet hit"
OK
Annuler
Aide



REMARQUE : pour plus d'informations sur les commandes et les paramètres, reportez-vous au « Chapitre 5 : Balises META de Wizard et de Sentinel » du guide des références utilisateur ainsi qu'à la section Sortie de corrélation.

- Créer un incident : la création d'un incident fait partie des actions possibles pour un événement corrélé.
- Attacher le processus iTRAC : un processus iTrac peut être associé à un incident.

Création d'une règle de corrélation RuleLg de format libre

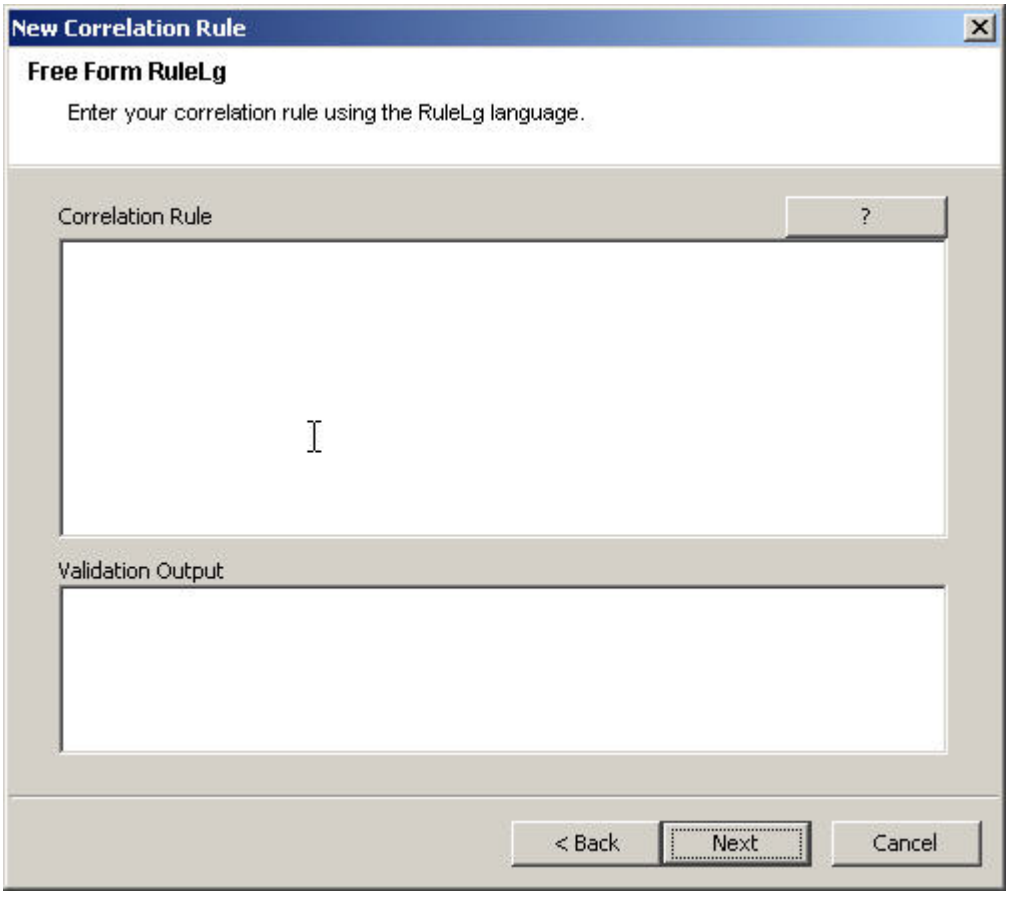
Le moteur de corrélation est construit selon trois opérations fondamentales. Ces opérations sont combinées pour former une règle à l'aide des opérateurs flow, union et intersection. Les trois opérations fondamentales sont les suivantes :

- Opération filter
- Opération window
- Opération trigger

ATTENTION : si vous avez renommé une balise, n'utilisez pas le nom d'origine pour créer une règle de corrélation.

Le langage de règle reflète directement ces opérations et la façon dont elles peuvent être combinées intuitivement pour définir des règles de corrélation. Ces opérations ont été conçues et implémentées pour des performances élevées. Elles fonctionnent à partir d'un ensemble d'événements : réception d'un groupe d'événements d'entrée et retour d'un groupe d'événements. L'événement en cours de traitement par une règle revêt souvent une signification spéciale en termes de sémantique du langage. L'événement en cours fait toujours partie du groupe d'événements à l'intérieur et à l'extérieur d'une opération, sauf si le groupe est vide. Si un groupe d'entrée d'une opération est vide, l'opération n'est pas évaluée.

Pour simplifier, considérons qu'une règle de corrélation traite les événements entrant dans le moteur de corrélation de manière sérialisée, un par un. En réalité, le moteur de corrélation est capable de traiter plusieurs événements et d'évaluer plusieurs règles à la fois pour un même événement.



Opération filter

Une opération filter (expression booléenne) permet d'appliquer un filtre en fonction du contenu de l'événement en cours, à savoir des valeurs de ses balises META et de l'expression booléenne spécifiée via le filtre. La sortie d'une opération filter est l'ensemble d'événements vide (si l'événement en cours ne correspond pas au filtre) ou un ensemble contenant l'événement en cours et tous les autres événements du groupe entrant.

- Les filtres s'appliquent sur l'événement en cours de traitement et en évaluent l'expression booléenne :
  - L'opération filter retourne le groupe d'entrée si l'expression booléenne se vérifie.
  - L'opération filter retourne le groupe vide si l'expression booléenne ne se vérifie pas.
- L'expression booléenne est composée d'instructions de comparaison et de mise en correspondance et comprend les opérateurs booléens « et », « ou » et « non ».

Opération filter : Priorité et association des opérateurs RuleLg

Ordre de priorité de l'opérateur booléen filter (du plus élevé [haut] au plus bas [bas]) :

Opérateur	Signification	Type d'opérateur	Associations
Non	Non logique	Unaire	Aucune
Et	Et logique	Binaire	De gauche à droite
Ou	Ou logique	Binaire	De gauche à droite

Les règles suivantes s'appliquent :

- Les instructions de comparaison permettent de comparer des valeurs de balises META d'événements avec d'autres valeurs ou constantes de balises META d'événements.
- Les opérateurs de comparaison disponibles sont : =, !=, >, <, >=, <=.
- Les instructions de mise en correspondance disponibles sont match regex() pour la mise en correspondance d'expressions rationnelles et match subnet() pour la mise en correspondance de sous-réseaux.
- Les instructions de comparaison et de mise en correspondance peuvent être imbriquées par l'utilisation de parenthèses à n'importe quel niveau de profondeur.
- Le nom des balises META dans les instructions de comparaison et de mise en correspondance doit toujours commencer par « e. » pour spécifier l'événement en cours.
- Si un filtre constitue la dernière ou la seule opération d'une règle de corrélation,
- le groupe de sortie du filtre est utilisé pour concevoir un événement corrélé, les événements corrélés étant le groupe d'événements de sortie de l'opération de filtrage (événement en cours en premier).
- Si un filtre ne constitue pas la dernière opération d'une règle de corrélation (à savoir qu'un opérateur flow se trouve à sa droite), le groupe de sortie d'un filtre est utilisé comme groupe d'entrée dans les autres opérations (via l'opérateur flow).

Par exemple : Si l'événement en cours de traitement présente un niveau de gravité égal à 4 et que la balise META des ressources contient « FW » ou « Comm », un événement corrélé est envoyé avec l'événement en cours (événement unique) comme événement corrélé.

```
filter(e.sev = 4 and (e.res match regex ("FW") or e.res
   match regex ("Comm")))
```

Si l'une des balises META de l'événement en cours contient « ABC », un événement corrélé est envoyé avec l'événement en cours (événement unique) comme événement corrélé.

```
filter(e.all match regex("ABC"))
```

Opération window

Une opération window (expression booléenne simple[, expression de filtre], durée) porte sur l'événement en cours par rapport à une fenêtre d'événements passés. Les événements passés sont conservés par l'opération window elle-même. La sortie d'une opération window est le groupe vide (si l'événement en cours ne correspond pas à l'expression booléenne simple) ou un groupe contenant l'événement en cours et tous les événements passés, pour lesquels l'expression booléenne simple est vérifiée.

L'expression booléenne simple constitue une instruction de comparaison unique ou une instruction de mise en correspondance unique entre une valeur de balise META d'un événement passé et une

valeur ou une constante de balise META d'événement en cours.
Pour les expressions booléennes :

- Vous devez ajouter « e. » devant le nom d'une balise META pour spécifier l'événement en cours ou « w. » pour spécifier les événements passés.
- Les opérateurs de comparaison disponibles sont =, !=, >, <, >=, <=, « dans » et « n'est pas dans ».
- Les instructions de mise en correspondance disponibles sont match regex() pour la mise en correspondance d'expressions rationnelles et match subnet() pour la mise en correspondance de sous-réseaux.
- La mention « w.[balise META] » doit être présente dans une expression booléenne simple d'opération window.
- Si un évènement passé correspond à un événement en cours lors d'une évaluation à l'aide de l'expression booléenne simple, le groupe de sortie contient l'événement entrant ainsi que toutes les correspondances présentes dans la fenêtre d'événements.
- Si aucun événement de la fenêtre ne correspond à l'événement en cours pour l'expression booléenne simple, un groupe vide est généré en sortie.

Les événements passés sont conservés pendant la durée spécifiée pour l'opération window.

Le paramètre d'expression de filtre facultatif d'une fenêtre vous permet de contrôler les événements que la fenêtre conserve. Cette expression peut être n'importe quel filtre valide.

- Chaque événement entrant dans le moteur de corrélation et qui passe à travers ce filtre est placé dans la fenêtre des événements passés.
- S'il n'existe aucune expression de filtre, tous les événements entrant dans le moteur de corrélation sont conservés par la fenêtre.
- L'événement en cours est placé dans la fenêtre une fois que l'évaluation de type window pour l'événement en cours est terminée.
- Seuls les composants pertinents des événements passés sont effectivement conservés par la fenêtre (pour limiter l'utilisation de mémoire).

Si une fenêtre constitue la dernière ou la seule opération d'une règle de corrélation, le groupe de sortie de la fenêtre est utilisé pour concevoir un événement corrélé, les événements corrélés étant le groupe d'événements de sortie de l'opération de filtrage (événement en cours en premier).

Exemple 1

```
window(e.sip = w.sip, filter(e.sip match subnet
   (<xxx.xxx.x.x/yy>)), 60)
```

Dans l'exemple ci-dessus, si l'événement en cours comporte une adresse IP source de type xxx.xxx.x.x/yy avec un masque de sous-réseau CIDR (Classless Inter-Domain Routing - Routage inter-domaine sans classes) et qu'il correspond à un ou plusieurs événements qui se sont produits dans les 60 secondes précédentes, un événement corrélé est envoyé avec l'événement en cours et tout événement passé correspondant comme événements corrélés (événement en cours en premier).

Exemple 2

```
window(e.sip = w.dip, 3600) intersection
window(e.dp = w.dp, 3600) intersection
window(e.evt = w.evt, 3600)
```

La règle utilisée ci-avant est de type domino. Un attaquant exploite un système vulnérable et l'utilise comme plate-forme d'attaque.

Exemple 3

```
filter(e.sev > 3) flow (window(e.sip = w.sip, filter
   (e.sev >3), 5) intersection window(e.evt = w.evt,
   filter(e.sev >3), 5) intersection window(e.dip =
   w.dip, filter(e.sev >3), 5) intersection window(e.sn!
   = w.sn, filter(e.sev > 3),5)
```

La règle utilisée dans l'exemple ci-dessus est de type interne/externe. Une signature d'attaque est détectée sur deux systèmes de détection d'intrusion, l'un à l'intérieur du pare-feu et l'autre à l'extérieur, et l'attaque présente un niveau de gravité supérieur à 3.

Opération trigger

L'objectif principal d'une opération trigger est de compter un nombre d'événements pendant une durée déterminée. Si le décompte spécifié est atteint dans la durée indiquée, un groupe d'événements contenant tous les événements conservés par le déclencheur est généré en sortie. Dans le cas contraire, un groupe vide est généré en sortie.

- L'opération trigger reçoit en entrée un groupe d'événements à retourner comme partie du groupe d'événements de sortie si le décompte, la durée et le(s) discriminant(s) spécifiés pour les groupes d'entrée précédents et le groupe d'entrée en cours répondent aux critères définis par l'opération trigger.
- Le décompte est un nombre entier précisant le nombre d'événements qui doivent se produire dans la fenêtre de temps pour qu'un groupe non vide soit généré en sortie.
- La durée est un nombre entier exprimé en secondes qui spécifie la durée pendant laquelle les événements sont conservés par l'opération trigger.
- Si la durée est égale à zéro, une opération trigger compare simplement le nombre d'événements du groupe d'entrée au décompte, puis génère en sortie l'événement en cours si ce nombre est supérieur ou égal au décompte.
- À la réception d'un nouveau groupe d'événements d'entrée, un déclencheur ignore d'abord les événements périmés (événements ayant été conservés pendant un laps de temps supérieur à la durée spécifiée), puis insère l'événement en cours.
  Si le nombre d'événements résultants est supérieur ou égal au décompte spécifié, le déclencheur génère en sortie un groupe contenant tous les événements.
- Si un déclencheur constitue la dernière ou la seule opération d'une règle de corrélation, le groupe de sortie de l'opération trigger est utilisé pour concevoir un événement corrélé, les événements corrélés étant le groupe d'événements de sortie de l'opération trigger (événement en cours en premier).
- Si un déclencheur ne correspond pas à la dernière opération d'une règle de corrélation (à savoir qu'un opérateur flow se trouve à sa droite), le groupe de sortie d'un déclencheur est utilisé comme groupe d'entrée dans les autres opérations (via l'opérateur flow).
- Les critères d'une opération trigger étant satisfaits une première fois (l'opération trigger génère en sortie un groupe d'événements), le moteur de corrélation ne génère pas de nouvel événement corrélé mais une mise à jour de l'événement corrélé précédent si les critères sont de nouveau satisfaits, qu'ils contiennent au moins un des événements de sortie précédemment générés et que le déclencheur constitue la dernière ou la seule opération effectuée.
- Le discriminant (liste de balises META) est une liste de balises META séparées par une virgule. Une opération trigger conserve différents décomptes pour chaque combinaison des balises META du discriminant.

Par exemple, si 5 événements comportant la même adresse IP source se produisent dans un laps de temps de 10 secondes, envoyez un événement corrélé avec ces 5 événements comme événements corrélés (événement en cours en premier).

```
trigger(5,10,discriminator(e.sip))
```

Bien que vous ayez la possibilité de créer des expressions extrêmement complexes grâce aux règles de format libre, ces dernières ne sont pas nécessairement compréhensibles. Habituellement, une expression RuleLg se compose de trois parties : la section filter, la section window et la section trigger. Ces trois sections sont ensuite reliées à l'aide d'un opérateur flow.

La section filter peut contenir plusieurs filtres connectés.

Exemple :

```
(filter(e.sev = 5) union filter(e.sev =4))
(filter(e.sev = 5 or e.sev =4))
```

REMARQUE : cette section est facultative. Lorsqu'elle n'est pas utilisée, elle équivaut à l'expression filter(1=1).

La section window peut contenir plusieurs fenêtres dont les valeurs se croisent.

Exemple :

(window(w.sev = e.sev,10) intersection window(w.sip = e.sip,10))

REMARQUE : cette section est facultative.

La section trigger peut contenir une opération de déclencheur.

Exemple

```
(trigger(5,10))
```

REMARQUE : cette section est facultative. Lorsque cette section n'est pas utilisée, la règle se comporte comme si elle se terminait par l'expression « trigger(1,0) ».

Opérateurs à associer à des opérations pour créer des règles

Les opérateurs qu'il est possible d'associer à des opérations pour créer des règles sont les suivants :

- Opérateur flow
- Opérateur union
- Opérateur intersection

L'ordre de priorité de l'opérateur des opérations filtrer, window et trigger est le suivant (du plus élevé [haut] au plus bas [bas]) :

Opérateur	Signification	Type d'opérateur	Associations
flow	Le groupe de sortie devient le groupe d'entrée.	Binaire	De gauche à droite
intersection	Définit l'intersection (supprime les doublons).	Binaire	De gauche à droite
union	Définit l'union (supprime les doublons).	Binaire	De gauche à droite

Opérateur flow

Le groupe d'événements de sortie de l'opération située à gauche correspond au groupe des événements d'entrée pour l'opération située à droite.

Par exemple :

```
filter(e.sev = 5) flow trigger(3, 60)
```

La sortie de l'opération de filtre correspond aux données d'entrée de l'opération de déclencheur.
Le déclencheur compte uniquement les événements d'un niveau de gravité égal à 5.

Opérateur union

Il s'agit de l'union du groupe de sortie de l'opération située à gauche et de celui de l'opération située à droite. Le groupe de sortie résultant contient des événements du groupe de sortie de l'opération située à gauche ou du groupe de sortie de l'opération située à droite, sans doublons.

Par exemple :

```
filter(e.sev = 5) union filter(e.sip = 192.168.0.1)
```

équivaut à :

```
filter(e.sev = 5 or e.sip = 192.168.0.1)
```

Opérateur intersection

Il s'agit de l'intersection du groupe de sortie de l'opération située à gauche et de celui de l'opération située à droite. Le groupe de sortie résultant contient des événements communs au groupe de sortie de l'opération située à gauche et au groupe de sortie de l'opération située à droite, sans doublons.

Par exemple :

```
filter(e.sev = 5) intersection filter(e.sip =
   192.17.16.32)
```

équivaut à :

```
filter(e.sev = 5 and e.sip = 192.17.16.32)
```

Exemples de règles de corrélation

Cette section fournit un ensemble d'exemples de règles de corrélation ainsi que les conditions requises pour que ces règles fonctionnent correctement. Vos règles sont susceptibles de différer selon le système d'exploitation que vous utilisez.

Les balises e.rv50 à e.rv53 faisant partie des exemples de règles RuleLg correspondent aux assignations définies dans les fichiers d'assignation du collecteur. Par exemple, si vous ouvrez le fichier windows_v2000_mapv*.csv ou snort_v20_mapv*.csv :

- la colonne Culture correspond à la balise e.rv50 ;
- la colonne Community (Communauté) correspond à la balise e.rv51 ;
- la colonne Family (Famille) correspond à la balise e.rv52 ;
- la colonne Event (Événement) correspond à la balise e.rv53.
-

Par exemple :

```
filter (e.rv52 = "Worm") flow trigger (3, 300)
```

Cette règle fait référence à la taxinomie NIDS (Network Intrusion Detection System - Système de détection d'intrusion réseau). Si vous vous référez à la colonne Family (Famille) du fichier d'assignation Snort, vous pouvez voir plus d'une quarantaine d'occurrences du terme Worm (ver). Cette règle est capable de se déclencher pour plus de quarante attaques de vers informatiques si elles se produisent trois fois en cinq minutes.

Voici des types d'attaque possibles pour les exemples de règles de corrélation :

- Attaques en force - source et cible sont identiques
- Dépassement de mémoire tampon - même source vers une même cible
- Dépassement de mémoire tampon - arrêt du service
- Refus de service
- Échecs de connexion - toute source vers toute destination
- Échecs de connexion - même source vers même destination
- Microsoft - accès anonyme
- Microsoft - authentification Windows
- Microsoft - IE
- Microsoft – IIS
- Microsoft - authentification LAN Manager
- Microsoft – MDAC
- Microsoft - accès à distance du registre
- Microsoft– SQL Server
- Microsoft - NETBIOS
- Microsoft - scripts Windows
- Porte dérobée depuis plusieurs sources
- Porte dérobée depuis une source unique
- Cheval de Troie
- UNIX - serveur Web Apache
- UNIX - BIND/DNS
- UNIX - FTP
- UNIX - authentification en général
- UNIX - démon d'impression
- UNIX - appels de procédure à distance
- UNIX - services distants
- UNIX - secure shell
- UNIX - sendmail
- UNIX – SNMP
- Détection de virus
- Détection de vers informatiques

Attaque par dépassement de mémoire tampon et arrêt du service

Cette règle repère une éventuelle brèche de sécurité après une attaque par dépassement de mémoire tampon. Elle déclenche une alerte si l'un des services de la cible de l'attaque s'est arrêté dans les 60 secondes qui ont suivi l'attaque.
Un collecteur basé sur l'hôte, HIDS/OS, peut détecter si un service est en cours d'arrêt. L'attaque par dépassement de mémoire tampon peut être détectée par le collecteur NIDS, HIDS ou OS.

Si un système a été touché par une telle attaque, l'événement doit être examiné avec attention.

Fréquence de la règle	**Conditions requises**	**Taxinomie de la règle**
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS) ▪ Plates-formes HIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS HIDS/OS

Syntaxe RuleLg pour cette règle

```
filter ((e.rv51 = "Service" and e.rv52 = "Stop" ) and
   (e.st = "H")) flow window (w.dip = e.sip, filter
   (e.rv52 = "Buffer_Overflow"), 60) flow trigger(1, 0)
```

Attaque par refus de service et arrêt du service

Cette règle repère une éventuelle brèche de sécurité après une attaque par refus de service. Elle déclenche une alerte si l'un des services de la cible de l'attaque s'est arrêté dans les 60 secondes qui ont suivi l'attaque. L'arrêt du service est détecté par un collecteur basé sur l'hôte, à savoir HIDS/OS. L'attaque par dépassement de mémoire tampon peut être détectée par les collecteurs NIDS, HIDS ou OS.

Si un système a été touché par une telle attaque, l'événement doit être examiné avec attention.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS) ▪ Plates-formes HIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS HIDS/OS

Syntaxe RuleLg pour cette règle

```
filter ((e.rv51 = "Service" and e.rv52 = "Stop" ) and
   (e.st = "H")) flow window (w.dip = e.sip, filter
   (e.rv52 ="DoS" ), 60) flow trigger(1, 0)
```

Détection de virus

Cette règle permet de repérer si un virus connu attaque un système au sein d'uneinfrastructure.

Lorsque le virus attaque, un ou plusieurs systèmes peuvent être touchés, ce qui entraîne le redémarrage complet du système et des applications ou la perte définitive du matériel. La détection d'un virus en cours d'exécution permet d'empêcher ou de limiter de manière significative les pertes.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
3 fois en 5 minutes	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv52 ="Virus") flow trigger (3, 300)
```

Détection de vers informatiques

Cette règle permet de repérer si un ver connu s'est infiltré dans un système au sein d'une infrastructure.

Lorsque le ver attaque, un ou plusieurs systèmes peuvent être touchés, ce qui oblige à redémarrer entièrement le système et les applications ou qui entraîne la perte définitive du matériel.
La détection d'un ver en cours d'exécution permet de limiter de manière significative la responsabilité de l'entreprise en cas de dommages.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
3 fois en 5 minutes	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv52 = "Worm") flow trigger (3, 300)
```

Détection de chevaux de Troie

Cette règle permet de repérer si un cheval de Troie connu s'est introduit dans un système au sein d'une infrastructure.

Lorsqu'un cheval de Troie parvient à contaminer le système voulu, ce dernier peut être sérieusement mis à mal.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
3 fois en 5 minutes	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS) ▪ Plates-formes HIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS HIDS/OS

Syntaxe RuleLg pour cette règle

```
filter (e.rv52 ="Trojan") flow trigger (3, 500)
```

Attaques répétées par porte dérobée depuis une source unique

Cette règle établit une corrélation pour des tentatives répétées d'insertion ou d'exécution d'une porte dérobée depuis une seule source.

Un programme de porte dérobée s'utilise généralement pour s'emparer du contrôle total d'un système cible et de là, lancer d'autres attaques. La règle correspondante repère les imposteurs qui recherchent un système infecté ou essaient d'en infecter un.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
5 fois en 2 minutes	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS) ▪ Plates-formes HIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS HIDS/OS

Syntaxe RuleLg pour cette règle

```
filter (e.rv50 = "Attack" and e.rv52 = "Backdoor" ) flow
   trigger(5, 120, discriminator (e.sip))
```

Attaques répétées par porte dérobée depuis plusieurs sources

Cette règle établit une corrélation pour des tentatives répétées d'insertion ou d'exécution coordonnée d'une porte dérobée depuis plusieurs systèmes avec une seule cible pour objectif.

Un programme de porte dérobée s'utilise généralement pour s'emparer du contrôle total d'un système cible et de là, lancer d'autres attaques. La règle correspondante permet de déterminer si :

- le système cible a été infecté ;
- l'imposteur essaie de se servir du système infecté ;
- l'imposteur tente de brouiller les pistes en procédant à une attaque coordonnée ;
- ou, l'imposteur a repéré que la cible était vulnérable face à ce type d'attaque. Si tel est le cas, il est possible que l'imposteur s'en soit rendu compte en passant par une source interne.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
5 fois en 2 minutes	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS) ▪ Plates-formes HIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS HIDS/OS

Syntaxe RuleLg pour cette règle

```
filter (e.rv50 = "Attack" and e.rv52 = "Backdoor" ) flow
   trigger( 5, 120, discriminator(e.dip))
```

Échecs répétés de connexion d'une source vers une destination

Cette règle détecte les échecs de connexion à des systèmes d'un même type.

Des échecs de connexion répétés vers un même type de compte ou de système peut indiquer qu'un imposteur connaît déjà le réseau et les systèmes critiques installés sur ce réseau. Cette configuration doit déclencher une alerte. Plus l'imposteur possède d'informations, plus il lui est aisé de trouver un système dont il peut se servir.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
5 fois en 2 minutes	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter ((e.rv52 = "Access" or e.rv52 = "Brute_Force") and
   e.rv51 = "User" and e.rv50 = "Attack") flow trigger
   (5, 120)
```

Échecs répétés de connexion d'une même source vers une même destination

Cette règle détecte les échecs de connexion répétés d'une même source à une même destination.

Des échecs de connexion répétés vers un même type de compte ou de système peut indiquer qu'un imposteur connaît déjà le réseau et les systèmes critiques installés sur ce réseau. Cette configuration doit déclencher une alerte. Plus l'imposteur possède d'informations, plus il lui est aisé de trouver un système dont il peut se servir.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
3 fois en 5 minutes	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter ((e.rv52 = "Access" or e.rv52 = "Brute_Force") and
   e.rv51 = "User" and e.rv50 = "Attack") flow trigger
   (5, 120, discriminator (e.sip, e.dip))
```

Attaque par dépassement de mémoire tampon d'une même source vers une même cible

Cette règle détecte une attaque par dépassement de mémoire tampon provenant d'une même adresse IP et visant une même adresse IP.

Les attaques par dépassement de la mémoire tampon sont les plus courantes sur un réseau et sont utilisées pour mettre à mal un système. Ces types d'attaque peuvent uniquement être bloqués au niveau du périmètre. L'identification du système qui est à l'origine de l'attaque facilite son blocage.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
5 fois en 3 minutes	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS) ▪ Plates-formes HIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS HIDS/OS

Syntaxe RuleLg pour cette règle

```
filter (e.rv52 ="Buffer_Overflow" ) flow trigger (5, 180,
   discriminator (e.sip, e.dip))
```

Succès des attaques en force lorsque source et cible sont identiques

Cette règle est capable d'identifier un système infiltré par cassage du mot de passe.

Des essais ininterrompus de toutes les combinaisons de noms d'utilisateur et de mots de passe possibles pour accéder à un système, suivis d'une éventuelle réussite de connexion indique qu'un imposteur dispose peut-être d'un accès
au système suite à une attaque en force. Si cette attaque réussit, le compte auquel l'imposteur a accédé doit être fermé.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois en 3 minutes	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS) ▪ Plates-formes HIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS HIDS/OS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53="Other" and rv52="Access" e.rv51 ="User"
   and e.rv50="Prob" and e.
   st = "H") flow window (w.dip = e.sip, filter
   (e.rv52="Brute Force" and e.rv50="Compromise"), 180)
   flow trigger(1, 180, discriminator(e.sip, e.dip))
```

Microsoft : vérification d'attaques touchant les services Internet (IIS)

Cette règle prend en charge les 10 attaques les plus courantes contre les services IIS de Microsoft selon l'Institut SANS. Si vous utilisez l'application IIS de Microsoft, votre système peut être vulnérable face à ce type d'attaque.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_IIS") flow trigger(1,60)
```

Microsoft Data Access Connector (MDAC) : vérification d'attaques touchant les services de données distants

Cette règle prend en charge les 10 attaques les plus courantes contre le connecteur MDAC de Microsoft selon l'Institut SANS. L'utilisation de produits Microsoft peut rendre votre système vulnérable face aux attaques. MDAC est un outil sous-jacent servant à intégrer les produits Microsoft.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_MDAC") flow trigger(1,60)
```

Microsoft SQL Server : vérification d'attaques touchant SQL Server

Cette règle prend en charge les 10 attaques les plus courantes contre Microsoft SQL Server selon l'Institut SANS. L'utilisation de Microsoft SQL Server peut rendre votre système vulnérable face aux attaques. Il existe plusieurs vulnérabilités d'un niveau de gravité élevé qui permet aux hackers d'obtenir des informations sensibles, de créer des situations d'alerte au niveau des bases de données, de compromettre les serveurs SQL et les hôtes des serveurs.

Fréquence de la règle	**Conditions requises**	**Taxinomie de la règle**
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_SQLServer") flow trigger(1,60)
```

Microsoft NETBIOS : vérification d'attaques touchant les partages réseau Windows non protégés

Cette règle prend en charge les 10 attaques les plus courantes contre Microsoft NETBIOS selon l'Institut SANS. L'utilisation de NETBIOS pour de la gestion de réseau avec Microsoft peut rendre votre système vulnérable face à une attaque.
À l'origine, NETBIOS était le logiciel de communication en réseau de Microsoft. Les réseaux Microsoft actuels n'utilisent plus NETBIOS comme moyen de transport des données.

Fréquence de la règle	**Conditions requises**	**Taxinomie de la règle**
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_NETBIOS") flow trigger(1,60)
```

Microsoft : vérification d'attaques touchant les sessions Null accessibles de façon anonyme

Cette règle prend en charge les 10 attaques les plus courantes touchant les sessions Null selon l'Institut SANS. Si vous utilisez la session Null de Microsoft, votre système peut être vulnérable face aux attaques. Un utilisateur anonyme peut récupérer des informations en passant par le réseau ou se connecter sans avoir besoin d'authentification.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_NullSessions") flow
   trigger(1,60)
```

Microsoft : vérification d'attaques exploitant la faiblesse du hachage LAN Manager (LM) lors de l'authentification

Cette règle prend en charge les 10 attaques les plus courantes qui exploitent la faiblesse du hachage LAN Manager (LM) selon l'Institut SANS. LM utilise un schéma de chiffrement beaucoup plus vulnérable que les protocoles d'authentification Microsoft actuels (NTLM et NTLMv2) qui rend les mots de passe LM cassables en très peu de temps.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_LM") flow trigger(1,60)
```

Microsoft : vérification d'attaques touchant l'authentification Windows dans son ensemble

Cette règle prend en charge les 10 attaques de mots de passe les plus courantes selon l'Institut SANS. Lorsque des mots de passe faibles sont découverts, ils doivent être changés.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_WeakPasswords") flow
   trigger(1,60)
```

Microsoft : vérification d'attaques touchant Internet Explorer (IE)

Cette règle prend en charge les 10 attaques les plus courantes contre Microsoft Internet Explorer (IE) selon l'Institut SANS. Les versions les plus récentes d'IE ont intégré cette application à l'interface utilisateur du système d'exploitation. Les attaques connues concernant IE peuvent venir de la corruption d'un environnement Microsoft exécuté sous une version ultérieure à Windows 2000.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_IE") flow trigger(1,60)
```

Microsoft : vérification d'attaques touchant l'accès distant au Registre

Cette règle prend en charge les 10 attaques les plus courantes contre le Registre de Microsoft selon l'Institut SANS. Pour un système d'exploitation Microsoft, le Registre correspond à l'emplacement de toutes les variables définies par le système. La possibilité de modifier ou remplacer ce Registre peut porter sérieusement atteinte au bon fonctionnement ou à la sécurité de la plate-forme Microsoft.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_Registry") flow trigger(1,60)
```

Microsoft : vérification d'attaques touchant des scripts Windows

Cette règle prend en charge les 10 attaques les plus courantes contre des scripts Microsoft Windows selon l'Institut SANS. Un certain nombre d'applications Microsoft sont conçues à l'aide du langage de programmation Visual Basic. Étant donné que l'exécution des commandes se fait par script, un imposteur peut accéder et contrôler un système Microsoft en utilisant un script.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_MS_Scripting") flow trigger(1,60)
```

UNIX : vérification d'attaques touchant les appels de procédure à distance (RPC)

Cette règle prend en charge les 10 attaques les plus courantes contre des appels de procédure à distance ou RPC (Remote Procedure Call) sous UNIX selon l'Institut SANS. Un appel de procédure à distance est une méthode permettant, dans un environnement UNIX, d'accéder à des applications ou à des fichiers qui se trouvent sur un système distant (ou de les exécuter) sans authentification. Si vous laissez l'appel de procédure à distance ouvert, n'importe quel utilisateur peut exécuter sur votre système des commandes qui exigent des droits particuliers, et ce, sans autorisation. L'appel de procédure à distance permet donc les attaques à distance.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_RPC") flow trigger(1,60)
```

UNIX : vérification d'attaques touchant le serveur Web Apache

Cette règle prend en charge les 10 attaques les plus courantes contre les serveurs Web Apache selon l'Institut SANS. Le serveur Web Apache est une application gratuite qui permet la prise en charge de différents serveurs Web. L'exécution d'Apache est donc susceptible de rendre votre système vulnérable face à ce type d'attaque.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_Apache") flow trigger(1,60)
```

UNIX : vérification d'attaques touchant Secure Shell

Cette règle prend en charge les 10 attaques les plus courantes contre Secure Shell pour UNIX selon l'Institut SANS. Suite à de nombreux problèmes rencontrés avec Telnet et FTP, Secure Shell a été développé pour chiffrer les échanges entre deux machines. Cette application fournit une méthode sécurisée pour le transfert des données ou l'interaction avec des systèmes distants. Cependant, des bogues ont été identifiés pour certaines versions de l'application. Or, ces bogues constituent des vulnérabilités pour les hackers qui peuvent ainsi prendre le contrôle du système ciblé.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_SSH") flow trigger(1,60)
```

UNIX : vérification d'attaques relatives au protocole SNMP (Simple Network Management Protocol)

Cette règle prend en charge les 10 attaques les plus courantes contre le protocole SNMP sous UNIX selon l'Institut SANS. SNMP était au départ destiné à gérer des nœuds sur un réseau. Aucune mesure de sécurité n'a jamais été implémentée pour la première version de SNMP. La version 3.0 n'en comportant que quelques-unes, SNMP reste très vulnérable face à de nombreuses attaques.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_SNMP") flow trigger(1,60)
```

UNIX : vérification d'attaques relatives au protocole FTP (File Transfer Protocol)

Cette règle prend en charge les 10 attaques les plus courantes contre le protocole FTP sous UNIX selon l'Institut SANS. Le protocole FTP est un élément essentiel de la communication par Internet. C'est pourquoi il est une cible privilégiée pour les hackers qui redirigent les accès vers le Web et depuis celui-ci.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_FTP") flow trigger(1,60)
```

UNIX : vérification d'attaques touchant les services distants

Cette règle prend en charge les 10 attaques les plus courantes contre des services distants sous UNIX selon l'Institut SANS. Sous UNIX, les services distants permettent d'accéder à des applications ou à des fichiers qui se trouvent sur un système distant (ou de les exécuter) sans authentification. Si vous laissez les services distants ouverts, n'importe quel utilisateur peut exécuter sur votre système des commandes qui exigent des droits particuliers, et ce, sans autorisation. Les services distants permettent donc les attaques à distance.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_RemoteServices") flow
   trigger(1,60)
```

UNIX : vérification d'attaques touchant les démons d'impression LPD

Cette règle prend en charge les 10 attaques les plus courantes contre le démon d'impression LPD sous UNIX selon l'Institut SANS. Le démon LPD est le mécanisme utilisé par UNIX pour imprimer des fichiers. Cette application s'exécute dans un environnement UNIX sous le compte racine. De nombreux bogues détectés dans cette application constituent des vulnérabilités permettant à un imposteur de prendre le contrôle total d'un environnement UNIX.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_LPD") flow trigger(1,60)
```

UNIX : vérification d'attaques touchant Sendmail

Cette règle prend en charge les 10 attaques les plus courantes contre Sendmail sous UNIX selon l'Institut SANS. L'application de messagerie Sendmail utilise le protocole SMTP (Simple Mail Transport Protocol). Ce protocole est un élément essentiel de la communication par Internet. Il constitue une cible privilégiée pour les hackers qui redirigent les accès vers le Web et depuis celui-ci.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_SendMail") flow trigger(1,60)
```

UNIX : vérification d'attaques touchant BIND/DNS

Cette règle prend en charge les 10 attaques les plus courantes contre le service DNS (Domain Name Service) sous UNIX selon l'Institut SANS. DNS étant un élément vital de la communication par Internet, il constitue une cible privilégiée pour les hackers qui redirigent les accès vers le Web et depuis celui-ci.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_DNS") flow trigger(1,60)
```

UNIX : vérification d'attaques relatives à l'authentification sous UNIX en général

Cette règle prend en charge les 10 attaques de mots de passe les plus courantes sous UNIX selon l'Institut SANS. Lorsque des mots de passe faibles sont découverts, ils doivent être changés.

Fréquence de la règle	Conditions requises	Taxinomie de la règle
1 fois	Définir les éléments suivants avant d'implémenter cette règle : ▪ Plates-formes NIDS traduisibles par la taxinomie Sentinel (pour plus d'informations, reportez-vous au tableau Taxinomie NIDS)	NIDS

Syntaxe RuleLg pour cette règle

```
filter (e.rv53 = "Sans_Unix_WeakPasswords") flow
   trigger(1,60)
```

Tableaux de taxinomie

Cette section contient deux tableaux. Il s'agit des tableaux suivants :

- Taxinomie NIDS
- Taxinomie HIDS et OS

Ces tableaux présentent les différentes valeurs de e.rv50, e.rv51, etc. pour les exemples RuleLg fournis.

Tableau de taxinomie NIDS

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level4 (Niveau4) (e.rv53)**
Attaque	Discussion en ligne	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	DNS	Access (Accès)	Sans_Unix_DNS (DNS sous Unix selon l'Institut SANS)
		Buffer_Overflow (Dépassement de mémoire tampon)	Sans_Unix_DNS (DNS sous Unix selon l'Institut SANS)
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Courrier électronique	Access (Accès)	Sans_Unix_SendMail (Sendmail sous UNIX selon l'Institut SANS)
		Buffer_Overflow (Dépassement de mémoire tampon)	Sans_Unix_SendMail (Sendmail sous UNIX selon l'Institut SANS) Sans_MS_IE (IE sous Microsoft selon l'Institut SANS)
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Telnet	Access (Accès)	

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level4 (Niveau4) (e.rv53)**
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Fichier	Access (Accès)	Sans_Unix_FTP (FTP sous Unix selon l'Institut SANS) Sans_MS_WeakPasswords (mots de passe faibles sous Microsoft selon l'Institut SANS) Sans_MS_NETBIOS (NETBIOS sous Microsoft selon l'Institut SANS)
		Buffer_Overflow (Dépassement de mémoire tampon)	Sans_Unix_FTP (FTP sous Unix selon l'Institut SANS)
		Backdoor (Porte dérobée)	Sans_Unix_FTP (FTP sous Unix selon l'Institut SANS)
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Web	Access (Accès)	Sans_Unix_Apache (Apache sous UNIX selon l'Institut SANS) Sans_MS_NETBIOS (NETBIOS sous Microsoft selon l'Institut SANS) Sans_MS_WeakPasswords (mots de passe faibles sous Microsoft selon l'Institut SANS) Sans_MS_IIS (IIS sous Microsoft selon l'Institut SANS) Sans_MS_Scripting (scripts sous Windows selon l'Institut SANS) Sans_MS_SQLServer (SQL Server sous Microsoft selon l'Institut SANS) Sans_MS_IE (IE sous Microsoft selon l'Institut SANS) SANS_MS_MDAC (MDAC sous Microsoft selon l'Institut SANS)
		Buffer_Overflow	Sans_Unix_Apache (Apache sous

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level4 (Niveau4) (e.rv53)**
		(Dépassement de mémoire tampon)	UNIX selon l'Institut SANS) Sans_MS_IIS (IIS sous Microsoft selon l'Institut SANS)
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	Sans_MS_IIS (IIS sous Microsoft selon l'Institut SANS)
		DoS (Déni de service)	Sans_Unix_Apache (Apache sous UNIX selon l'Institut SANS) Sans_MS_IIS (IIS sous Microsoft selon l'Institut SANS)
	PC	Virus	Sans_MS_IE (IE sous Microsoft selon l'Institut SANS) Sans_MS_IIS (IIS sous Microsoft selon l'Institut SANS)
		Script	
		Worm (Ver)	Sans_MS_SQLServer (SQL Server sous Microsoft selon l'Institut SANS)
		Trojan (Cheval de Troie)	
	Serveur	Access (Accès)	Scan_MS_IIS (IIS sous Microsoft selon l'Institut SANS) Sans_MS_Registry (Registre sous Microsoft selon l'Institut SANS) Sans_MS_SQLServer (SQL Server sous Microsoft selon l'Institut SANS) Sans_MS_NETBIOS (NETBIOS sous Microsoft selon l'Institut SANS) Sans_Unix_remoteServices (services distants sous UNIX selon l'Institut SANS) Sans_Unix_RPC (RPC sous Unix selon l'Institut SANS) Sans_Unix_SSH (SSH sous Unix selon l'Institut SANS)
		Buffer_Overflow (Dépassement de mémoire tampon)	Sans_Unix_remoteServices (services distants sous UNIX selon l'Institut SANS) Sans_Unix_WeakPasswords (mots de passe faibles sous UNIX selon l'Institut SANS) Sans_Unix_RPC (RPC sous Unix selon l'Institut SANS)

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level4 (Niveau4) (e.rv53)**
			Sans_Unix_LPD (LPD sous Unix selon l'Institut SANS) Sans_MS_SQLServer (SQL Server sous Microsoft selon l'Institut SANS) Sans_MS_MDAC (MDAC sous Microsoft selon l'Institut SANS) Sans_MS_NETBIOS (NETBIOS sous Microsoft selon l'Institut SANS) Sans_Unix_SSH (SSH sous Unix selon l'Institut SANS)
		Backdoor (Porte dérobée)	Sans_Unix_RPC (RPC sous Unix selon l'Institut SANS)
		Brute_Force (Attaque en force)	Sans_MS_SQLServer (SQL Server sous Microsoft selon l'Institut SANS) Sans_MS_WeakPasswords (mots de passe faibles sous Microsoft selon l'Institut SANS)
		DoS (Déni de service)	
	Protocole	IP	
		TCP	
		UDP	
		ICMP	
		HTTP	
		Route	
		Talk	
		XFS	
		SSH	
		IGMP	
		Heure	
		News	
		Windows	
		RIP	
		IDS	
		SNMP	Sans_Unix_SNMP (SNMP sous Unix selon l'Institut SANS)
		BGP	
	User (Utilisateur)	Access (Accès)	Sans_Unix_WeakPasswords (mots de passe faibles sous UNIX selon l'Institut SANS) Sans_Unix_remoteServices (services distants sous UNIX selon

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level4 (Niveau4) (e.rv53)**
			l'Institut SANS)
		Buffer_Overflow (Dépassement de mémoire tampon)	Sans_Unix_remoteServices (services distants sous UNIX selon l'Institut SANS) Sans_MS_NETBIOS (NETBIOS sous Microsoft selon l'Institut SANS)
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
Vérification	Discussion en ligne		
	DNS		
	Courrier électronique		
	Fichier		Sans_Unix_FTP (FTP sous Unix selon l'Institut SANS)
	Web		Sans_MS_IIS (IIS sous Microsoft selon l'Institut SANS) Sans_Unix_Apache (Apache sous UNIX selon l'Institut SANS)
	PC		
	Serveur		Sans_MS_NullSessions (sessions Null sous Microsoft selon l'Institut SANS) Sans_MS_Registry (Registre sous Microsoft selon l'Institut SANS)
	Protocole	IP	
		TCP	
		RIP	
		SNMP	Sans_Unix_SNMP (SNMP sous Unix selon l'Institut SANS)
		SSH	
		Talk	
		Heure	
		Windows	
		UDP	
		ICMP	
		DHCP	
	Analyse		
	Telnet		Sans_MS_LM (LM sous Microsoft selon l'Institut SANS)

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level4 (Niveau4) (e.rv53)**
	User (Utilisateur)		Sans_MS_LM (LM sous Microsoft selon l'Institut SANS)
	IDS		
Stratégie	Pornographie		
Danger	Discussion en ligne	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	Sans_Unix_Weak_Passwords (mots de passe faibles sous UNIX selon l'Institut SANS)
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	DNS	Access (Accès)	Sans_Unix_DNS (DNS sous Unix selon l'Institut SANS)
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Courrier électronique	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	Sans_Unix_SendMail (Sendmail sous UNIX selon l'Institut SANS)
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Telnet	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level4 (Niveau4) (e.rv53)**
		DoS (Déni de service)	
	Fichier	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Web	Access (Accès)	Sans_Unix_Apache (Apache sous UNIX selon l'Institut SANS)
		Buffer_Overflow (Dépassement de mémoire tampon)	Sans_MS_IIS (IIS sous Microsoft selon l'Institut SANS)
		Backdoor (Porte dérobée)	Sans_Unix_Apache (Apache sous UNIX selon l'Institut SANS) Sans_MS_Registry (Registre sous Microsoft selon l'Institut SANS)
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	PC	Virus	
		Script	
		Worm (Ver)	
		Trojan (Cheval de Troie)	
	Serveur	Access (Accès)	Sans_MS_SQLServer (SQL Server sous Microsoft selon l'Institut SANS)
		Buffer_Overflow (Dépassement de mémoire tampon)	Sans_Unix_RPC (RPC sous Unix selon l'Institut SANS)
		Backdoor (Porte dérobée)	Sans_MS_WeakPasswords (mots de passe faibles sous Microsoft selon l'Institut SANS) Sans_MS_Registry (Registre sous Microsoft selon l'Institut SANS) Sans_Unix_SNMP (SNMP sous Unix selon l'Institut SANS) Sans_Unix_WeakPasswords (mots de passe faibles sous UNIX selon l'Institut SANS)

Action – Level1 (Niveau1) (e.rv50)	Système – Level2 (Niveau2) (e.rv51)	Détails – Level3 (Niveau3) (e.rv52)	Résultats – Level4 (Niveau4) (e.rv53)
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	User (Utilisateur)	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	

Tableau de taxinomie HIDS et OS

Action – Level1 (Niveau1) (e.rv50)	Système – Level2 (Niveau2) (e.rv51)	Détails – Level3 (Niveau3) (e.rv52)	Résultats – Level 4 (Niveau4) (e.rv53)
Attaque	Fichier	Delete (Suppression)	App OS
		Execute (Exécution)	App OS
		Create (Création)	App OS
		Modify (Modification)	App OS
		Access (Accès)	App OS
	Service	Delete (Suppression)	App OS
		Stop (Arrêter)	App OS
		Start (Démarrage)	App OS
		Create (Création)	App OS
		Access (Accès)	App OS Priv (privé) Courrier électronique ID Réseau Fichier Système

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level 4 (Niveau4) (e.rv53)**
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		DoS (Déni de service)	
	Config	Delete (Suppression)	App OS
		Modify (Modification)	App OS
		Create (Création)	App OS
		Enable (Activation)	App OS
		Access (Accès)	App OS
	User (Utilisateur)	Create (Création)	ID Auth (authentification) Param (paramètre) Priv (privé)
		Modify (Modification)	ID Auth (authentification) Param (paramètre) Priv (privé)
		Delete (Suppression)	ID Auth (authentification) Param (paramètre) Priv (privé)
		Access (Accès)	Guest (invité) Priv (privé) Root (racine) Autre
	Groupe	Create (Création)	Member (membre) Groupe
		Modify (Modification)	Member (membre) Groupe
		Delete (Suppression)	Member (membre) Groupe
	Système	Informations	
		Memory (Mémoire)	
		Debug (Débogage)	
	Anomalie		
	Telnet	Access (Accès)	

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level 4 (Niveau4) (e.rv53)**
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Web	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	PC	Virus	
		Script	
		Backdoor (Porte dérobée)	
		Worm (Ver)	
		Trojan (Cheval de Troie)	
	DNS	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Courrier électronique	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
Vérification	Fichier	Delete (Suppression)	App

Action – Level1 (Niveau1) (e.rv50)	**Système – Level2 (Niveau2) (e.rv51)**	**Détails – Level3 (Niveau3) (e.rv52)**	**Résultats – Level 4 (Niveau4) (e.rv53)**
			OS
		Execute (Exécution)	App OS
		Create (Création)	App OS
		Modify (Modification)	App OS
		Access (Accès)	App OS
	Service	Delete (Suppression)	App OS
		Stop (Arrêter)	App OS
		Start (Démarrage)	App OS
		Create (Création)	App OS
		Access (Accès)	App OS Fichier ID Courrier électronique Priv (privé) Réseau Système
	Config	Delete (Suppression)	App OS
		Modify (Modification)	App OS
		Create (Création)	App OS
		Enable (Activation)	App OS
		Access (Accès)	App OS
	User (Utilisateur)	Create (Création)	ID Auth (authentification) Param (paramètre) Priv (privé)
		Modify (Modification)	ID Auth (authentification) Param (paramètre) Priv (privé)
		Delete (Suppression)	ID Auth (authentification)

Action – Level1 (Niveau1) (e.rv50)	Système – Level2 (Niveau2) (e.rv51)	Détails – Level3 (Niveau3) (e.rv52)	Résultats – Level 4 (Niveau4) (e.rv53)
			Param (paramètre) Priv (privé)
		Access (Accès)	Guest (invité) Root (racine) Autre
	Groupe	Create (Création)	Member (membre) Groupe
		Modify (Modification)	Member (membre) Groupe
		Delete (Suppression)	Member (membre) Groupe
	Système	Informations	
		Memory (Mémoire)	
		Debug (Débogage)	
	Anomalie		
	Web	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Courrier électronique	Access (Accès)	
		Buffer_Overflow (Dépassement de mémoire tampon)	
		Backdoor (Porte dérobée)	
		Brute_Force (Attaque en force)	
		DoS (Déni de service)	
	Protocole	IP	
		TCP	
		UDP	
		ICMP	
		HTTP	
		Route	
		Talk	
		XFS	
		SSH	
		IGMP	
		Heure	
		News	
		Windows	
		RIP	

Action – Level1 (Niveau1) (e.rv50)	Système – Level2 (Niveau2) (e.rv51)	Détails – Level3 (Niveau3) (e.rv52)	Résultats – Level 4 (Niveau4) (e.rv53)
		IDS	
		SNMP	
		BGP	

Sortie de corrélation

La structure de sortie du moteur de corrélation permet de trier, filtrer et créer des rapports sur des données générées suite à l'application d'une règle de liste de surveillance ou de corrélation.

Structure de la sortie d'une règle de corrélation

Les valeurs de sortie par défaut sont les suivantes :

- RES est défini sur « corrélation » s'il n'est pas défini par l'utilisateur.
- SubRes est défini sur « <règle>.<nomrègle> » s'il n'est pas défini par l'utilisateur.
- Sev est défini sur 4 s'il n'est pas défini par l'utilisateur.
- ST (type de capteur : C).
- EI (modèle de la règle : SIP='1.2.3.4.', puis un point-virgule et enfin, le seuil de la règle au format de type 3-2-m, à savoir 3 fois en 2 minutes, par exemple).
- RT2 (nom de la règle).

Paramètres de script transmis

Les paramètres de script transmis influent sur la règle de liste de surveillance ainsi que sur la règle de corrélation. Les paramètres de script doivent être spécifiés dans la zone de texte Effectuer l'opération de l'onglet Critères d'activation en respectant le format %xyz% où « xyz » correspond au nom du paramètre. Les noms des paramètres qui représentent des balises META peuvent être abrégés (exemple : sip) ou indiqués en toutes lettres (exemple : SourceIP). Une distinction entre les majuscules et les minuscules est faite pour les noms de paramètres.

Paramètres

Les onze premiers paramètres sont des paramètres spécifiques. Il ne s'agit pas de balises META. Ils correspondent à des événements corrélés. Les paramètres 12 à 47 sont des paramètres représentant des balises META.

1. `%RuleName%` : nom de la règle qui s'est déclenchée (format : « règle.nomrègle »).
2. `%RuleType% :` type de la règle qui s'est déclenchée. C pour corrélation. W pour liste de surveillance.
3. `%RuleDescription%` : description qui a été entrée au moment de la création de la règle.
4. `%RuleSeverity%` : niveau de gravité de la règle qui s'est déclenchée.
5. `%RuleResource%` : nom de la ressource de la règle qui s'est déclenchée.
6. `%RuleSubResource%` : nom de la sous-ressource de la règle qui s'est déclenchée.
7. `%RuleLg%` : règle énoncée dans le langage de règle propre au moteur de corrélation (RuleLg).
8. `%RuleCount%` : décompte de la règle qui s'est déclenchée.
9. `%RuleDuration%` : durée (en secondes) de la règle qui s'est déclenchée.

10. `%RulePattern%` : liste de toutes les balises en langage de règle, et de toutes les valeurs de ces balises, élaborée à partir du dernier événement qui a déclenché la règle. Le format des éléments est tsn1=‘value1=’value2’tsn3=’value3’, où :
    - tns1 correspond au nom abrégé de la balise n°1 et
    - tns2 correspond au nom abrégé de la balise n°2.

    Par exemple :

    ```
    sip=‘192.168.0.3’dip=‘2.168.0.2’
    ```

11. `%CorrelatedEventID%` : identificateur de l'événement corrélé généré par la règle qui s'est déclenchée.
12. %MessageText% : texte du message de la règle qui s'est déclenchée.
13. %EventName% : nom de l'événement de la règle qui s'est déclenchée.

Les balises suivantes correspondent au champ du dernier événement ayant déclenché l'événement corrélé.

14. %sev% : gravité. Sévérité normalisée de l'événement (de 0 à 5).
15. %vul% : vulnérabilité. Vulnérabilité de l'actif identifié dans cet évènement.
16. %crt% : sévérité. Importance de l'actif identifié dans cet évènement.
17. %dt% : DateTime. Date et heure normalisées de l'évènement, fournies par le collecteur.
18. %sip% : SourceIP. Adresse IP source à partir de laquelle l'évènement s'est produit
19. %dip% : DestinationIP. Adresse IP de destination vers lequel l'évènement a été ciblé.
20. %id% : EventID. UUID (Universal Unique Identifier) de l'événement concerné.
21. %src% : SourceID. UUID du processus Sentinel qui a généré cet évènement.
22. %port% : WizardPort. Description du port du collecteur Sentinel.
23. %agent% : WizardCollector. Description du port du collecteur Sentinel.
24. %res% : Resource. Nom de la ressource.
25. %sres% : SubResource. Nom de la sous-ressource.
26. %evt% : EventName. Nom descriptif de l'évènement indiqué (ou fourni) par le capteur. Exemple : « Analyse des ports ».
27. %sn% : SensorName. Nom du « détecteur ultime » de l'évènement lors de sa réception dans les données brutes. Exemple : « FW1 » pour un pare-feu.
28. %st% : SensorType. Indicateur composé d'un seul caractère désignant le type de capteur (N, H, O, V, C, W). H : basé sur l'hôte ; N : basé sur le réseau ; O : autre ; V : antivirus ; C : corrélation ; W : liste de surveillance.
29. %et% : EventTime. Heure normalisée de l'évènement indiquée par le capteur et analysée dans le format suivant : A-M-J-H:M:S~AMPM24~TZ.
30. %prot% : Protocol. Protocole réseau de l'évènement.
31. %shn% : SourceHostName. Nom d'hôte source à partir duquel l'évènement s'est produit.
32. %sp% : SourcePort. Port source à partir duquel l'évènement s'est produit.
33. %dhn% : DestinationHostName. Nom de l'hôte de destination vers lequel l'évènement a été ciblé.
34. %dp% : DestinationPort. Port de destination vers lequel l'évènement a été ciblé.

35. %sun% : SourceUserName. Nom d'utilisateur source utilisé pour initier un évènement. Exemple : « jdupond » durant une tentative de « su ».
36. %dun% : DestinationUserName. Nom d'utilisateur de destination sur lequel une action a été tentée. Exemple : tentatives de réinitialiser le mot de passe de l'utilisateur racine.
37. %fn% : FileName. Nom du programme exécuté ou du fichier accédé, modifié ou affecté. Exemple : nom d'un fichier infecté par un virus ou d'un programme détecté par un IDS.
38. %ei% : ExtendedInformation. Stocke des informations supplémentaires collectées par le collecteur. Les valeurs incluses dans cette variable sont séparées par des points-virgules (;). Exemple : un domaine pour un ID ou des noms de fichier.
39. %rn% : ReporterName. Nom d'hôte ou adresse IP du périphérique vers lequel ou laquelle un événement a été consigné où à partir duquel ou de laquelle l'événement est envoyé.
40. %pn% : ProductName. Indique le type, le nom de code produit et de fournisseur du capteur à partir duquel l'événement a été généré. Exemple : Check Point FireWall=CPFW.
41. %msg% : Message. Texte de message de format libre pour l'événement.
42. %rt1% : réservé par Novell pour l'expansion. À utiliser avec Advisor (chaîne).
43. %rt2% : réservé par Novell pour l'expansion (chaîne).
44. %ct1% : réservé à l'utilisation par des clients pour des données spécifiques du client (chaîne).
45. %ct2% : réservé à l'utilisation par des clients pour des données spécifiques du client (chaîne).
46. %rt3% : réservé par Novell pour l'expansion (nombre).
47. %ct3% : réservé à l'utilisation par des clients pour des données spécifiques du client (nombre).
48. Paramètres 46 à 145 : %rv1% à %rv100%.

    Il s'agit de balises META d'événements en cours représentant des variables réservées.
49. Paramètres 146 à 245 : %cv1% à %cv100%.

    Il s'agit de balises META d'événements en cours représentant des variables client.

REMARQUE : pour plus d'informations sur les commandes et les paramètres, reportez-vous au « Chapitre 5 : Balises META de Wizard et de Sentinel » du guide des références utilisateur ainsi qu'à la section portant sur les règles de corrélation au « Chapitre 9 : Onglet Admin » du guide de l'utilisateur.

Lors de l'utilisation de la commande %all% :

- Si un paramètre n'est pas défini ou qu'il est défini par une valeur nulle, la valeur affichée sera E_NULL ou <absence de balise>. De cette façon, 45 paramètres seront systématiquement présents, même si certains des champs ne sont pas renseignés.
- Lorsque vous configurez le moteur de corrélation de manière que le script de l'interface HP OVO démarre, vous devez spécifier le nom du script ainsi que la balise de paramètre %all% :

  ```
  esec_ovo %all%
  ```

- Lorsque vous configurez le moteur de corrélation de manière que le script de l'interface BMC démarre, vous devez spécifier le nom du script ainsi que la balise de paramètre %all% :

  ```
  bmc_interface.csh %all%
  ```

- Lorsque vous configurez le moteur de corrélation pour envoyer un courrier électronique, vous devez spécifier le nom du script du message ainsi que le paramètre %all% , l'adresse électronique et le sujet (facultatif) du message :

  ```
  email_interface.csh %all% <nom>@<nom du domaine>
     "sujet"
  ```

- Tous les scripts et les applications exécutés par le moteur de corrélation doivent être placés sous le répertoire $ESEC_HOME/sentinel/exec (UNIX) ou %ESEC_HOME%\sentinel\bin (Windows).
- Par défaut, le moteur de corrélation ne transmet PAS tous les paramètres aux scripts qu'il exécute. Vous devez utiliser les balises %tags% décrites plus haut si vous voulez que tous les paramètres soient transmis aux scripts.
- Lorsque vous définissez des paramètres pour un script, vous pouvez les regrouper en les plaçant entre guillemets doubles. Voici quelques exemples :

  ```
  %sip% %dip% : paramètres traités séparément.

  "%sip% %dip%" : paramètres traités comme un seul
     paramètre.

  "Hello World" %sip% : paramètres traités séparément.

  "The message is %msg%" : paramètres traités comme
     un seul paramètre.

  %msg% : paramètre traité comme un seul paramètre
     (même si le message inséré contient des espaces).

  "%msg%" : également traité comme un seul paramètre
     (même si le message inséré contient des espaces).
  ```

8 Options de ligne de commande du moteur de corrélation Sentinel

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

Les options de ligne de commande doivent être utilisées par des utilisateurs expérimentés. Il est recommandé aux utilisateurs moins expérimentés de ne pas se servir de ces options pour effectuer des modifications. Pour accéder aux options de ligne de commande :

Sous UNIX :

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

Sous Windows :

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

Pour exécuter l'option de ligne de commande du moteur de corrélation Sentinel, entrez la ligne suivante :

```
correlation_engine <correlation command line option>
```

Options de ligne de commande de corrélation	**Description**
-debug	Mode débogage (impression d'informations de débogage détaillées)
-noErrorLogging	Désactivation de la consignation des erreurs pour le journal des événements Windows
-ruleFile <fichier>	Spécification du fichier texte contenant les règles qui doivent être traitées par une instance du moteur de corrélation
-ruleFile <fichier>	Spécification d'un fichier de configuration XML pour stocker en local une copie des règles contenues dans la base de données Fichier par défaut : startup_correlation_rules.xml
-inputChannel <chaîne>	Spécification d'un canal d'entrée de la couche de communication pour le moteur de corrélation Canal par défaut : ewizard_binary_event
-outputChannel <chaîne>	Spécification d'un canal de sortie de la couche de communication pour le moteur de corrélation Canal par défaut : correlation_binary_event

Options de ligne de commande de corrélation	Description
-outputUpdateChannel <chaîne>	Spécification d'un canal de mise à jour de sortie au niveau de la couche de communication pour le moteur de corrélation Canal par défaut : correlation_binary_event_update
-outputExecuteChannel <chaîne>	Spécification d'un canal d'exécution de sortie au niveau de la couche de communication pour le moteur de corrélation Canal par défaut : execute
-outputIncidentChannel <chaîne>	Spécification d'un canal d'incident de sortie au niveau de la couche de communication pour le moteur de corrélation Canal par défaut : app_incident_req
-service <chaîne>	Spécification d'un service de communication (paramètre de configuration) pour le moteur de corrélation Service par défaut : correlation_engine
-mgmtInputChannel <chaîne>	Spécification d'un canal d'entrée de gestion au niveau de la couche de communication pour le moteur de corrélation Canal par défaut : correlation_mgmt_input_channel
-mgmtOutputChannel <chaîne>	Spécification d'un canal de sortie de gestion au niveau de la couche de communication pour le moteur de corrélation Canal par défaut : correlation_mgmt_output_channel
-mgmtService <chaîne>	Spécification d'un service de gestion de la communication (paramètre de configuration) pour le moteur de corrélation Valeur par défaut : correlation_engine_mgmt
-configurationFile <fichier>	Spécification d'un fichier pour remplacer les paramètres de démarrage configurés par défaut pour le moteur de corrélation Valeur par défaut : ± 30 secondes par rapport à l'heure indiquée par le serveur Sentinel Server
-noStartupRules	Paramétrage du moteur de corrélation afin qu'il s'exécute sans extraire de règles stockées dans la base de données. L'option -ruleFile permet également de ne pas passer par cette étape d'extraction.

Options de ligne de commande de corrélation	**Description**
-dbTimeout <timeout en millisecondes>	Définition de la valeur du timeout pour l'extraction de règles stockées dans la base de données Valeur par défaut : 5 000 millisecondes
-dbRetries <nombre>	Définition du nombre de tentatives de communication avec la base de données Valeur par défaut : 6
-name <nom du moteur>	Définition du nom de programme reporteur pour ce moteur de corrélation Valeur par défaut : moteur de corrélation
-affinityOneProcessor	Paramétrage du moteur de corrélation de sorte qu'il s'exécute uniquement sur un processeur
-useEventTime	Ligne de commande test qui ne doit pas être utilisée
-useNullOutput	Ligne de commande test qui ne doit pas être utilisée
-logFile <nom de fichier>	Envoi du statut vers un fichier
-logPeriod <secondes>	Contrôle de la fréquence à laquelle le statut doit être écrit dans le fichier
-version	Affichage de la version et fermeture
-help	Affichage de l'aide de ligne de commande et fermeture

9 Service d'accès aux données (DAS) Sentinel

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

Le processus DAS (Data Access Service) constitue le service de persistance de Sentinel Server et fournit une interface MOM (Message-Oriented Middleware, intergiciel orienté message) ou bus message à la base de données. Il permet un accès régi par les données à la base de données principale. Le service DAS reçoit les requêtes XML 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 au format XML. 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.

Fichiers conteneur DAS

Le processus 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 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
- das_aggregation.xml : utilisé lors de l'opération de regroupement.
- das_itrac.xml : utilisé pour l'exécution et la configuration du service d'activités ainsi que pour la configuration du service de flux de travail
  .
- das_rt.xml : utilisé pour configurer la fonction Active Views dans la console Sentinel Control Console.

ATTENTION : ne modifiez pas manuellement les fichiers XML. Servez-vous de l'utilitaire dbconfig pour toute modification des valeurs dans les fichiers XML.

Chacun des processus ci-dessus dispose d'un fichier journal actif situé sous %ESEC_HOME%\Sentinel\log ou sous $ESEC_HOME/Sentinel/log. Ces fichiers sont les suivants :

- das_query0.*.log : tous les fichiers journaux das_query.
- das_binary0.*.log : tous les fichiers journaux das_binary.
- das_itrac0_*.log : fichiers journaux des activités et des flux de travail.
- das_aggregation0.*.log : fichiers journaux des regroupements.
- das_rt0.*.log : fichiers journaux des vues actives.

Les fichiers XML indiquent les éléments suivants :

ConnectionManager

- Nom d'utilisateur
- Mot de passe
- Nom d'hôte
- Numéro de port
- Nom de la base de données
- Serveur (Oracle ou MSSQL)
- Nombre maximum de connexions
- Taille du lot
- Taille de la charge

DispatchManager — Ce fichier indique au processus DAS les canaux du bus message à écouter. Il indique également la classe Java à utiliser pour convertir les requêtes XML en objets Java et le gestionnaire auquel envoyer l'objet Java pour traiter le message. Par exemple : une requête d'événement est convertie en objet Java à l'aide du script esecurity.cracker.QuickQueryRequestCracker. Ce script casseur de mot de passe envoie ensuite l'objet Java au gestionnaire esecurity.event.request, qui le transmet à l'un des services pour traitement.

Autres composants qui fournissent des services DAS pertinents.

Pour reconfigurer les propriétés de connexion à la base de données sous Windows, servez-vous de l'utilitaire dbconfig.

Reconfiguration des propriétés de connexion à la base de données

Cette procédure doit être effectuée pour chacun des noms de fichier conteneur (containerFilename) suivants :

- das_binary.xml
- das_query.xml
- das_rt.xml
- das_aggregation.xml
- das_itrac.xml

Pour reconfigurer les propriétés de connexion à la base de données sous Windows

REMARQUE : toutes les 10 secondes, le fichier des propriétés de consignation est vérifié pour savoir si une modification a été apportée depuis sa dernière lecture. Si le fichier a été modifié, le processus LogManagerRefreshService le relit.

1 Ouvrez une session en tant qu'utilisateur doté des droits d'administrateur sur la machine où la base de données a été installée.

2 Accédez à :

Sous Windows :

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

Sous UNIX :

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

3 Entrez la ligne de commande suivante :

```
dbconfig -n <containerFilename> [-u username] [-p
   password] [-h hostname] [-t port number] [-d
   database] [-s server(mssql or oracle)] [-help]
   [-version]
```

Fichiers de configuration DAS

Pour configurer la consignation du processus DAS, les fichiers suivants sont utilisés :

- das_query_log.prop
- das_binary_log.prop
- das_rt_log.prop
- das_itrac_log.prop
- das_aggregation_log.prop

Ces fichiers se trouvent aux emplacements suivants :

Sous Windows :

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

Sous UNIX :

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

Ces fichiers contiennent les informations de configuration concernant le gestionnaire de console chargé de publier les messages dans un format de sortie standard ainsi que celles du gestionnaire de fichier qui publie les messages dans un fichier. La configuration de chaque gestionnaire permet de spécifier les options qui leur sont propres. Dans les fichiers suivants, il est possible de définir les messages de consignation à publier ou pas. Les différents niveaux de consignation sont les suivants :

- OFF : toutes les consignations sont désactivées.
- SEVERE (niveau le plus élevé) : un composant ne fonctionne plus correctement ou des données critiques ont été perdues ou corrompues.
- WARNING : une action est susceptible d'entraîner un dysfonctionnement futur de l'un des composants ou des données non critiques ont été perdues ou corrompues.
- INFO : informations d'audit.
- CONFIG
- FINE : débogage.
- FINER : débogage.
- FINEST (niveau le plus bas) : débogage.
- ALL : consignation à tous les niveaux.

Lorsqu'un niveau de consignation est spécifié, tous les messages de consignation de ce niveau et des niveaux supérieurs de la liste ci-dessus sont effectivement consignés. Par exemple, si le niveau de consignation est défini sur INFO, tous les messages INFO, WARNING et SEVERE sont consignés.

Si vous effectuez des modifications dans les fichiers, il vous faut redémarrer le processus DAS afin que ces modifications soient appliquées.

Les consignations sont écrites aux emplacements suivants :

Sous Windows :

```
%ESEC_HOME%\sentinel\log\das_query_0.*.log
%ESEC_HOME%\sentinel\log\das_binary_0.*.log
%ESEC_HOME%\sentinel\log\das_itrac_0.*.log
%ESEC_HOME%\sentinel\log\das_aggregation0.*.log
```

Sous UNIX :

```
$ESEC_HOME/sentinel/log/das_query0.*.log
$ESEC_HOME/sentinel/log/das_binary0.*.log
$ESEC_HOME/sentinel/log/das_itrac_0.*.log
$ESEC_HOME/sentinel/log/das_aggregation0.*.log
```

L'astérisque (*) indique un numéro unique permettant de résoudre d'éventuels conflits entre les fichiers journaux ainsi qu'un numéro de création permettant de marquer une différence avec les fichiers journaux ayant subi une permutation circulaire. Par exemple, das_query0.0.log est le fichier journal d'index 0 (le premier fichier) dans un ensemble de fichiers journaux permutés relatifs au processus DAS.

Connecteurs de base de données natifs pour l'insertion d'événements

Les connecteurs de base de données natifs permettent une insertion très performante des événements. Le connecteur à utiliser dépend de la plate-forme utilisée pour la base de données.

Connecteur de base de données natif MS SQL

Servez-vous du récepteur d'événements natif ADO.Net.

Pour configurer le connecteur natif MS SQL

1. Sur la machine où le service DAS est installé, installez .Net Framework.
2 Dans le fichier das_binary.xml, remplacez la propriété « insert.strategy » définie pour EventStoreService > Persistor par :

```
esecurity.ccs.comp.event.jdbc.ADOLoadStrategy
```

Connecteur de base de données natif Oracle

Servez-vous du récepteur d'événements natif OCI. Le client Oracle doit au moins être installé sur la machine où le service DAS est exécuté.

Pour configurer le connecteur natif Oracle

2. Créez un fichier « .profile » dans le répertoire privé de l'utilisateur esecadm. Dans ce fichier, insérez le texte suivant (modifiez ORACLE_HOME pour votre installation) :

```
ORACLE_HOME=/build/home/oracle/OraHome
export ORACLE_HOME
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

3. Dans le fichier das_binary.xml, remplacez la propriété « insert.strategy » définie pour EventStoreService > Persistor par :

esecurity.ccs.comp.event.jdbc.OCILoadStrategy

10 Modification des mots de passe utilisateur par défaut

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

Ce chapitre présente la procédure de modification des mots de passe pour les utilisateurs par défaut de Sentinel :

Authentification Oracle et MS SQL :	**Authentification Windows :**
esecadm	Administrateur Sentinel
esecapp	Utilisateur de base de données d'application Sentinel
esecdba	Administrateur de base de données Sentinel
esecrpt	Utilisateur de rapports Sentinel

Modification des mots de passe utilisateur par défaut pour l'authentification Oracle et MS SQL

REMARQUE : pour modifier les mots de passe, vous devez disposer des droits d'administration.

Modification du mot de passe esecadm

Pour modifier le mot de passe esecadm

1. Ouvrez une session sur la console Sentinel, cliquez sur l'onglet *Admin*.
2. Ouvrez la fenêtre *Gestionnaire d'utilisateurs*.
3. Double-cliquez sur le compte d'utilisateur esecadm ou cliquez avec le bouton droit > *Détails de l'utilisateur*.
4. Modifiez le mot de passe du compte.
5. Cliquez sur *OK*.

Modification du mot de passe esecapp

Pour modifier le mot de passe esecapp

1. Pour l'authentification MS SQL, utilisez MS SQL Enterprise Manager pour changer le mot de passe du compte esecapp.
2. Pour l'authentification Oracle, utilisez Oracle Enterprise Manager pour changer le mot de passe du compte esecapp.
3. À l'aide de l'utilitaire dbconfig, mettez à jour tous les fichiers xml conteneur. Cette opération est obligatoire, car ce sont ces fichiers xml qui stockent le mot de passe

esecapp (chiffré) afin de permettre au service DAS (Data Access Service) et à Advisor de se connecter à la base de données.

das_binary.xml	workflow_container.xml
das_query.xml	das_rt.xml
activity_container.xml	

Vous pouvez trouver ces fichiers xml aux emplacements suivants :

Pour Windows :

%ESEC_HOME%\sentinel\config

Pour Oracle :

$ESEC_HOME/sentinel/config

Pour plus d'informations sur l'utilisation de l'utilitaire dbconfig, consultez le chapitre 9 relatif au service d'accès aux données Sentinel du présent guide.

```
dbconfig –a <Répertoire du conteneur> -p <mot
   de passe>
```

Modification du mot de passe esecdba

Pour modifier le mot de passe esecdba

1. Pour l'authentification MS SQL, utilisez MS SQL Enterprise Manager pour changer le mot de passe du compte esecdba.
2. Pour l'authentification Oracle, utilisez Oracle Enterprise Manager pour changer le mot de passe du compte esecdba.
3. Afin que les tâches automatisées du Gestionnaire de données Sentinel puissent continuer de s'exécuter (par exemple l'ajout ou l'archivage de partitions), mettez à jour le mot de passe de la base de données dans le fichier sdm.connect, en utilisant le nouveau mot de passe esecdba, par le biais de l'interface utilisateur graphique du Gestionnaire ou de la ligne de commande. Pour plus d'informations, consultez le chapitre 10 relatif au Gestionnaire de données Sentinel du Guide de l'utilisateur de Sentinel.

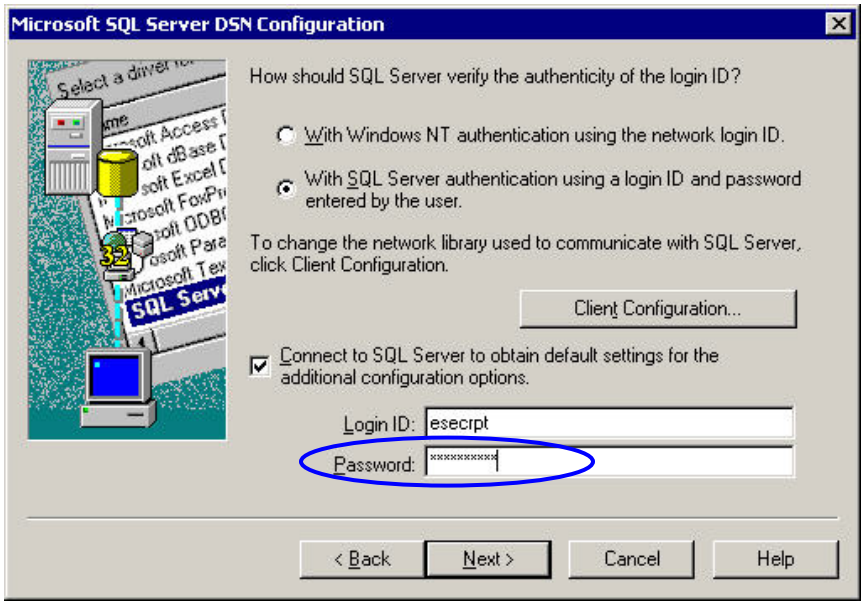
   ```
   sdm -action saveConnection -server <oracle/mssql> -
      host <IP de l'hôte/Nom de l'hôte> -port <numéro
      du port> -database <Nom de la base de données/SID>
      [-driverProps <Fichier de propriétés>] {-user
      <Utilisateur de la base de données> -password <Mot
      de passe de la base de données>} -connectFile <nom
      du fichier d'enregistrement de la connexion>
   ```

Modification du mot de passe esecrpt

Pour modifier le mot de passe esecrpt

1. Pour la base de données Sentinel MS SQL, utilisez MS SQL Enterprise Manager pour changer le mot de passe du compte esecrpt.
2. Pour la base de données Sentinel Oracle, utilisez Oracle Enterprise Manager pour changer le mot de passe du compte esecrpt.

3. Pour Crystal Server pour Sentinel MS SQL, le cas échéant, sur l'ordinateur Crystal Server, mettez à jour le DSN ODBC (*Panneau de configuration* > *Outils d'administration* > *Sources de données* (ODBC)).
   a. Dans l'onglet System DSN, sélectionnez sentineldb et cliquez sur *Configurer*.
   b. Cliquez sur *Suivant*. Mettez à jour le mot de passe.
   c. Cliquez sur *Suivant* jusqu'à l'affichage du bouton Terminer. Cliquez sur *Terminer*.



4. Crystal Server pour Sentinel Oracle, pas de modifications requises.

Modification des mots de passe utilisateur par défaut pour l'authentification Windows

Modification du mot de passe de l'administrateur Sentinel

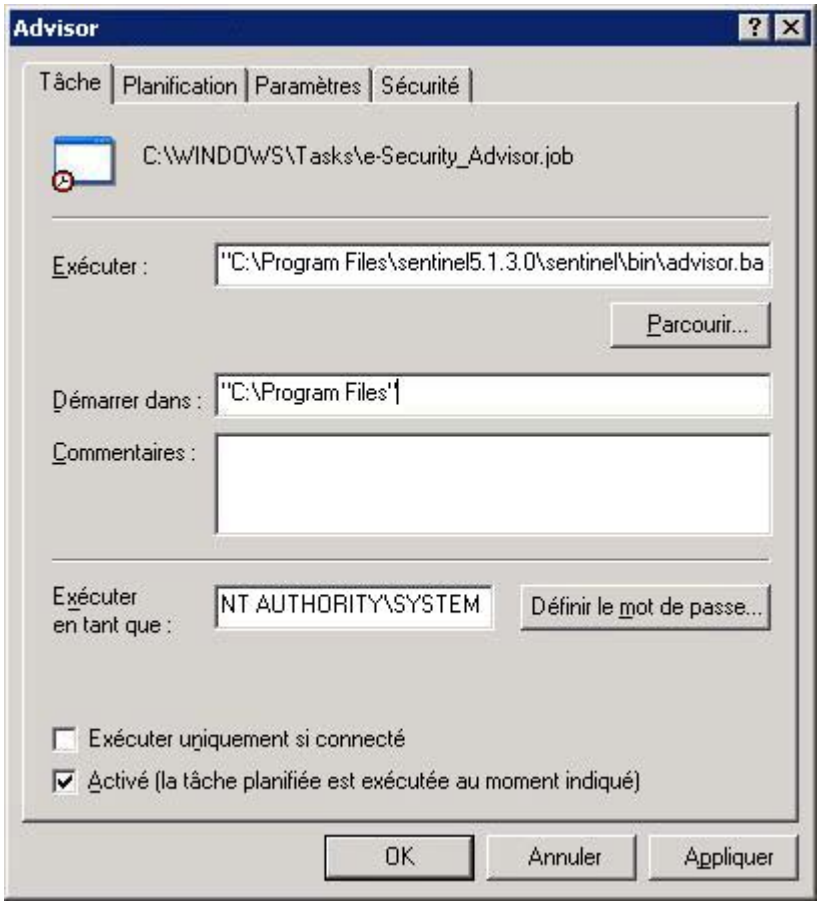
Pour modifier le mot de passe de l'administrateur Sentinel

1. Modifiez le mot de passe dans le système d'exploitation Windows.

Modification du mot de passe de l'administrateur de base de données Sentinel

Pour modifier le mot de passe de l'administrateur de base de données Sentinel

1. Modifiez le mot de passe dans le système d'exploitation Windows.
2. Si des tâches planifiées du Gestionnaire de données Sentinel sont en cours d'exécution (par exemple l'ajout ou l'archivage de partitions), vous devez mettre à jour la propriété « Exécuter en tant que » (*Panneau de configuration* > *Tâches planifiées* > cliquez avec le bouton droit sur *Propriétés*).

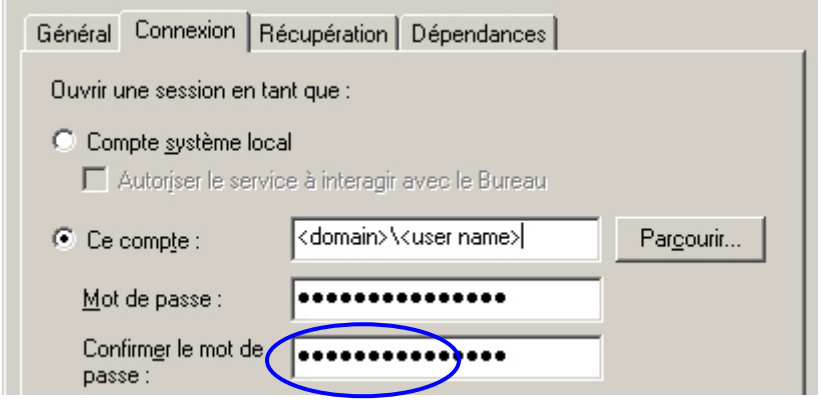


3. Cliquez sur *Définir le mot de passe*. Entrez le nouveau mot de passe à deux reprises et cliquez sur *OK*. Cliquez sur *Appliquer*, puis sur *OK*.

Modification du mot de passe de l'administrateur de base de données d'application Sentinel

Pour modifier le mot de passe de l'administrateur de base de données d'application Sentinel

1. Modifiez le mot de passe dans le système d'exploitation Windows.
2. Sur votre machine DAS, ouvrez les services Windows (*Panneau de configuration* > *Outils d'administration* > *Services*).
3. Cliquez avec le bouton droit sur *Sentinel* > *Propriétés*. Cliquez sur l'onglet *Connexion* et mettez à jour le mot de passe *Ouvrir une session en tant que*. Cliquez sur *Appliquer*, puis sur *OK*.



4. Si Advisor est installé, vous devez mettre à jour la propriété « Exécuter en tant que » des tâches planifiées d'Advisor (*Panneau de configuration* > *Tâches planifiées* > cliquez avec le bouton droit sur *Propriétés*).
5. Cliquez sur *Définir le mot de passe*. Entrez le nouveau mot de passe à deux reprises et cliquez sur *OK*. Cliquez sur *Appliquer*, puis sur *OK*.

Modification du mot de passe de l'utilisateur de rapports Sentinel

Pour modifier le mot de passe de l'utilisateur des rapports Sentinel

Modifiez le mot de passe dans le système d'exploitation Windows.

11 Vues de base de données Sentinel pour Oracle

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

Ce chapitre répertorie les vues des schémas Sentinel pour Oracle. Ces dernières contiennent des informations vous permettant de développer vos propres rapports (rapports Crystal).

Vues

ADV_ALERT_CVE_RPT_V

Cette vue fait référence à la table ADV_ALERT_CVE contenant le numéro d'identification des alertes Advisor.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	number	Identificateur d'annotation - numéro de séquence
CVE	varchar2	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_ALERT_PRODUCT_RPT_V

Cette vue fait référence à la table ADV_ALERT_PRODUCT contenant les informations de produit Advisor, telles que le numéro d'identification du Service Pack, la version et la date de création.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	number	Identificateur d'annotation - numéro de séquence
SERVICE_PACK_ID	number	
VENDOR	varchar2	
PRODUCT	varchar2	
VERSION	varchar2	Contient le numéro de version
SERVICE_PACK	varchar2	
PRIMARY_FLAG	number	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_ALERT_RPT_V

Cette vue fait référence à la table ADV_ALERT contenant les informations sur les alertes Advisor, telles que le nom, le type de menace et la date de publication.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	number	Identificateur d'annotation - numéro de séquence
VERSION	number	Contient le numéro de version
TEMPLATE_ID	number	
TEMPLATE_NAME	varchar2	
THREAT_CATEGORY_NAME	varchar2	
THREAT_TYPE_NAME	varchar2	
HEADLINE	clob	
FIRST_PUBLISHED	date	
LAST_PUBLISHED	date	
STATUS	varchar2	
URGENCY_ID	number	
CREDIBILITY_ID	number	
SEVERITY_ID	number	
SUMMARY	clob	
LEGAL_DISCLAIMER	clob	
COPYRIGHT	varchar2	
BEGIN_EFFECTIVE_DATE	date	
END_EFFECTIVE_DATE	date	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_ATTACK_ALERT_RPT_V

Cette vue fait référence à la table ADV_ATTACK_ALERT contenant les informations sur les attaques Advisor, telles que le nom, le type de menace et la date de publication.

Nom de la colonne	Type de données	Commentaire
ATTACK_ID	number	
ALERT_ID	number	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_ATTACK_CVE_RPT_V

Cette vue fait référence à la table ADV_ATTACK_CVE contenant les informations CVE Advisor.

Nom de la colonne	Type de données	Commentaire
ATTACK_ID	number	
CVE	varchar2	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_ATTACK_MAP_RPT_V

Cette vue fait référence à la table ADV_ATTACK_MAP contenant les informations d'assignation Advisor.

Nom de la colonne	Type de données	Commentaire
ATTACK_KEY	number	
ATTACK_ID	number	
SERVICE_PACK_ID	number	
ATTACK_NAME	varchar2	
ATTACK_CODE	varchar2	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_by	number	ID utilisateur

ADV_ATTACK_PLUGIN_RPT_V

Cette vue fait référence à la table ADV_ATTACK_PLUGIN contenant les informations de plug-in Advisor.

Nom de la colonne	Type de données	Commentaire
PLUGIN_KEY	number	
ATTACK_ID	number	
SERVICE_PACK_ID	number	
PLUGIN_ID	varchar2	
PLUGIN_NAME	varchar2	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_ATTACK_RPT_V

Cette vue fait référence à la table ADV_ATTACK contenant les informations sur les attaques Advisor.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	number	
TRUSECURE_ATTACK_NAME	number	
FEED_DATE_CREATED	date	
FEED_DATE_UPDATED	date	
ATTACK_CATEGORY	varchar2	
URGENCY_ID	number	
SEVERITY_ID	number	
LOCAL	number	
REMOTE	number	
BEGIN_EFFECTIVE_DATE	date	
END_EFFECTIVE_DATE	date	
DESCRIPTION	clob	
SCENARIO	clob	
IMPACT	clob	
SAFEGUARDS	clob	
PATCHES	clob	
FALSE_POSITIVES	clob	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_CREDIBILITY_RPT_V

Cette vue fait référence à la table ADV_CREDIBILITY contenant les informations de crédibilité Advisor.

Nom de la colonne	Type de données	Commentaire
CREDIBILITY_ID	number	
CREDIBILITY_RATING	varchar2	
CREDIBILITY_EXPLANATION	varchar2	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_FEED_RPT_V

Cette vue fait référence à la table ADV_FEED contenant les informations de flux de données Advisor, telles que le nom des flux de données et la date.

Nom de la colonne	Type de données	Commentaire
FEED_NAME	varchar2	
FEED_FILE	varchar2	
BEGIN_DATE	date	
END_DATE	date	
FEED_INSERT	number	
FEED_UPDATE	number	
FEED_EXPIRE	number	

ADV_PRODUCT_RPT_V

Cette vue fait référence à la table ADV_PRODUCT contenant les informations de produit Advisor, telles que le nom du fournisseur et l'ID de produit.

Nom de la colonne	Type de données	Commentaire
PRODUCT_ID	number	
VENDOR_ID	number	
PRODUCT_CATEGORY_ID	number	
PRODUCT_CATEGORY_NAME	varchar2	
PRODUCT_TYPE-ID	number	
PRODUCT_TYPE_NAME	varchar2	
PRODUCT_NAME	varchar2	
PRODUCT_DESCRIPTION	varchar2	
FEED_DATE_CREATED	date	
FEED_DATE_UPDATED	date	
ACTIVE_FLAG	number	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_PRODUCT_SERVICE_PACK_RPT_V

Cette vue fait référence à la table ADV_PRODUCT_SERVICE _PACK contenant les informations sur le Service Pack Advisor, telles que le nom du Service Pack, l'ID de version et la date.

Nom de la colonne	Type de données	Commentaire
SERVICE_PACK_ID	number	
VERSION_ID	number	Contient le numéro de version
SERVICE_PACK_NAME	varchar2	
FEED_DATE_CREATED	date	
FEED_DATE_UPDATED	date	

Nom de la colonne	Type de données	Commentaire
ACTIVE_FLAG	number	
BEGIN_EFFECTIVE_DATE	date	
END_EFFECTIVE_DATE	date	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_PRODUCT_VERSION_RPT_V

Cette vue fait référence à la table ADV_PRODUCT_VERSION contenant les informations de version du produit Advisor, telles que le nom de la version, l'ID de produit et l'ID de version.

Nom de la colonne	Type de données	Commentaire
VERSION_ID	number	Contient le numéro de version
PRODUCT_ID	number	
VERSION_NAME	varchar2	
FEED_DATE_CREATED	date	
FEED_DATE_UPDATED	date	
ACTIVE_FLAG	number	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	number	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_SEVERITY_RPT_V

Cette vue fait référence à la table ADV_SEVERITY contenant les informations relatives au taux de gravité Advisor.

Nom de la colonne	Type de données	Commentaire
SEVERITY_ID	number	
SEVERITY_RATING	varchar2	
SEVERITY_EXPLANATION	varchar2	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_SUBALERT_RPT_V

Cette vue fait référence à la table ADV_SUBALERT.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	number	
SUBALERT_ID	number	

Nom de la colonne	Type de données	Commentaire
CHANGED_SECTIONS	varchar2	
VARIANTS	clob	
VIRUS_NAME	clob	
DESCRIPTION	clob	
IMPACT	clob	
WARNING_INDICATORS	clob	
TECHNICAL_INFO	clob	
TRUSECURE_COMMENTS	clob	
VENDOR_ANNOUNCEMENTS	clob	
SAFEGUARDS	clob	
PATCHES_SOFTWARE	clob	
ALERT_HISTORY	clob	
BACKGROUND_INFO	clob	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_URGENCY_RPT_V

Cette vue fait référence à la table ADV_URGENCY.

Nom de la colonne	Type de données	Commentaire
URGENCY_ID	number	
URGENCY_RATING	varchar2	
URGENCY_EXPLANATION	varchar2	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_VENDOR_RPT_V

Cette vue fait référence à la table ADV_VENDOR contenant les coordonnées associées à Advisor.

Nom de la colonne	Type de données	Commentaire
VENDOR_ID	number	
VENDOR_NAME	varchar2	
CONTACT_PERSON	varchar2	
ADDRESS_LINE_1	varchar2	
ADDRESS_LINE_2	varchar2	
ADDRESS_LINE_3	varchar2	
ADDRESS_LINE_4	varchar2	
CITY	varchar2	
STATE	varchar2	

Nom de la colonne	Type de données	Commentaire
COUNTRY	varchar2	
ZIP_CODE	varchar2	
URL	varchar2	
PHONE	varchar2	
FAX	varchar2	
EMAIL	varchar2	
PAGER	varchar2	
FEED_DATE_CREATED	date	
FEED_DATE_UPDATED	date	
ACTIVE_FLAG	number	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ADV_VULN_PRODUCT_RPT_V

Cette vue fait référence à la table ADV_VULN_PRODUCT contenant les ID de vulnérabilité Advisor et les ID de Service Pack.

Nom de la colonne	Type de données	Commentaire
ATTACK_ID	number	
SERVICE_PACK_ID	number	
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

ANNOTATIONS_RPT_V

Cette vue fait référence à la table ANNOTATIONS contenant la documentation ou les notes pouvant être associées aux objets du système Sentinel, telles que les incidents.

Nom de la colonne	Type de données	Commentaire
ANN_ID	NUMBER	Identificateur d'annotation - numéro de séquence
TEXT	VARCHAR2(4000)	Documentation ou notes
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
ACTION	Varchar2(255)	Action

ASSET_CTGRY_RPT_V

Cette vue fait référence à la table ASSET_CTGRY contenant les informations sur les catégories d'actifs (par exemple, matériel, logiciel, système d'exploitation, base de données, etc.).

Nom de la colonne	Type de données	Commentaire
ASSET_CATAGORY_ID	number	Identificateur de la catégorie d'actifs
ASSET_CATAGORY_NAME	varchar2(100)	Nom de la catégorie d'actifs
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_HOSTNAME_RPT_V

Cette vue fait référence à la table ASSET_HOSTNAME contenant les informations sur les noms d'hôte de remplacement des actifs.

Nom de la colonne	Type de données	Commentaire
ASSET_HOSTNAME_ID	Varchar2(36)	Identificateur du nom d'hôte de remplacement de l'actif
PHYSICAL_ASSET_ID	varchar2(36)	Identificateur de l'actif physique
HOST_NAME	Varchar2(255)	Nom de l'hôte
CUSTOMER_ID	number	Identificateur du client
DATE_CREATED	date	Date de la dernière mise à jour
DATE_MODIFIED	date	ID de l'utilisateur à l'origine de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_IP_RPT_V

Cette vue fait référence à la table ASSET_IP contenant les informations sur les adresses IP de remplacement des actifs.

Nom de la colonne	Type de données	Commentaire
ASSET_IP_ID	Varchar2(36)	Identificateur de l'adresse IP de remplacement de l'actif
PHYSICAL_ASSET_ID	varchar2(36)	Identificateur de l'actif physique
IP_ADDRESS	number	Adresse IP de l'actif
CUSTOMER_ID	number	Identificateur du client
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_LOCATION_RPT_V

Cette vue fait référence à la table ASSET_LOC contenant les informations sur l'emplacement géographique des actifs.

Nom de la colonne	Type de données	Commentaire
LOCATION_ID	number	Identificateur de l'emplacement
CUSTOMER_ID	number	Identificateur du client
BUILDING_NAME	varchar2(255)	Nom du bâtiment
ADDRESS_LINE_1	varchar2(255)	Adresse 1
ADDRESS_LINE_2	varchar2(255)	Adresse 2
CITY	varchar2(100)	Ville
STATE	varchar2(100)	État
COUNTRY	varchar2(100)	Pays
ZIP_CODE	varchar2(50)	Code postal
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_RPT_V

Cette vue fait référence à la table ASSET contenant les informations sur les actifs physiques et non physiques.

Nom de la colonne	Type de données	Commentaire
ASSET_ID	varchar2(36)	Identificateur de l'actif
CUSTOMER_ID	number	Identificateur du client
ASSET_NAME	varchar2(255)	Nom de l'actif
PHYSICAL_ASSET_ID	varchar2(36)	Identificateur de l'actif physique
PRDT_ID	number	Identificateur du produit
ASSET_CATEGORY_ID	number	Identificateur de la catégorie d'actifs
ENVIRONMENT_IDENTITY_CD	varchar2(5)	Code d'identification de l'environnement
PHYSICAL_ASSET_IND	number(1)	Indicateur de l'actif physique
ASSET_VALUE_CODE	varchar2(5)	Code de la valeur de l'actif
CRITICALITY_CODE	varchar2(5)	Code de sévérité de l'actif
SENSITIVITY_CODE	varchar2(5)	Code de sensibilité de l'actif
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_VALUE_RPT_V

Cette vue fait référence à la table ASSET_VAL_LKUP contenant les informations sur la valeur des actifs.

Nom de la colonne	Type de données	Commentaire
ASSET_VALUE_CODE	varchar2(5)	Code de la valeur de l'actif
ASSET_VALUE_NAME	varchar2(50)	Nom de la valeur de l'actif
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_X_ENTITY_X_ROLE_RPT_V

Cette vue fait référence à la table ASSET_X_ENTITY_X_ROLE qui associe une personne ou une organisation à un actif.

Nom de la colonne	Type de données	Commentaire
PERSON_ID	varchar2(36)	Identificateur de la personne
ORGANIZATION_ID	varchar2(36)	Identificateur de l'organisation
ROLE_CODE	varchar2(5)	Code du rôle
ASSET_ID	varchar2(36)	Identificateur de l'actif
ENTITY_TYPE_CODE	varchar2(5)	Code du type d'entité
PERSON_ROLE_SEQUENCE	number	Ordre des personnes appartenant à un rôle donné
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	Utilisateur à l'origine de la dernière mise à jour

ASSOCIATIONS_RPT_V

Cette vue fait référence à la table ASSOCIATIONS qui associe les utilisateurs aux incidents, les incidents aux annotations, etc.

Nom de la colonne	Type de données	Commentaire
TABLE1	VARCHAR2(64)	Nom de la table 1. Par exemple, incidents
ID1	VARCHAR2(36)	ID1. Par exemple, ID de l'incident
TABLE2	VARCHAR2(64)	Nom de la table 2. Par exemple, utilisateurs
ID2	VARCHAR2(36)	ID2. Par exemple, ID de l'utilisateur
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

ATTACHMENTS_RPT_V

Cette vue fait référence à la table ATTACHMENTS contenant les informations sur les pièces jointes.

Nom de la colonne	Type de données	Commentaire
ATTACHMENT_ID	number	Identificateur de la pièce jointe
NAME	varchar2(255)	Nom de la pièce jointe
SOURCE_REFERENCE	varchar2(64)	Référence de la source
TYPE	varchar2(32)	Type de la pièce jointe
SUB_TYPE	varchar2(32)	Sous-type de la pièce jointe
FILE_EXTENSION	varchar2(32)	Extension du fichier
ATTACHMENT_DESCRIPTION	varchar2(255)	Description de la pièce jointe
DATA	clob	Données de la pièce jointe
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur qui a procédé à l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

CONFIGS_RPT_V

Cette vue fait référence à la table CONFIGS contenant les informations générales de configuration de l'application.

Nom de la colonne	Type de données	Commentaire
USR_ID	VARCHAR2(32)	Nom de l'utilisateur
APPLICATION	VARCHAR2(255)	Identificateur de l'application
UNIT	VARCHAR2(64)	Unité de l'application
VALUE	VARCHAR2(255)	Valeur de texte le cas échéant
DATA	CLOB	Données XML
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

CONTACTS_RPT_V

Cette vue fait référence à la table CONTACTS contenant les informations sur les contacts.

Nom de la colonne	Type de données	Commentaire
CNT_ID	NUMBER	ID du contact - numéro de séquence
FIRST_NAME	VARCHAR2(20)	Prénom du contact
LAST_NAME	VARCHAR2(30)	Nom du contact
TITLE	VARCHAR2(128)	Titre du contact
DEPARTMENT	VARCHAR2(128)	Service
PHONE	VARCHAR2(64)	Téléphone du contact

Nom de la colonne	Type de données	Commentaire
EMAIL	VARCHAR2(255)	Adresse électronique du contact
PAGER	VARCHAR2(64)	Pager du contact
CELL	VARCHAR2(64)	Téléphone portable du contact
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

CORRELATED_EVENTS_RPT_V

Cette vue fait référence aux tables CORRELATED_EVENTS_* contenant les informations sur les événements corrélés.

Nom de la colonne	Type de données	Commentaire
PARENT_EVT_ID	varchar2	UUID (Universal Unique Identifier) de l'événement parent
CHILD_EVT_ID	varchar2	UUID (Universal Unique Identifier) de l'événement enfant
PARENT_EVT_TIME	DATE	Heure de l'événement parent
CHILD_EVT_TIME	DATE	Heure de l'événement enfant
DATE_CREATED	DATE	Date d'insertion créée par le service DAS
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

CORRELATED_EVENTS_RPT_V1

Cette vue contient les événements corrélés historiques et actuels (événements corrélés importés des archives).

Nom de la colonne	Type de données	Commentaire
PARENT_EVT_ID	varchar2	UUID (Universal Unique Identifier) de l'événement parent
CHILD_EVT_ID	varchar2	UUID (Universal Unique Identifier) de l'événement enfant
PARENT_EVT_TIME	DATE	Heure de l'événement parent
CHILD_EVT_TIME	DATE	Heure de l'événement enfant
DATE_CREATED	DATE	Date d'insertion créée par le service DAS
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

CRITICALITY_RPT_V

Cette vue fait référence à la table CRIT_LKUP contenant les informations sur le degré de sévérité des actifs.

Nom de la colonne	Type de données	Commentaire
CRITICALITY_CODE	varchar2(5)	Code de sévérité de l'actif
CRITICALITY_NAME	varchar2(50)	Nom relatif à la sévérité de l'actif
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

CUST_RPT_V

Cette vue fait référence à la table CUST contenant les informations sur les clients MSSP.

Nom de la colonne	Type de données	Commentaire
CUSTOMER_ID	number	Identificateur du client
CUSTOMER_NAME	varchar2(255)	Nom du client
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ENTITY_TYPE_RPT_V

Cette vue fait référence à la table ENTITY_TYP qui contient les informations sur les types d'entités (personne, organisation).

Nom de la colonne	Type de données	Commentaire
ENTITY_TYPE_CODE	varchar2(5)	Code du type d'entité
ENTITY_TYPE_NAME	varchar2(50)	Nom du type d'entité
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ENV_IDENTITY_RPT_V

Cette vue fait référence à la table ENV_IDENTITY_LKUP contenant les informations sur l'identité de l'environnement des actifs.

Nom de la colonne	Type de données	Commentaire
ENVIRONMENT_IDENTITY_CODE	varchar2(5)	Code de l'identité de l'environnement

Nom de la colonne	Type de données	Commentaire
ENVIRONMENT_IDENTITY_NAME	varchar2(255)	Nom de l'identité de l'environnement
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ESEC_DISPLAY_RPT_V

Cette vue fait référence à la table ESEC_DISPLAY qui contient les propriétés affichables des objets. Elle est actuellement utilisée pour renommer les balises META et dans le cadre de la configuration des événements (en rapport avec l'entreprise).

Nom de la colonne	Type de données	Commentaire
DISPLAY_OBJECT	VARCHAR2(32)	Objet parent de la propriété
TAG	VARCHAR2(32)	Nom de balise natif de la propriété
LABEL	VARCHAR2(32)	Chaîne d'affichage de la balise
POSITION	NUMBER	Emplacement de la balise affichée
WIDTH	NUMBER	Largeur de la colonne
ALIGNMENT	NUMBER	Alignement horizontal
FORMAT	NUMBER	Mise en forme énumérée de l'affichage de la propriété
ENABLED	VARCHAR2(1)	Indique si la balise est affichée
TYPE	NUMBER	Indique le type de données de la balise 1 = string 2 = ulong 3 = date 4 = uuid 5 = ipv4
DESCRIPTION	VARCHAR2(255)	Texte de description de la balise
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour
REF_CONFIG	VARCHAR2(4000)	Configuration des données de référence

ESEC_PORT_REFERENCE_RPT_V

Cette vue fait référence à la table ESEC_PORT_REFERENCE qui contient les numéros de port standard.

Nom de la colonne	Type de données	Commentaire
PORT_NUMBER	NUMBER	Conformément aux informations du site http://www.iana.org/assignments/port-numbers, représentation numérique du port. Ce numéro est généralement associé au niveau Protocole de transport dans la pile TCP/IP.
PROTOCOL_NUMBER	NUMBER	Conformément aux informations du site http://www.iana.org/assignments/protocol-numbers, identificateurs numériques utilisés pour représenter les protocoles encapsulés dans un paquet IP.
PORT_KEYWORD	VARCHAR2(64)	Conformément aux informations du site http://www.iana.org/assignments/port-numbers, mot clé du port.
PORT_DESCRIPTION	VARCHAR2(512)	Description du port
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière modification

ESEC_PROTOCOL_REFERENCE_RPT_V

Cette vue fait référence à la table ESEC_PROTOCOL_REFERENCE qui contient les numéros de protocole standard.

Nom de la colonne	Type de données	Commentaire
PROTOCOL_NUMBER	NUMBER	Conformément aux informations du site http://www.iana.org/assignments/protocol-numbers, identificateurs numériques utilisés pour représenter les protocoles encapsulés dans un paquet IP.

Nom de la colonne	Type de données	Commentaire
PROTOCOL_KEYWORD	VARCHAR2(64)	Conformément aux informations du site http://www.iana.org/assignments/protocol-numbers, mot clé utilisé pour représenter les protocoles encapsulés dans un paquet IP.
PROTOCOL_DESCRIPTION	VARCHAR2(512)	Description du protocole du paquet IP
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

ESEC_SEQUENCE _RPT_V

Cette vue fait référence à la table ESEC_SEQUENCE utilisée pour générer les numéros de séquence de clés primaires pour les tables Sentinel.

Nom de la colonne	Type de données	Commentaire
TABLE_NAME	VARCHAR2(32)	Nom de la table
COLUMN_NAME	VARCHAR2(32)	Nom de la colonne
SEED	NUMBER	Valeur actuelle de la clé primaire
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

EVENTS_ALL_RPT_V (fournie à des fins de compatibilité descendante)

Cette vue contient les événements historiques et actuels (événements importés des archives).

Nom de la colonne	Type de données	Commentaire
EVENT_ID	varchar2	Identificateur de l'événement
RESOURCE_NAME	varchar2(255)	Nom de la ressource
SUB_RESOURCE	varchar2(255)	Nom de la sous-ressource
SEVERITY	number	Degré de gravité de l'événement
EVENT_PARSE_TIME	date	Heure de l'événement
EVENT_DATE_TIME	date	Heure de l'événement
BASE_MESSAGE	varchar2(4000)	Message de base
EVENT_NAME	varchar2(255)	Nom de l'événement indiqué par le capteur

Nom de la colonne	Type de données	Commentaire
EVENT_TIME	varchar2(255)	Heure de l'événement indiquée par le capteur
SENSOR_NAME	varchar2(255)	Nom du capteur
SENSOR_TYPE	varchar2(5)	Type de capteur : H : basé sur l'hôte N : basé sur le réseau V : virus O : autre
PROTOCOL	varchar2(255)	Nom du protocole
SOURCE-IP	number	Adresse IP source au format numérique
SOURCE_HOST_NAME	varchar2(255)	Nom de l'hôte source
SOURCE_PORT	varchar2(32)	Port source
DESTINATION_IP	number	Adresse IP de destination au format numérique
DESTINATION_HOST_NAME	varchar2(255)	Nom de l'hôte de destination
DESTINATION_PORT	varchar2(32)	Port de destination
SOURCE_USER_NAME	varchar2(255)	Nom d'utilisateur source
DESTINATION_USER_NAME	varchar2(255)	Nom d'utilisateur de destination
FILE_NAME	varchar2(1000)	Nom du fichier
EXTENDED_INFO	varchar2(1000)	Informations développées
REPORT_NAME	varchar2(255)	Nom de programme reporteur
PRODUCT_NAME	varchar2(255)	Nom du produit de rapport
CUSTOM_TAG_1	varchar2(255)	Balise client 1
CUSTOM_TAG_2	varchar2(255)	Balise client 2
CUSTOM_TAG_3	number	Balise client 3
RESERVED_TAG_1	VARCHAR2(255)	Balise réservée 1 Réservé pour utilisation ultérieure par Novell. Ce champ sert à contenir les informations Advisor sur les descriptions des attaques.
RESERVED_TAG_2	varchar2(255)	Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RESERVED_TAG_3	number	Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
SOURCE_UUID	varchar(36)	UUID source
PORT	varchar(64)	Port du collecteur
AGENT	varchar2(64)	Nom du collecteur

Nom de la colonne	Type de données	Commentaire
VULNERABILITY_RATING	number	Taux de vulnérabilité
CRITICALITY_RATING	number	Taux de sévérité
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur
RV01 - 10	NUMBER	Valeur réservée 1 - 10 Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV11 - 20	DATE	Valeur réservée 11 - 20 Réservé à une utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV21 - 25	varchar2	Valeur réservée 21 - 25 Réservé à une utilisation ultérieure par Novell pour le stockage des UUID. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV26 - 31	VARCHAR2(255)	Valeur réservée 26 - 31 Réservé à une utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV32	VARCHAR2(255)	Valeur réservée 32 Réservé pour DeviceCategory. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV33	VARCHAR2(255)	Valeur réservée 33 Réservé pour EventContex. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV34	VARCHAR2(255)	Valeur réservée 34 Réservé pour SourceThreatLevel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV35	VARCHAR2(255)	Valeur réservée 35 Réservé pour SourceUserContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV36	VARCHAR2(255)	Valeur réservée 36 Réservé pour DataContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV37	VARCHAR2(255)	Valeur réservée 37 Réservé pour SourceFunction. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV38	VARCHAR2(255)	Valeur réservée 38 Réservé pour SourceOperationalContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV39	VARCHAR2(255)	Valeur réservée 39 Réservé pour MSSPCustomerName. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV40 - 43	VARCHAR2(255)	Valeur réservée 40 - 43 Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV44	VARCHAR2(255)	Valeur réservée 44 Réservé pour DestinationThreatLevel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV45	VARCHAR2(255)	Valeur réservée 45 Réservé pour DestinationUserContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV46	VARCHAR2(255)	Valeur réservée 46 Réservé pour VirusStatus. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV47	VARCHAR2(255)	Valeur réservée 47 Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV48	VARCHAR2(255)	Valeur réservée 48 Réservé pour DestinationOperationalContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV49	VARCHAR2(255)	Valeur réservée 49 Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV50	VARCHAR2(255)	Niveau de taxinomie 1
RV51	VARCHAR2(255)	Niveau de taxinomie 2
RV52	VARCHAR2(255)	Niveau de taxinomie 3
RV53	VARCHAR2(255)	Niveau de taxinomie 4
CV01 - 10	NUMBER	Valeur personnalisée 1 - 10 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles
CV11 - 20	DATE	Valeur personnalisée 11 - 20 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles

Nom de la colonne	Type de données	Commentaire
CV21 - 100	VARCHAR2(255)	Valeur personnalisée 21 - 100 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles

EVENTS_ALL_RPT_V1 (fournie à des fins de compatibilité descendante)

Cette vue contient les événements actuels. Ses colonnes sont les mêmes que pour la vue EVENT_ALL_RPT_V.

EVENTS_RPT_V (fournie à des fins de compatibilité descendante)

Cette vue contient les événements historiques et actuels. Ses colonnes sont les mêmes que pour la vue EVENT_ALL_RPT_V.

EVENTS_RPT_V1 (fournie à des fins de compatibilité descendante)

Cette vue contient les événements actuels. Ses colonnes sont les mêmes que pour la vue EVENT_ALL_RPT_V.

EVENTS_RPT_V2 (tous les nouveaux rapports Sentinel 5 doivent utiliser cette vue)

Cette vue contient les événements historiques et actuels.

Nom de la colonne	Type de données	Commentaire
EVENT_ID	varchar2	Identificateur de l'événement
RESOURCE_NAME	varchar2(255)	Nom de la ressource
SUB_RESOURCE	varchar2(255)	Nom de la sous-ressource
SEVERITY	number	Degré de gravité de l'événement
EVENT_PARSE_TIME	date	Heure de l'événement
EVENT_DATETIME	date	Heure de l'événement
BASE_MESSAGE	varchar2(4000)	Message de base
EVENT_NAME	varchar2(255)	Nom de l'événement indiqué par le capteur
EVENT_TIME	varchar2(255)	Heure de l'événement indiquée par le capteur
TAXONOMY_ID	number	Identificateur de taxinomie
PROTOCOL_ID	number	Identificateur du protocole
AGENT_ID	number	Identificateur du collecteur
SOURCE_IP	number	Adresse IP source au format numérique
SOURCE_HOST_NAME	varchar2(255)	Nom de l'hôte source
SOURCE_PORT	varchar2(32)	Port source
DESTINATION_IP	number	Adresse IP de destination au format numérique

Nom de la colonne	Type de données	Commentaire
DESTINATION_HOST_NAME	varchar2(255)	Nom de l'hôte de destination
DESTINATION_PORT	varchar2(32)	Port de destination
SOURCE_USER_NAME	varchar2(255)	Nom d'utilisateur source
DESTINATION_USER_NAME	varchar2(255)	Nom d'utilisateur de destination
FILE_NAME	varchar2(1000)	Nom du fichier
EXTENDED_INFO	varchar2(1000)	Informations développées
CUSTOM_TAG_1	varchar2(255)	Balise client 1
CUSTOM_TAG 2	varchar2(255)	Balise client 2
CUSTOM_TAG 3	number	Balise client 3
RESERVED_TAG_1	VARCHAR2(255)	Balise réservée 1 Réservé pour utilisation ultérieure par Novell. Ce champ sert à contenir les informations Advisor sur les descriptions des attaques.
RESERVED_TAG_2	varchar2(255)	Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RESERVED_TAG_3	number	Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
VULNERABILITY_RATING	number	Taux de vulnérabilité
CRITICALITY_RATING	number	Taux de sévérité
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour
RV01 - 10	NUMBER	Valeur réservée 1 - 10 Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV11 - 20	DATE	Valeur réservée 1 - 31 Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV21 - 25	varchar2	Valeur réservée 21 - 25 Réservé à une utilisation ultérieure par Novell pour le stockage des UUID. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV26 - 31	VARCHAR2(255)	Valeur réservée 26 - 31 Réservé à une utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV33	VARCHAR2(255)	Valeur réservée 33 Réservé pour EventContex. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV34	VARCHAR2(255)	Valeur réservée 34 Réservé pour SourceThreatLevel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV35	VARCHAR2(255)	Valeur réservée 35 Réservé pour SourceUserContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV36	VARCHAR2(255)	Valeur réservée 36 Réservé pour DataContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV37	VARCHAR2(255)	Valeur réservée 37 Réservé pour SourceFunction. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV38	VARCHAR2(255)	Valeur réservée 38 Réservé pour SourceOperationalContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV40 - 43	VARCHAR2(255)	Valeur réservée 40 - 43 Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV44	VARCHAR2(255)	Valeur réservée 44 Réservé pour DestinationThreatLevel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV45	VARCHAR2(255)	Valeur réservée 45 Réservé pour DestinationUserContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV46	VARCHAR2(255)	Valeur réservée 46 Réservé pour VirusStatus. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV47	VARCHAR2(255)	Valeur réservée 47 Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV48	VARCHAR2(255)	Valeur réservée 48 Réservé pour DestinationOperationalContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV49	VARCHAR2(255)	Valeur réservée 49 Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
REFERENCE_ID 01 - 20	number	Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
CV01 - 10	NUMBER	Valeur personnalisée 1 - 10 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles
CV11 - 20	DATE	Valeur personnalisée 11 - 20 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles
CV21 - 100	VARCHAR2(255)	Valeur personnalisée 21 - 100. Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles

EVT_AGENT_RPT_V

Cette vue fait référence à la table EVT_AGENT contenant les informations sur les collecteurs.

Nom de la colonne	Type de données	Commentaire
AGENT_ID	number	Identificateur du collecteur
AGENT	varchar2(64)	Nom du collecteur
PORT	varchar2(64)	Port du collecteur
REPORT_NAME	varchar2(255)	Nom de programme reporteur
PRODUCT_NAME	varchar2(255)	Nom du produit
SENSOR_NAME	varchar2(255)	Nom du capteur
SENSOR_TYPE	varchar2(5)	Type de capteur : H : basé sur l'hôte N : basé sur le réseau V : virus O : autre
DEVICE_CTGRY	varchar2(255)	Catégorie de périphérique
SOURCE_UUID	varchar2	UUID (Universal Unique Identifier) du composant source
DATE_CREATED	date	Date d'insertion

Nom de la colonne	Type de données	Commentaire
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_ASSET_RPT_V

Cette vue fait référence à la table EVT_ASSET contenant les informations sur les actifs.

Nom de la colonne	Type de données	Commentaire
EVENT_ASSET_ID	number	Identificateur des actifs de l'événement
ASSET_NAME	varchar2(255)	Nom de l'actif
PHYSICAL_ASSET_NAME	varchar2(255)	Nom de l'actif physique
REFERENCE_ASSET_ID	varchar2(100)	Identificateur de l'actif de référence, lien vers le système de gestion des actifs source.
MAC_ADDRESS	varchar2(100)	Adresse MAC
RACK_NUMBER	varchar2(50)	Numéro de rack
ROOM_NAME	varchar2(100)	Nom de la salle
BUILDING_NAME	varchar2(255)	Nom du bâtiment
CITY	varchar2(100)	Ville
STATE	varchar2(100)	État
COUNTRY	varchar2(100)	Pays
ZIP_CODE	varchar2(50)	Code postal
ASSET_CATEGORY_NAME	varchar2(100)	Nom de la catégorie d'actifs
NETWORK_IDENTITY_NAME	varchar2(255)	Nom de l'identité du réseau des actifs
ENVIRONMENT_IDENTITY_NAME	varchar2(255)	Nom de l'environnement
ASSET_VALUE_NAME	varchar2(50)	Nom de la valeur de l'actif
CRITICALITY_NAME	varchar2(50)	Nom relatif à la sévérité de l'actif
SENSITIVITY_NAME	varchar2(50)	Nom relatif à la sensibilité de l'actif
CONTACT_NAME_1	varchar2(255)	Nom du contact/organisation 1
CONTACT_NAME_2	varchar2(255)	Nom du contact/organisation 2
ORGANIZATION_NAME_1	varchar2(100)	Niveau d'organisation du propriétaire de l'actif 1
ORGANIZATION_NAME_2	varchar2(100)	Niveau d'organisation du propriétaire de l'actif 2
ORGANIZATION_NAME_3	varchar2(100)	Niveau d'organisation du propriétaire de l'actif 3
ORGANIZATION_NAME_4	varchar2(100)	Niveau d'organisation du propriétaire de l'actif 4
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_DEST_EVT_NAME_SMRY_1_RPT_V

Cette vue récapitule les événements par destination, taxinomie, nom, gravité et heure.

Nom de la colonne	Type de données	Commentaire
DESTINATION_IP	number	Adresse IP cible
DESTINATION_EVENT_ASSET_ID	number	Identificateur des actifs de l'événement
TAXONOMY_ID	number	Identificateur de taxinomie
EVENT_NAME_ID	number	Identificateur du nom de l'événement
SEVERITY	number	Degré de gravité de l'événement
CUSTOMER_ID	number	Identificateur du client
EVT_TIME	date	Heure de l'événement
EVT_COUNT	number	Nombre d'événements
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_DEST_SMRY_1_RPT_V

Cette vue contient les informations récapitulatives sur la destination des événements.

Nom de la colonne	Type de données	Commentaire
DESTINATION_IP	number	Adresse IP cible
DESTINATION_EVENT_ASSET_ID	number	Identificateur des actifs de l'événement
DESTINATION_PORT	varchar2(32)	Port de destination
DESTINATION_USR_ID	number	Identificateur de l'utilisateur de destination
TAXONOMY_ID	number	Identificateur de taxinomie
EVENT_NAME_ID	number	Identificateur du nom de l'événement
RESOURCE_ID	number	Identificateur de la ressource
AGENT_ID	number	Identificateur du collecteur
PROTOCOL_ID	number	Identificateur du protocole
SEVERITY	number	Degré de gravité de l'événement
CUSTOMER_ID	number	Identificateur du client
EVENT_TIME	date	Heure de l'événement
EVENT_CNT	number	Nombre d'événements
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_DEST_TXNMY_SMRY_1_RPT_V

Cette vue récapitule les événements par destination, taxinomie, gravité et heure.

Nom de la colonne	Type de données	Commentaire
DESTINATION_IP	number	Adresse IP cible
DESTINATION_EVENT_ASSET_ID	number	Identificateur des actifs de l'événement
TAXONOMY_ID	number	Identificateur de taxinomie
SEVERITY	number	Degré de gravité de l'événement
CUSTOMER_ID	number	Identificateur du client
EVENT_TIME	date	Heure de l'événement
EVENT_COUNT	number	Nombre d'événements
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_NAME_RPT_V

Cette vue fait référence à la table EVT_NAME contenant les informations de nom des événements.

Nom de la colonne	Type de données	Commentaire
EVENT_NAME_ID	number	Identificateur du nom de l'événement
EVENT_NAME	varchar2(255)	Nom de l'événement
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_PORT_SMRY_1_RPT_V

Cette vue récapitule les événements par port de destination, gravité et heure.

Nom de la colonne	Type de données	Commentaire
DESTINATION_PORT	Varchar2(32)	Port de destination
SEVERITY	number	Degré de gravité de l'événement
CUSTOMER_ID	number	Identificateur du client
EVENT_TIME	date	Heure de l'événement
EVENT_COUNT	number	Nombre d'événements
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_PRTCL_RPT_V

Cette vue fait référence à la table EVT_PRTCL contenant les informations sur les protocoles des événements.

Nom de la colonne	Type de données	Commentaire
PROTOCOL_ID	number	Identificateur du protocole
PROTOCOL_NAME	varchar2(255)	Nom du protocole
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_RSRC_RPT_V

Cette vue fait référence à la table EVT_RSRC contenant les informations sur les ressources des événements.

Nom de la colonne	Type de données	Commentaire
RESOURCE_ID	number	Identificateur de la ressource
RESOURCE_NAME	varchar2(255)	Nom de la ressource
SUBRESOURCE_NAME	varchar2(255)	Nom de la sous-ressource
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_SEV_SMRY_1_RPT_V

Cette vue récapitule les événements par gravité et heure.

Nom de la colonne	Type de données	Commentaire
SEVERITY	number	Degré de gravité de l'événement
CUSTOMER_ID	number	Identificateur du client
EVENT_TIME	date	Heure de l'événement
EVENT_COUNT	number	Nombre d'événements
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_SRC_SMRY_1_RPT_V

Cette vue contient les informations récapitulatives sur la destination et la source des événements.

Nom de la colonne	Type de données	Commentaire
SOURCE_IP	number	Adresse IP source
SOURCE_EVENT_ASSET_ID	number	Identificateur des actifs de l'événement source
SOURCE_PORT	varchar2(32)	Port source
SOURCE_USER_ID	number	Identificateur de l'utilisateur source
TAXONOMY_ID	number	Identificateur de taxinomie
EVENT_NAME_ID	number	Identificateur du nom de l'événement
RESOURCE_ID	number	Identificateur de la ressource
AGENT_ID	number	Identificateur du collecteur
PROTOCOL_ID	number	Identificateur du protocole
SEVERITY	number	Degré de gravité de l'événement
CUSTOMER_ID	number	Identificateur du client
EVENT_TIME	date	Heure de l'événement
EVENT_COUNT	number	Nombre d'événements
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_TXNMY_RPT_V

Cette vue fait référence à la table EVT_TXNMY contenant les informations de taxinomie des événements.

Nom de la colonne	Type de données	Commentaire
TAXONOMY_ID	number	Identificateur de taxinomie
TAXONOMY_LEVEL_1	varchar2(100)	Niveau de taxinomie 1
TAXONOMY_LEVEL_2	varchar2(100)	Niveau de taxinomie 2
TAXONOMY_LEVEL_3	varchar2(100)	Niveau de taxinomie 3
TAXONOMY_LEVEL_4	varchar2(100)	Niveau de taxinomie 4
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_USR_RPT_V

Cette vue fait référence à la table EVT_USR contenant les informations sur les utilisateurs des événements.

Nom de la colonne	Type de données	Commentaire
USER_ID	number	Identificateur de l'utilisateur
USER_NAME	varchar2(255)	Nom de l'utilisateur
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

EXTERNAL_DATA_RPT_V

Cette vue fait référence à la table EXTERNAL_DATA contenant les données externes.

Nom de la colonne	Type de données	Commentaire
EXTERNAL_DATA_ID	number	Identificateur des données externes
SOURCE_NAME	varchar2(50)	Nom de la source
SOURCE_DATA_ID	varchar2(255)	Identificateur des données sources
EXTERNAL_DATA	text	Données externes
EXTERNAL_DATA_TYPE	varchar2(10)	Type de données externes
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

HIST_ EVENTS_RPT_V

Cette vue contient les événements historiques (événements restaurés des archives).

HIST_ INCIDENTS_RPT_V

Cette vue contient les événements historiques (événements restaurés des archives).

IMAGES_RPT_V

Cette vue fait référence à la table IMAGES contenant les informations sur les images du système.

Nom de la colonne	Type de données	Commentaire
NAME	VARCHAR2(128)	Nom de l'image
TYPE	VARCHAR2(64)	Type d'image
DATA	CLOB	Données de l'image
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion

Nom de la colonne	Type de données	Commentaire
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

INCIDENTS_ASSETS_RPT_V

Cette vue fait référence à la table INCIDENTS_ASSETS contenant les informations sur les actifs concernés par les incidents créés dans la console Sentinel.

Nom de la colonne	Type de données	Commentaire
INC_ID	NUMBER	Identificateur de l'incident - numéro de séquence
ASSET_ID	varchar2	UUID (Universal Unique Identifier) de l'actif
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

INCIDENTS_EVENTS_RPT_V

Cette vue fait référence à la table INCIDENTS_EVENTS contenant les informations sur les événements des incidents créés dans la console Sentinel.

Nom de la colonne	Type de données	Commentaire
INC_ID	NUMBER	Identificateur de l'incident - numéro de séquence
EVT_ID	varchar2	UUID (Universal Unique Identifier) de l'événement
EVT_TIME	DATE	Heure de l'événement
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

INCIDENTS_RPT_V

Cette vue fait référence à la table INCIDENTS contenant les informations détaillées sur les incidents créés dans la console Sentinel.

Nom de la colonne	Type de données	Commentaire
INC_ID	NUMBER	Identificateur de l'incident - numéro de séquence
NAME	VARCHAR2(255)	Nom de l'incident
SEVERITY	NUMBER	Degré de gravité de l'incident
STT_ID	NUMBER	ID de l'état de l'incident

Nom de la colonne	Type de données	Commentaire
SEVERITY_RATING	VARCHAR2(32)	Moyenne de tous les degrés de gravité des événements liés à un incident
VULNERABILITY_RATING	VARCHAR2(32)	Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
CRITICALITY_RATING	VARCHAR2(32)	Réservé pour utilisation ultérieure par Novell. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour
INC_DESC	varchar2(4000)	Description de l'incident
INC_PRIORITY	number	Priorité de l'incident
INC_CAT	varchar2(255)	Catégorie de l'incident
INC_RES	varchar2(4000)	Résolution de l'incident

INCIDENTS_VULN_RPT_V

Cette vue fait référence à la table INCIDENTS_VULN contenant les informations sur la vulnérabilité des incidents créés dans la console Sentinel.

Nom de la colonne	Type de données	Commentaire
INC_ID	NUMBER	Identificateur de l'incident - numéro de séquence
VULN_ID	varchar2(36)	UUID (Universal Unique Identifier) de la vulnérabilité
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

L_STAT_RPT_V

Cette vue fait référence à la table L_STAT contenant les statistiques.

Nom de la colonne	Type de données	Commentaire
RES_NAME	VARCHAR2(32)	Nom de la ressource
STATS_NAME	VARCHAR2(32)	Nom de la statistique
STATS_VALUE	VARCHAR2(32)	Valeur de la statistique
OPEN_TOT_SECS	NUMBER	Nombre de secondes depuis 1970.

LOGS_RPT_V

Cette vue fait référence à la table LOGS_RPT contenant les informations de consignation.

Table LOGS		
Nom de la colonne	**Type de données**	**Commentaire**
LOG_ID	NUMBER	Numéro de séquence
TIME	DATE	Date du journal
MODULE	VARCHAR2(64)	Module auquel est destiné le fichier journal
TEXT	VARCHAR2(4000)	Texte du journal

NETWORK_IDENTITY_RPT_V

Cette vue fait référence à la table NETWORK_IDENTITY_LKUP contenant les informations sur l'identité de réseau des actifs.

Nom de la colonne	Type de données	Commentaire
NETWORK_IDENTITY_CD	varchar2(5)	Code d'identité du réseau
NETWORK_IDENTITY_NAME	varchar2(255)	Nom de l'identité du réseau
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ORGANIZATION_RPT_V

Cette vue fait référence à la table ORGANIZATION contenant les informations sur les organisations (actifs).

Nom de la colonne	Type de données	Commentaire
ORGANIZATION_ID	varchar2	Identificateur de l'organisation
ORGANIZATION_NAME	varchar2(100)	Nom de l'organisation
CUSTOMER_ID	number	Identificateur du client
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

PERSON_RPT_V

Cette vue fait référence à la table PERSION contenant les informations sur les personnes (actifs).

Nom de la colonne	Type de données	Commentaire
PERSON_ID	varchar2	Identificateur de la personne
FIRST_NAME	varchar2(255)	Prénom
LAST_NAME	varchar2(255)	Nom
CUSTOMER_ID	number	Identificateur du client
PHONE_NUMBER	varchar2(50)	Numéro de téléphone
EMAIL_ADDRESS	varchar2(255)	Adresse électronique
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

PHYSICAL_ASSET_RPT_V

Cette vue fait référence à la table PHYSICAL_ASSET contenant les informations sur les actifs physiques.

Nom de la colonne	Type de données	Commentaire
PHYSICAL_ASSET_ID	varchar2	Identificateur de l'actif physique
CUSTOMER_ID	number	Identificateur du client
LOCATION_ID	number	Identificateur de l'emplacement
HOST_NAME	varchar2(255)	Nom de l'hôte
IP_ADDRESS	number	Adresse IP
NETWORK_IDENTITY_CD	varchar2(5)	Code d'identité du réseau
MAC_ADDRESS	varchar2(100)	Adresse MAC
RACK_NUMBER	varchar2(50)	Numéro de rack
ROOM_NAME	varchar2(100)	Nom de la salle
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

○PRODUCT_RPT_V

Cette vue fait référence à la table PRDT contenant les informations produit des actifs.

Nom de la colonne	Type de données	Commentaire
PRODUCT_ID	number	Identificateur du produit
PRODUCT_NAME	varchar2(255)	Nom du produit
PRODUCT_VERSION	varchar2(100)	Version du produit
VENDOR_ID	number	Identificateur du fournisseur
DATE_CREATED	date	Date d'insertion

Nom de la colonne	Type de données	Commentaire
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

ROLE_RPT_V

Cette vue fait référence à la table ROLE_LKUP contenant les informations sur les rôles des utilisateurs (actifs).

Nom de la colonne	Type de données	Commentaire
ROLE_CODE	varchar2(5)	Code du rôle
ROLE_NAME	varchar2(255)	Nom du rôle
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

SENSITIVITY_RPT_V

Cette vue fait référence à la table SENSITIVITY_LKUP contenant les informations de sensibilité des actifs.

Nom de la colonne	Type de données	Commentaire
SENSITIVITY_CODE	varchar2(5)	Code de sensibilité de l'actif
SENSITIVITY_NAME	varchar2(50)	Nom relatif à la sensibilité de l'actif
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID utilisateur
MODIFIED_BY	number	ID utilisateur

STATES_RPT_V

Cette vue fait référence à la table STATES qui contient les définitions des états définis par les applications ou le contexte.

Nom de la colonne	Type de données	Commentaire
STT_ID	NUMBER	ID de l'état - numéro de séquence
CONTEXT	VARCHAR2(64)	Contexte de l'état, à savoir cas, incident, utilisateur
NAME	VARCHAR2(64)	Nom de l'état
TERMINAL_FLAG	VARCHAR2(1)	Indique si l'état de l'incident est résolu
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour

Vue UNASSIGNED_INCIDENTS_RPT_V

Cette vue fait référence aux tables CASES et INCIDENTS qui rapportent les cas non attribués.

Nom	Type de données
INC_ID	NUMBER
NAME	VARCHAR2(255)
SEVERITY	NUMBER
STT_ID	NUMBER
SEVERITY_RATING	VARCHAR2(32)
VULNERABILITY_RATING	VARCHAR2(32)
CRITICALITY_RATING	VARCHAR2(32)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER
INC_DESC	VARCHAR2(4000)
INC_PRIORITY	NUMBER
INC_CAT	VARCHAR2(255)
INC_RES	VARCHAR2(4000)

USERS_RPT_V

Cette vue fait référence à la table USERS qui répertorie l'ensemble des utilisateurs de l'application. Des utilisateurs de base de données seront également créés pour permettre l'utilisation d'outils de rapports tiers.

Nom de la colonne	Type de données	Commentaire
USR_ID	NUMBER	Identificateur de l'utilisateur - numéro de séquence
NAME	VARCHAR2(64)	Nom d'utilisateur court et unique utilisé pour la connexion
CNT_ID	NUMBER	ID du contact - numéro de séquence
STT_ID	NUMBER	ID de l'état. Le statut est actif ou inactif.
DESCRIPTION	VARCHAR2(512)	Commentaires
DATE_CREATED	DATE	Date d'insertion
DATE_MODIFIED	DATE	Date de la dernière mise à jour
CREATED_BY	NUMBER	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	NUMBER	ID de l'utilisateur à l'origine de la dernière mise à jour
PERMISSIONS	VARCHAR2(4000)	Autorisations actuellement attribuées à l'utilisateur Sentinel
FILTER	VARCHAR2(128)	Filtre de sécurité actuellement attribué à l'utilisateur Sentinel
UPPER_NAME	VARCHAR2(64)	Nom d'utilisateur en majuscules
DOMAIN_AUTH_IND	NUMBER	Indication de l'authentification de

Nom de la colonne	Type de données	Commentaire
		domaine

VENDOR_RPT_V

Cette vue fait référence à la table VNDR contenant les informations relatives aux fournisseurs de produits associés aux actifs.

Nom de la colonne	Type de données	Commentaire
VENDOR_ID	number	Identificateur du fournisseur
VENDOR_NAME	varchar2(255)	Nom du fournisseur
DATE_CREATED	date	Date d'insertion
DATE_MODIFIED	date	Date de la dernière mise à jour
CREATED_BY	number	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	number	ID de l'utilisateur à l'origine de la dernière mise à jour

VULN_CALC_SEVERITY_RPT_V

Cette vue fait référence aux tables VULN_RSRC et VULN pour le calcul du taux de gravité de la vulnérabilité du système Sentinel en fonction des vulnérabilités actuelles.

Nom de la colonne	Type de données
RSRC_ID	VARCHAR22(36)
IP	VARCHAR22(32)
HOST_NAME	VARCHAR22(255)
CRITICALITY	NUMBER
ASSIGNED_VULN_SEVERITY	NUMBER
VULN_COUNT	Nombre de vulnérabilités pour la ressource spécifiée
CALC_SEVERITY	Gravité calculée en fonction des valeurs ASSIGNED_VULN_SEVERITY et CRITICALITY

VULN_CODE_RPT_V

Cette vue fait référence à la table VULN_CODE contenant les codes de vulnérabilité standard tels que les CAN et les CVE de Mitre.

Nom de la colonne	Type de données
VULN_CODE_ID	VARCHAR2(36)
VULN_ID	VARCHAR2(36)
VULN_CODE_TYPE	VARCHAR2(64)
VULN_CODE_VALUE	VARCHAR2(255)
URL	VARCHAR2(512)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_INFO_RPT_V

Cette vue fait référence à la table VULN_INFO contenant les informations supplémentaires rapportées au cours d'une analyse.

Nom de la colonne	Type de données
VULN_INFO_ID	VARCHAR2(36)
VULN_ID	VARCHAR2(36)
VULN_INFO_TYPE	VARCHAR2(36)
VULN_INFO_VALUE	VARCHAR2(2000)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_RPT_V

Cette vue fait référence à la table VULN contenant les informations relatives au système analysé. Chaque scanner dispose de sa propre entrée pour chacun des systèmes.

Nom de la colonne	Type de données
VULN_ID	VARCHAR2(36)
RSRC_ID	VARCHAR2(36)
PORT_NAME	VARCHAR2(64)
PORT_NUMBER	NUMBER
NETWORK_PROTOCOL	NUMBER
APPLICATION_PROTOCOL	VARCHAR2(64)
ASSIGNED_VULN_SEVERITY	NUMBER
COMPUTED_VULN_SEVERITY	NUMBER
VULN_DESCRIPTION	CLOB
VULN_SOLUTION	CLOB
VULN_SUMMARY	VARCHAR2(1000)
BEGIN_EFFECTIVE_DATE	DATE
END_EFFECTIVE_DATE	DATE
DETECTED_OS	VARCHAR2(64)
DETECTED_OS_VERSION	VARCHAR2(64)
SCANNED_APP	VARCHAR2(64)
SCANNED_APP_VERSION	VARCHAR2(64)
VULN_USER_NAME	VARCHAR2(64)
VULN_USER_DOMAIN	VARCHAR2(64)
VULN_TAXONOMY	VARCHAR2(1000)
SCANNER_CLASSIFICATION	VARCHAR2(255)
VULN_NAME	VARCHAR2(300)
VULN_MODULE	VARCHAR2(64)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_RSRC_RPT_V

Cette vue fait référence à la table VULN_RSRC contenant toutes les ressources analysées au cours d'une analyse donnée.

Nom de la colonne	Type de données
RSRC_ID	VARCHAR2(36)
SCANNER_ID	VARCHAR2(36)
IP	VARCHAR2(32)
HOST_NAME	VARCHAR2(255)
LOCATION	VARCHAR2(128)
DEPARTMENT	VARCHAR2(128)
BUSINESS_SYSTEM	VARCHAR2(128)
OPERATIONAL_ENVIRONMENT	VARCHAR2(64)
CRITICALITY	NUMBER
REGULATION	VARCHAR2(128)
REGULATION_RATING	VARCHAR2(64)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_RSRC_SCAN_RPT_V

Cette vue fait référence à la table VULN_RSRC_SCAN contenant toutes les ressources analysées au cours d'une analyse donnée.

Nom de la colonne	Type de données
RSRC_ID	VARCHAR2(36)
SCAN_ID	VARCHAR2(36)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_SCAN_RPT_V

Cette vue fait référence à la table qui contient les informations relatives aux analyses.

Nom de la colonne	Type de données
SCAN_ID	VARCHAR2(36)
SCANNER_ID	VARCHAR2(36)
SCAN_TYPE	VARCHAR2(10)
SCAN_START_DATE	DATE
SCAN_END_DATE	DATE
CONSOLIDATION_SERVER	VARCHAR2(64)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_SCAN_VULN_RPT_V

Cette vue fait référence à la table VULN_SCAN_VULN contenant les vulnérabilités détectées au cours des analyses.

Nom de la colonne	Type de données
SCAN_ID	VARCHAR2(36)
VULN_ID	VARCHAR2(36)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

VULN_SCANNER_RPT_V

Cette vue fait référence à la table VULN_SCANNER contenant les informations relatives aux scanners recherchant les vulnérabilités.

Nom de la colonne	Type de données
SCANNER_ID	VARCHAR2(36)
PRODUCT_NAME	VARCHAR2(100)
PRODUCT_VERSION	VARCHAR2(64)
SCANNER_TYPE	VARCHAR2(64)
VENDOR	VARCHAR2(100)
SCANNER_INSTANCE	VARCHAR2(64)
DATE_CREATED	DATE
DATE_MODIFIED	DATE
CREATED_BY	NUMBER
MODIFIED_BY	NUMBER

12 Vues de base de données Sentinel pour Microsoft SQL Server

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

Ce chapitre répertorie les vues des schémas Sentinel pour Microsoft SQL Server. Ces dernières contiennent des informations vous permettant de développer vos propres rapports (rapports Crystal).

Vues

ADV_ALERT_CVE_RPT_V

Cette vue fait référence à la table ADV_ALERT_CVE contenant le numéro d'identification des alertes Advisor.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	int	Identificateur d'annotation - numéro de séquence
CVE	varchar	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_ALERT_PRODUCT_RPT_V

Cette vue fait référence à la table ADV_ALERT_PRODUCT contenant les informations de produit Advisor, telles que le numéro d'identification du Service Pack, la version et la date de création.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	int	Identificateur d'annotation - numéro de séquence
SERVICE_PACK_ID	int	
VENDOR	varchar	
PRODUCT	varchar	
VERSION	varchar	Contient le numéro de version
SERVICE_PACK	varchar	
PRIMARY_FLAG	int	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour

Nom de la colonne	Type de données	Commentaire
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_ALERT_RPT_V

Cette vue fait référence à la table ADV_ALERT contenant les informations sur les alertes Advisor, telles que le nom, le type de menace et la date de publication.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	int	Identificateur d'annotation - numéro de séquence
VERSION	int	Contient le numéro de version
TEMPLATE_ID	int	
TEMPLATE_NAME	varchar	
THREAT_CATEGORY_NAME	varchar	
THREAT_TYPE_NAME	varchar	
HEADLINE	text	
FIRST_PUBLISHED	datetime	
LAST_PUBLISHED	datetime	
STATUS	varchar	
URGENCY_ID	int	
CREDIBILITY_ID	int	
SEVERITY_ID	int	
SUMMARY	text	
LEGAL_DISCLAIMER	text	
COPYRIGHT	varchar	
BEGIN_EFFECTIVE_DATE	datetime	
END_EFFECTIVE_DATE	datetime	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_ATTACK_ALERT_RPT_V

Cette vue fait référence à la table ADV_ATTACK_ALERT contenant les informations sur les attaques Advisor, telles que le nom, le type de menace et la date de publication.

Nom de la colonne	Type de données	Commentaire
ATTACK_ID	int	
ALERT_ID	int	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_ATTACK_CVE_RPT_V

Cette vue fait référence à la table ADV_ATTACK_CVE contenant les informations CVE Advisor.

Nom de la colonne	Type de données	Commentaire
ATTACK_ID	int	
CVE	varchar	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_ATTACK_MAP_RPT_V

Cette vue fait référence à la table ADV_ATTACK_MAP contenant les informations d'assignation Advisor.

Nom de la colonne	Type de données	Commentaire
ATTACK_KEY	int	
ATTACK_ID	int	
SERVICE_PACK_ID	int	
ATTACK_NAME	varchar	
ATTACK_CODE	varchar	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_by	int	ID utilisateur

ADV_ATTACK_PLUGIN_RPT_V

Cette vue fait référence à la table ADV_ATTACK_PLUGIN contenant les informations de plug-in Advisor.

Nom de la colonne	Type de données	Commentaire
PLUGIN_KEY	int	
ATTACK_ID	int	
SERVICE_PACK_ID	int	
PLUGIN_ID	varchar	
PLUGIN_NAME	varchar	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_ATTACK_RPT_V

Cette vue fait référence à la table ADV_ATTACK contenant les informations sur les attaques Advisor.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	int	
TRUSECURE_ATTACK_NAME	int	
FEED_DATE_CREATED	datetime	
FEED_DATE_UPDATED	datetime	
ATTACK_CATEGORY	varchar	
URGENCY_ID	int	
SEVERITY_ID	int	
LOCAL	int	
REMOTE	int	
BEGIN_EFFECTIVE_DATE	datetime	
END_EFFECTIVE_DATE	datetime	
DESCRIPTION	text	
SCENARIO	text	
IMPACT	text	
SAFEGUARDS	text	
PATCHES	text	
FALSE_POSITIVES	text	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_CREDIBILITY_RPT_V

Cette vue fait référence à la table ADV_CREDIBILITY contenant les informations de crédibilité Advisor.

Nom de la colonne	Type de données	Commentaire
CREDIBILITY_ID	int	
CREDIBILITY_RATING	varchar	
CREDIBILITY_EXPLANATION	varchar	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_FEED_RPT_V

Cette vue fait référence à la table ADV_FEED contenant les informations de flux de données Advisor, telles que le nom des flux de données et la date.

Nom de la colonne	Type de données	Commentaire
FEED_NAME	varchar	
FEED_FILE	varchar	
BEGIN_DATE	datetime	
END_DATE	datetime	
FEED_INSERT	int	
FEED_UPDATE	int	
FEED_EXPIRE	int	

ADV_PRODUCT_RPT_V

Cette vue fait référence à la table ADV_PRODUCT contenant les informations de produit Advisor, telles que le nom du fournisseur et l'ID de produit.

Nom de la colonne	Type de données	Commentaire
PRODUCT_ID	int	
VENDOR_ID	int	
PRODUCT_CATEGORY_ID	int	
PRODUCT_CATEGORY_NAME	varchar	
PRODUCT_TYPE-ID	int	
PRODUCT_TYPE_NAME	varchar	
PRODUCT_NAME	varchar	
PRODUCT_DESCRIPTION	varchar	
FEED_DATE_CREATED	datetime	
FEED_DATE_UPDATED	datetime	
ACTIVE_FLAG	int	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_PRODUCT_SERVICE_PACK_RPT_V

Cette vue fait référence à la table ADV_PRODUCT_SERVICE _PACK contenant les informations sur le Service Pack Advisor, telles que le nom du Service Pack, l'ID de version et la date.

Nom de la colonne	Type de données	Commentaire
SERVICE_PACK_ID	int	
VERSION_ID	int	Contient le numéro de version
SERVICE_PACK_NAME	varchar	
FEED_DATE_CREATED	datetime	
FEED_DATE_UPDATED	datetime	

Nom de la colonne	Type de données	Commentaire
ACTIVE_FLAG	int	
BEGIN_EFFECTIVE_DATE	datetime	
END_EFFECTIVE_DATE	datetime	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_PRODUCT_VERSION_RPT_V

Cette vue fait référence à la table ADV_PRODUCT_VERSION contenant les informations de version du produit Advisor, telles que le nom de la version, l'ID de produit et l'ID de version.

Nom de la colonne	Type de données	Commentaire
VERSION_ID	int	Contient le numéro de version
PRODUCT_ID	int	
VERSION_NAME	varchar	
FEED_DATE_CREATED	datetime	
FEED_DATE_UPDATED	datetime	
ACTIVE_FLAG	int	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	int	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_SEVERITY_RPT_V

Cette vue fait référence à la table ADV_SEVERITY contenant les informations relatives au taux de gravité Advisor.

Nom de la colonne	Type de données	Commentaire
SEVERITY_ID	int	
SEVERITY_RATING	varchar	
SEVERITY_EXPLANATION	varchar	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_SUBALERT_RPT_V

Cette vue fait référence à la table ADV_SUBALERT.

Nom de la colonne	Type de données	Commentaire
ALERT_ID	int	
SUBALERT_ID	int	

Nom de la colonne	Type de données	Commentaire
CHANGED_SECTIONS	varchar	
VARIANTS	text	
VIRUS_NAME	text	
DESCRIPTION	text	
IMPACT	text	
WARNING_INDICATORS	text	
TECHNICAL_INFO	text	
TRUSECURE_COMMENTS	text	
VENDOR_ANNOUNCEMENTS	text	
SAFEGUARDS	text	
PATCHES_SOFTWARE	text	
ALERT_HISTORY	text	
BACKGROUND_INFO	text	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_URGENCY_RPT_V

Cette vue fait référence à la table ADV_URGENCY.

Nom de la colonne	Type de données	Commentaire
URGENCY_ID	int	
URGENCY_RATING	varchar	
URGENCY_EXPLANATION	varchar	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_VENDOR_RPT_V

Cette vue fait référence à la table ADV_VENDOR contenant les coordonnées associées à Advisor.

Nom de la colonne	Type de données	Commentaire
VENDOR_ID	int	
VENDOR_NAME	varchar	
CONTACT_PERSON	varchar	
ADDRESS_LINE_1	varchar	
ADDRESS_LINE_2	varchar	
ADDRESS_LINE_3	varchar	
ADDRESS_LINE_4	varchar	
CITY	varchar	
STATE	varchar	

Nom de la colonne	Type de données	Commentaire
COUNTRY	varchar	
ZIP_CODE	varchar	
URL	varchar	
PHONE	varchar	
FAX	varchar	
EMAIL	varchar	
PAGER	varchar	
FEED_DATE_CREATED	datetime	
FEED_DATE_UPDATED	datetime	
ACTIVE_FLAG	int	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ADV_VULN_PRODUCT_RPT_V

Cette vue fait référence à la table ADV_VULN_PRODUCT contenant les ID de vulnérabilité Advisor et les ID de Service Pack.

Nom de la colonne	Type de données	Commentaire
ATTACK_ID	int	
SERVICE_PACK_ID	int	
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

ANNOTATIONS_RPT_V

Cette vue fait référence à la table ANNOTATIONS contenant la documentation ou les notes pouvant être associées aux objets du système Sentinel, telles que les cas et les incidents.

Nom de la colonne	Type de données	Commentaire
ANN_ID	INT	Identificateur d'annotation - numéro de séquence
TEXT	VARCHAR(4000)	Documentation ou notes
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
ACTION	Varchar(255)	Opération

ASSET_CTGRY_RPT_V

Cette vue fait référence à la table ASSET_CTGRY contenant les informations sur les catégories d'actifs (par exemple, matériel, logiciel, système d'exploitation, base de données, etc.).

Nom de la colonne	Type de données	Commentaire
ASSET_CATEGORY_ID	bigint	Identificateur de la catégorie d'actifs
ASSET_CATEGORY_NAME	varchar(100)	Nom de la catégorie d'actifs
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_HOSTNAME_RPT_V

Cette vue fait référence à la table ASSET_HOSTNAME contenant les informations sur les noms d'hôte de remplacement des actifs.

Nom de la colonne	Type de données	Commentaire
ASSET_HOSTNAME_ID	uniqueidentifier	Identificateur du nom d'hôte de remplacement de l'actif
PHYSICAL_ASSET_ID	uniqueidentifier	Identificateur de l'actif physique
HOST_NAME	Varchar(255)	Nom de l'hôte
CUSTOMER_ID	bigint	Identificateur du client
DATE_CREATED	datetime	Date de la dernière mise à jour
DATE_MODIFIED	datetime	ID de l'utilisateur à l'origine de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_IP_RPT_V

Cette vue fait référence à la table ASSET_IP contenant les informations sur les adresses IP de remplacement des actifs.

Nom de la colonne	Type de données	Commentaire
ASSET_IP_ID	Uniqueidentifier	Identificateur de l'adresse IP de remplacement de l'actif
PHYSICAL_ASSET_ID	uniqueidentifier	Identificateur de l'actif physique
IP_ADDRESS	int	Adresse IP de l'actif
CUSTOMER_ID	bigint	Identificateur du client
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_LOCATION_RPT_V

Cette vue fait référence à la table ASSET_LOC contenant les informations sur l'emplacement géographique des actifs.

Nom de la colonne	Type de données	Commentaire
LOCATION_ID	bigint	Identificateur de l'emplacement
CUSTOMER_ID	bigint	Identificateur du client
BUILDING_NAME	varchar(255)	Nom du bâtiment
ADDRESS_LINE_1	varchar(255)	Adresse 1
ADDRESS_LINE_2	varchar(255)	Adresse 2
CITY	varchar(100)	Ville
STATE	varchar(100)	État
COUNTRY	varchar(100)	Pays
ZIP_CODE	varchar(50)	Code postal
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_RPT_V

Cette vue fait référence à la table ASSET contenant les informations sur les actifs physiques et non physiques.

Nom de la colonne	Type de données	Commentaire
ASSET_ID	uniqueidentifier	Identificateur de l'actif
CUSTOMER_ID	bigint	Identificateur du client
ASSET_NAME	varchar(255)	Nom de l'actif
PHYSICAL_ASSET_ID	uniqueidentifier	Identificateur de l'actif physique
PRODUCT_ID	bigint	Identificateur du produit
ASSET_CATEGORY_ID	bigint	Identificateur de la catégorie d'actifs
ENVIRONMENT_IDENTITY_CD	varchar(5)	Code d'identification de l'environnement
PHYSICAL_ASSET_IND	bit	Indicateur de l'actif physique
ASSET_VALUE_CD	varchar(5)	Code de la valeur de l'actif
CRITICALITY_CODE	varchar(5)	Code de sévérité de l'actif
SENSITIVITY_CODE	varchar(5)	Code de sensibilité de l'actif
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_VALUE_RPT_V

Cette vue fait référence à la table ASSET_VAL_LKUP contenant les informations sur la valeur des actifs.

Nom de la colonne	Type de données	Commentaire
ASSET_VALUE_CODE	varchar(5)	Code de la valeur de l'actif
ASSET_VALUE_NAME	varchar(50)	Nom de la valeur de l'actif
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSET_X_ENTITY_X_ROLE_RPT_V

Cette vue fait référence à la table ASSET_X_ENTITY_X_ROLE qui associe une personne ou une organisation à un actif.

Nom de la colonne	Type de données	Commentaire
PERSON_ID	uniqueidentifier	Identificateur de la personne
ORGANIZATION_ID	uniqueidentifier	Identificateur de l'organisation
ROLE_CODE	varchar(5)	Code du rôle
ASSET_ID	uniqueidentifier	Identificateur de l'actif
ENTITY_TYPE_CODE	varchar(5)	Code du type d'entité
PERSON_ROLE_SEQUENCE	int	Ordre des personnes appartenant à un rôle donné
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ASSOCIATIONS_RPT_V

Cette vue fait référence à la table ASSOCIATIONS qui associe les utilisateurs aux incidents, les incidents aux annotations, etc.

Nom de la colonne	Type de données	Commentaire
TABLE1	VARCHAR(64)	Nom de la table 1. Par exemple, incidents
ID1	VARCHAR(36)	ID1. Par exemple, ID de l'incident
TABLE2	VARCHAR(64)	Nom de la table 2. Par exemple, utilisateurs
ID2	VARCHAR(36)	ID2. Par exemple, ID de l'utilisateur
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion

Nom de la colonne	Type de données	Commentaire
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

ATTACHMENTS_RPT_V

Cette vue fait référence à la table ATTACHMENTS contenant les informations sur les pièces jointes.

Nom de la colonne	Type de données	Commentaire
ATTACHMENT_ID	int	Identificateur de la pièce jointe
NAME	varchar(255)	Nom de la pièce jointe
SOURCE_REFERENCE	varchar(64)	Référence de la source
TYPE	varchar(32)	Type de la pièce jointe
SUB_TYPE	varchar(32)	Sous-type de la pièce jointe
FILE_EXTENSION	varchar(32)	Extension du fichier
ATTACHMENT_DESCRIPTION	varchar(255)	Description de la pièce jointe
DATA	clob	Données de la pièce jointe
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

CONFIGS_RPT_V

Cette vue fait référence à la table CONFIGS contenant les informations générales de configuration de l'application.

Nom de la colonne	Type de données	Commentaire
USR_ID	VARCHAR(32)	Nom de l'utilisateur
APPLICATION	VARCHAR(255)	Identificateur de l'application
UNIT	VARCHAR(64)	Unité de l'application
VALUE	VARCHAR(255)	Valeur de texte le cas échéant
DATA	TEXT	Données XML
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

CONTACTS_RPT_V

Cette vue fait référence à la table CONTACTS contenant les informations sur les contacts.

Nom de la colonne	Type de données	Commentaire
CNT_ID	INT	ID du contact - numéro de séquence
FIRST_NAME	VARCHAR(20)	Prénom du contact

Nom de la colonne	Type de données	Commentaire
LAST_NAME	VARCHAR(30)	Nom du contact
TITLE	VARCHAR(128)	Titre du contact
DEPARTMENT	VARCHAR(128)	Service
PHONE	VARCHAR(64)	Téléphone du contact
EMAIL	VARCHAR(255)	Adresse électronique du contact
PAGER	VARCHAR(64)	Pager du contact
CELL	VARCHAR(64)	Téléphone portable du contact
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

CORRELATED_EVENTS_RPT_V

Cette vue fait référence aux tables CORRELATED_EVENTS_* contenant les informations sur les événements corrélés.

Nom de la colonne	Type de données	Commentaire
PARENT_EVT_ID	uniqueidentifier	UUID (Universal Unique Identifier) de l'événement parent
CHILD_EVT_ID	uniqueidentifier	UUID (Universal Unique Identifier) de l'événement enfant
PARENT_EVT_TIME	DATETIME	Date de création de l'événement parent
CHILD_EVT_TIME	DATETIME	Date de création de l'événement enfant
DATE_CREATED	DATE	Date d'insertion générée par le service DAS
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

CORRELATED_EVENTS_RPT_V1

Cette vue contient les événements corrélés historiques et actuels (événements corrélés importés des archives).

Nom de la colonne	Type de données	Commentaire
PARENT_EVT_ID	uniqueidentifier	UUID (Universal Unique Identifier) de l'événement parent
CHILD_EVT_ID	uniqueidentifier	UUID (Universal Unique Identifier) de l'événement enfant
PARENT_EVT_TIME	DATETIME	Heure de l'événement parent
CHILD_EVT_TIME	DATETIME	Heure de l'événement enfant
DATE_CREATED	DATETIME	Date d'insertion générée par le service DAS
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

CRITICALITY_RPT_V

Cette vue fait référence à la table CRIT_LKUP contenant les informations sur le degré de sévérité des actifs.

Nom de la colonne	Type de données	Commentaire
CRITICALITY_CODE	varchar(5)	Code de sévérité de l'actif
CRITICALITY_NAME	varchar(50)	Nom relatif à la sévérité de l'actif
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

CUST_RPT_V

Cette vue fait référence à la table CUST contenant les informations sur les clients MSSP.

Nom de la colonne	Type de données	Commentaire
CUSTOMER_ID	bigint	Identificateur du client
CUSTOMER_NAME	varchar(255)	Nom du client
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ENTITY_TYPE_RPT_V

Cette vue fait référence à la table ENTITY_TYP qui contient les informations sur les types d'entités (personne, organisation).

Nom de la colonne	Type de données	Commentaire
ENTITY_TYPE_CODE	varchar(5)	Code du type d'entité
ENTITY_TYPE_NAME	varchar(50)	Nom du type d'entité
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ENV_IDENTITY_RPT_V

Cette vue fait référence à la table ENV_IDENTITY_LKUP contenant les informations sur l'identité de l'environnement des actifs.

Nom de la colonne	Type de données	Commentaire
ENVIRONMENT_IDENTITY_CODE	varchar(5)	Code de l'identité de l'environnement
ENVIRONMENT_IDENTITY_NAME	varchar(255)	Nom de l'identité de l'environnement
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ESEC_DISPLAY_RPT_V

Cette vue fait référence à la table ESEC_DISPLAY qui contient les propriétés affichables des objets. Elle est actuellement utilisée pour renommer les balises META et dans le cadre de la configuration des événements (en rapport avec l'entreprise).

Nom de la colonne	Type de données	Commentaire
DISPLAY_OBJECT	VARCHAR(32)	Objet parent de la propriété
TAG	VARCHAR(32)	Nom de balise natif de la propriété
LABEL	VARCHAR(32)	Chaîne d'affichage de la balise
POSITION	INT	Emplacement de la balise affichée
WIDTH	INT	Largeur de la colonne
ALIGNMENT	INT	Alignement horizontal
FORMAT	INT	Mise en forme énumérée de l'affichage de la propriété
ENABLED	BIT	Indique si la balise est affichée
TYPE	INT	Indique le type de données de la balise 1 = string 2 = ulong 3 = date 4 = uuid 5 = ipv4
DESCRIPTION	VARCHAR(255)	Texte de description de la balise
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour
REF_CONFIG	VARCHAR(4000)	Configuration des données de référence

ESEC_PORT_REFERENCE_RPT_V

Cette vue fait référence à la table ESEC_PORT_REFERENCE qui contient les numéros de port standard.

Nom de la colonne	Type de données	Commentaire
PORT_NUMBER	INT	Conformément aux informations du site http://www.iana.org/assignments/port-numbers, représentation numérique du port. Ce numéro est généralement associé au niveau Protocole de transport dans la pile TCP/IP.
PROTOCOL_NUMBER	INT	Conformément aux informations du site http://www.iana.org/assignments/protocol-numbers, identificateurs numériques utilisés pour représenter les protocoles encapsulés dans un paquet IP.
PORT_KEYWORD	VARCHAR(64)	Conformément aux informations du site http://www.iana.org/assignments/port-numbers, mot clé du port.
PORT_DESCRIPTION	VARCHAR(512)	Description du port
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	Cette vue fait référence à la table ESEC_PORT_REFERENCE qui contient les numéros de port standard.	ID de l'utilisateur à l'origine de la dernière modification

ESEC_PROTOCOL_REFERENCE_RPT_V

Cette vue fait référence à la table ESEC_PROTOCOL_REFERENCE qui contient les numéros de protocole standard.

Nom de la colonne	Type de données	Commentaire
PROTOCOL_NUMBER	INT	Conformément aux informations du site http://www.iana.org/assignments/protocol-numbers, identificateurs numériques utilisés pour représenter les protocoles encapsulés dans un paquet IP.

Nom de la colonne	Type de données	Commentaire
PROTOCOL_KEYWORD	VARCHAR(64)	Conformément aux informations du site http://www.iana.org/assignments/protocol-numbers, mot clé utilisé pour représenter les protocoles encapsulés dans un paquet IP.
PROTOCOL_DESCRIPTION	VARCHAR(512)	Description du protocole du paquet IP
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

ESEC_SEQUENCE _RPT_V

Cette vue fait référence à la table ESEC_SEQUENCE utilisée pour générer les numéros de séquence de clés primaires pour les tables Sentinel.

Nom de la colonne	Type de données	Commentaire
TABLE_NAME	VARCHAR(32)	Nom de la table
COLUMN_NAME	VARCHAR(32)	Nom de la colonne
SEED	INT	Valeur actuelle de la clé primaire
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

EVENTS_ALL_RPT_V (fournie à des fins de compatibilité descendante)

Cette vue contient les événements historiques et actuels (événements importés des archives).

Nom de la colonne	Type de données	Commentaire
EVENT_ID	uniqueidentifier	Identificateur de l'événement
RESOURCE_NAME	varchar(255)	Nom de la ressource
SUB_RESOURCE	varchar(255)	Nom de la sous-ressource
SEVERITY	int	Degré de gravité de l'événement
EVENT_PARSE_TIME	datetime	Heure de l'événement
EVENT_DATETIME	datetime	Heure de l'événement
BASE_MESSAGE	varchar(4000)	Message de base
EVENT_NAME	varchar(255)	Nom de l'événement indiqué par le capteur

Nom de la colonne	Type de données	Commentaire
EVENT_TIME	varchar(255)	Heure de l'événement indiquée par le capteur
SENSOR_NAME	varchar(255)	Nom du capteur
SENSOR_TYPE	varchar(5)	Type de capteur : H : basé sur l'hôte N : basé sur le réseau V : virus O : autre
PROTOCOL	varchar(255)	Nom du protocole
SOURCE_IP	int	Adresse IP source au format numérique
SOURCE_HOST_NAME	varchar(255)	Nom de l'hôte source
SOURCE_PORT	varchar(32)	Port source
DESTINATION_IP	int	Adresse IP de destination au format numérique
DESTINATION_HOST_NAME	varchar(255)	Nom de l'hôte de destination
DESTINATION_PORT	varchar(32)	Port de destination
SOURCE_USER_NAME	varchar(255)	Nom d'utilisateur source
DESTINATION_USER_NAME	varchar(255)	Nom d'utilisateur de destination
FILE_NAME	varchar(1000)	Nom du fichier
EXTENDED_INFO	varchar(1000)	Informations développées
REPORT_NAME	varchar(255)	Nom de programme reporteur
PRODUCT_NAME	varchar(255)	Nom du produit de rapport
CUSTOM_TAG_1	varchar(255)	Balise client 1
CUSTOM_TAG 2	varchar(255)	Balise client 2
CUSTOM_TAG 3	int	Balise client 3
RESERVED_TAG_1	VARCHAR(255)	Balise réservée 1 Réservé pour utilisation ultérieure par Sentinel. Ce champ sert à contenir les informations Advisor sur les descriptions des attaques.
RESERVED_TAG_2	varchar(255)	Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RESERVED_TAG_3	int	Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
SOURCE_UUID	uniqueidentifier	UUID source
PORT	varchar(64)	Port du collecteur
AGENT	varchar(64)	Nom du collecteur
VULNERABILITY_RATING	int	Taux de vulnérabilité
CRITICALITY_RATING	int	Taux de sévérité
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour
RV01 - 10	INT	Valeur réservée 1 - 10 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV11 - 20	DATETIME	Valeur réservée 11 - 20 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV21 - 25	uniqueidentifier	Valeur réservée 21 - 25 Réservé à une utilisation ultérieure par Sentinel pour le stockage des UUID. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV26 - 31	VARCHAR(255)	Valeur réservée 26 - 31 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV32	VARCHAR(255)	Valeur réservée 32 Réservé pour DeviceCategory. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV33	VARCHAR(255)	Valeur réservée 33 Réservé pour EventContex. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV34	VARCHAR(255)	Valeur réservée 34 Réservé pour SourceThreatLevel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelleil est destiné.
RV35	VARCHAR(255)	Valeur réservée 35 Réservé pour SourceUserContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV36	VARCHAR(255)	Valeur réservée 36 Réservé pour DataContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV37	VARCHAR(255)	Valeur réservée 37 Réservé pour SourceFunction. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV38	VARCHAR(255)	Valeur réservée 38 Réservé pour SourceOperationalContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV39	VARCHAR(255)	Valeur réservée 39 Réservé pour MSSPCustomerName. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV40 - 43	VARCHAR(255)	Valeur réservée 40 - 43 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV44	VARCHAR(255)	Valeur réservée 44 Réservé pour DestinationThreatLevel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV45	VARCHAR(255)	Valeur réservée 45 Réservé pour DestinationUserContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV46	VARCHAR(255)	Valeur réservée 46 Réservé pour VirusStatus. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV47	VARCHAR(255)	Valeur réservée 47 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV48	VARCHAR(255)	Valeur réservée 48 Réservé pour DestinationOperationalContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV49	VARCHAR(255)	Valeur réservée 49 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV50	VARCHAR(255)	Niveau de taxinomie 1
RV51	VARCHAR(255)	Niveau de taxinomie 2
RV52	VARCHAR(255)	Niveau de taxinomie 3
RV53	VARCHAR(255)	Niveau de taxinomie 4

Nom de la colonne	Type de données	Commentaire
CV01 - 10	INT	Valeur personnalisée 1 - 10 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles
CV11 - 20	DATETIME	Valeur personnalisée 11 - 20 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles
CV21 - 100	VARCHAR(255)	Valeur personnalisée 21 - 100 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles

EVENTS_ALL_RPT_V1 (fournie à des fins de compatibilité descendante)

Cette vue contient les événements actuels. Ses colonnes sont les mêmes que pour la vue EVENT_ALL_RPT_V.

EVENTS_RPT_V (fournie à des fins de compatibilité descendante)

Cette vue contient les événements historiques et actuels. Ses colonnes sont les mêmes que pour la vue EVENT_ALL_RPT_V.

EVENTS_RPT_V1 (fournie à des fins de compatibilité descendante)

Cette vue contient les événements actuels. Ses colonnes sont les mêmes que pour la vue EVENT_ALL_RPT_V.

EVENTS_RPT_V2 (fournie à des fins de compatibilité descendante)

Cette vue contient les événements historiques et actuels.

Nom de la colonne	Type de données	Commentaire
EVENT_ID	uniqueidentifier	Identificateur de l'événement
RESOURCE_NAME	varchar(255)	Nom de la ressource
SUB_RESOURCE	varchar(255)	Nom de la sous-ressource
SEVERITY	int	Degré de gravité de l'événement
EVENT_PARSE_TIME	datetime	Heure de l'événement
EVENT_DATETIME	datetime	Heure de l'événement
BASE_MESSAGE	varchar(4000)	Message de base
EVENT_NAME	varchar(255)	Nom de l'événement indiqué par le capteur

Nom de la colonne	Type de données	Commentaire
EVENT_TIME	varchar(255)	Heure de l'événement indiquée par le capteur
TAXONOMY_ID	bigint	Identificateur de taxinomie
PROTOCOL_ID	bigint	Identificateur du protocole
AGENT_ID	bigint	Identificateur du collecteur
SOURCE_IP	int	Adresse IP source au format numérique
SOURCE_HOST_NAME	varchar(255)	Nom de l'hôte source
SOURCE_PORT	varchar(32)	Port source
DESTINATION_IP	int	Adresse IP de destination au format numérique
DESTINATION_HOST_NAME	varchar(255)	Nom de l'hôte de destination
DESTINATION_PORT	varchar(32)	Port de destination
SOURCE_USER_NAME	varchar(255)	Nom d'utilisateur source
DESTINATION_USER_NAME	varchar(255)	Nom d'utilisateur de destination
FILE_NAME	varchar(1000)	Nom du fichier
EXTENDED_INFO	varchar(1000)	Informations développées
CUSTOM_TAG_1	varchar(255)	Balise client 1
CUSTOM_TAG 2	varchar(255)	Balise client 2
CUSTOM_TAG 3	int	Balise client 3
RESERVED_TAG_1	VARCHAR(255)	Balise réservée 1 Réservé pour utilisation ultérieure par Sentinel. Ce champ sert à contenir les informations Advisor sur les descriptions des attaques.
RESERVED_TAG_2	varchar(255)	Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RESERVED_TAG_3	int	Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
VULNERABILITY_RATING	int	Taux de vulnérabilité
CRITICALITY_RATING	int	Taux de sévérité
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

Nom de la colonne	Type de données	Commentaire
RV01 - 10	INT	Valeur réservée 1 - 10 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV11 - 20	DATETIME	Valeur réservée 1 - 31 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV21 - 25	uniqueidentifier	Valeur réservée 21 - 25 Réservé à une utilisation ultérieure par Sentinel pour le stockage des UUID. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV26 - 31	VARCHAR(255)	Valeur réservée 26 - 31 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV33	VARCHAR(255)	Valeur réservée 33 Réservé pour EventContex. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV34	VARCHAR(255)	Valeur réservée 34 Réservé pour SourceThreatLevel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV35	VARCHAR(255)	Valeur réservée 35 Réservé pour SourceUserContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV36	VARCHAR(255)	Valeur réservée 36 Réservé pour DataContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV37	VARCHAR(255)	Valeur réservée 37 Réservé pour SourceFunction. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV38	VARCHAR(255)	Valeur réservée 38 Réservé pour SourceOperationalContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV40 - 43	VARCHAR(255)	Valeur réservée 40 - 43 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV44	VARCHAR(255)	Valeur réservée 44 Réservé pour DestinationThreatLevel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV45	VARCHAR(255)	Valeur réservée 45 Réservé pour DestinationUserContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV46	VARCHAR(255)	Valeur réservée 46 Réservé pour VirusStatus. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV47	VARCHAR(255)	Valeur réservée 47 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
RV48	VARCHAR(255)	Valeur réservée 48 Réservé pour DestinationOperationalContext. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.

Nom de la colonne	Type de données	Commentaire
RV49	VARCHAR(255)	Valeur réservée 49 Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
REFERENCE_ID 01 - 20	BIGINT	Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
CV01 - 10	INT	Valeur personnalisée 1 - 10 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles
CV11 - 20	DATETIME	Valeur personnalisée 11 - 20 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles
CV21 - 100	VARCHAR(255)	Valeur personnalisée 21 - 100 Réservé pour utilisation par le client, généralement en rapport avec les données professionnelles

EVT_AGENT_RPT_V

Cette vue fait référence à la table EVT_AGENT contenant les informations sur les collecteurs.

Nom de la colonne	Type de données	Commentaire
AGENT_ID	bigint	Identificateur du collecteur
AGENT	varchar(64)	Nom du collecteur
PORT	varchar(64)	Port du collecteur
REPORT_NAME	varchar(255)	Nom de programme reporteur
PRODUCT_NAME	varchar(255)	Nom du produit
SENSOR_NAME	varchar(255)	Nom du capteur
SENSOR_TYPE	varchar(5)	Type de capteur : H : basé sur l'hôte N : basé sur le réseau V : virus O : autre
DEVICE_CTGRY	varchar(255)	Catégorie de périphérique
SOURCE_UUID	uniqueidentifier	UUID (Universal Unique Identifier) du composant source

Nom de la colonne	Type de données	Commentaire
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_ASSET_RPT_V

Cette vue fait référence à la table EVT_ASSET contenant les informations sur les actifs.

Nom de la colonne	Type de données	Commentaire
EVENT_ASSET_ID	bigint	Identificateur des actifs de l'événement
ASSET_NAME	varchar(255)	Nom de l'actif
PHYSICAL_ASSET_NAME	varchar(255)	Nom de l'actif physique
REFERENCE_ASSET_ID	varchar(100)	Identificateur de l'actif de référence, lien vers le système de gestion des actifs source.
MAC_ADDRESS	varchar(100)	Adresse MAC
RACK_NUMBER	varchar(50)	Numéro de rack
ROOM_NAME	varchar(100)	Nom de la salle
BUILDING_NAME	varchar(255)	Nom du bâtiment
CITY	varchar(100)	Ville
STATE	varchar(100)	État
COUNTRY	varchar(100)	Pays
ZIP_CODE	varchar(50)	Code postal
ASSET_CATEGORY_NAME	varchar(100)	Nom de la catégorie d'actifs
NETWORK_IDENTITY_NAME	varchar(255)	Nom de l'identité du réseau des actifs
ENVIRONMENT_IDENTITY_NAME	varchar(255)	Nom de l'environnement
ASSET_VALUE_NAME	varchar(50)	Nom de la valeur de l'actif
CRITICALITY_NAME	varchar(50)	Nom relatif à la sévérité de l'actif
SENSITIVITY_NAME	varchar(50)	Nom relatif à la sensibilité de l'actif
CONTACT_NAME_1	varchar(255)	Nom du contact/organisation 1
CONTACT_NAME_2	varchar(255)	Nom du contact/organisation 2
ORGANIZATION_NAME_1	varchar(100)	Niveau d'organisation du propriétaire de l'actif 1
ORGANIZATION_NAME_2	varchar(100)	Niveau d'organisation du propriétaire de l'actif 2
ORGANIZATION_NAME_3	varchar(100)	Niveau d'organisation du propriétaire de l'actif 3
ORGANIZATION_NAME_4	varchar(100)	Niveau d'organisation du propriétaire de l'actif 4
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour

Nom de la colonne	Type de données	Commentaire
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_DEST_EVT_NAME_SMRY_1_RPT_V

Cette vue récapitule les événements par destination, taxinomie, nom, gravité et heure.

Nom de la colonne	Type de données	Commentaire
DESTINATION_IP	int	Adresse IP cible
DESTINATION_EVENT_ASSET_ID	bigint	Identificateur des actifs de l'événement
TAXONOMY_ID	bigint	Identificateur de taxinomie
EVENT_NAME_ID	bigint	Identificateur du nom de l'événement
SEVERITY	int	Degré de gravité de l'événement
CUSTOMER_ID	bigint	Identificateur du client
EVT_TIME	datetime	Heure de l'événement
EVT_COUNT	int	Nombre d'événements
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_DEST_SMRY_1_RPT_V

Cette vue contient les informations récapitulatives sur la destination des événements.

Nom de la colonne	Type de données	Commentaire
DESTINATION_IP	int	Adresse IP cible
DESTINATION_EVENT_ASSET_ID	bigint	Identificateur des actifs de l'événement
DESTINATION_PORT	varchar(32)	Port de destination
DESTINATION_USR_ID	bigint	Identificateur de l'utilisateur de destination
TAXONOMY_ID	bigint	Identificateur de taxinomie
EVENT_NAME_ID	bigint	Identificateur du nom de l'événement
RESOURCE_ID	bigint	Identificateur de la ressource
AGENT_ID	bigint	Identificateur du collecteur
PROTOCOL_ID	bigint	Identificateur du protocole
SEVERITY	int	Degré de gravité de l'événement
CUSTOMER_ID	bigint	Identificateur du client
EVENT_TIME	datetime	Heure de l'événement
EVENT_COUNT	int	Nombre d'événements
DATE_CREATED	datetime	Date d'insertion

Nom de la colonne	Type de données	Commentaire
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_DEST_TXNMY_SMRY_1_RPT_V

Cette vue récapitule les événements par destination, taxinomie, gravité et heure.

Nom de la colonne	Type de données	Commentaire
DESTINATION_IP	int	Adresse IP cible
DESTINATION_EVENT_ASSET_ID	bigint	Identificateur des actifs de l'événement
TAXONOMY_ID	bigint	Identificateur de taxinomie
SEVERITY	int	Degré de gravité de l'événement
CUSTOMER_ID	bigint	Identificateur du client
EVENT_TIME	datetime	Heure de l'événement
EVENT_COUNT	int	Nombre d'événements
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_NAME_RPT_V

Cette vue fait référence à la table EVT_NAME contenant les informations de nom des événements.

Nom de la colonne	Type de données	Commentaire
EVENT_NAME_ID	bigint	Identificateur du nom de l'événement
EVENT_NAME	varchar(255)	Nom de l'événement
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_PORT_SMRY_1_RPT_V

Cette vue récapitule les événements par port de destination, gravité et heure.

Nom de la colonne	Type de données	Commentaire
DESTINATION_PORT	Varchar(32)	Port de destination
SEVERITY	int	Degré de gravité de l'événement
CUSTOMER_ID	bigint	Identificateur du client

Nom de la colonne	Type de données	Commentaire
EVENT_TIME	datetime	Heure de l'événement
EVENT_COUNT	int	Nombre d'événements
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_PRTCL_RPT_V

Cette vue fait référence à la table EVT_PRTCL contenant les informations sur les protocoles des événements.

Nom de la colonne	Type de données	Commentaire
PROTOCOL_ID	bigint	Identificateur du protocole
PROTOCOL_NAME	varchar(255)	Nom du protocole
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_RSRC_RPT_V

Cette vue fait référence à la table EVT_RSRC contenant les informations sur les ressources des événements.

Nom de la colonne	Type de données	Commentaire
RESOURCE_ID	bigint	Identificateur de la ressource
RESOURCE_NAME	varchar(255)	Nom de la ressource
SUB_RESOURCE_NAME	varchar(255)	Nom de la sous-ressource
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_SEV_SMRY_1_RPT_V

Cette vue récapitule les événements par gravité et heure.

Nom de la colonne	Type de données	Commentaire
SEVERITY	int	Degré de gravité de l'événement
CUSTOMER_ID	bigint	Identificateur du client
EVENT_TIME	datetime	Heure de l'événement
EVENT_COUNT	int	Nombre d'événements
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour

Nom de la colonne	Type de données	Commentaire
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_SRC_SMRY_1_RPT_V

Cette vue contient les informations récapitulatives sur la destination et la source des événements.

Nom de la colonne	Type de données	Commentaire
SOURCE_IP	int	Adresse IP source
SOURCE_EVENT_ASSET_ID	bigint	Identificateur des actifs de l'événement
SOURCE_PORT	varchar(32)	Port source
SOURCE_USER_ID	bigint	Identificateur de l'utilisateur
TAXONOMY_ID	bigint	Identificateur de taxinomie
EVENT_NAME_ID	bigint	Identificateur du nom de l'événement
RESOURCE_ID	bigint	Identificateur de la ressource
AGENT_ID	bigint	Identificateur du collecteur
PROTOCOL_ID	bigint	Identificateur du protocole
SEVERITY	int	Degré de gravité de l'événement
CUSTOMER_ID	bigint	Identificateur du client
EVENT_TIME	datetime	Heure de l'événement
EVENT_COUNT	int	Nombre d'événements
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

EVT_TXNMY_RPT_V

Cette vue fait référence à la table EVT_TXNMY contenant les informations de taxinomie des événements.

Nom de la colonne	Type de données	Commentaire
TAXONOMY_ID	bigint	Identificateur de taxinomie
TAXONOMY _ LEVEL _1	varchar(100)	Niveau de taxinomie 1
TAXONOMY _ LEVEL _2	varchar(100)	Niveau de taxinomie 2
TAXONOMY _ LEVEL _3	varchar(100)	Niveau de taxinomie 3
TAXONOMY _ LEVEL _4	varchar(100)	Niveau de taxinomie 4
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion

Nom de la colonne	Type de données	Commentaire
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour
TAXONOMY_ID	bigint	Identificateur de taxinomie

EVT_USR_RPT_V

Cette vue fait référence à la table EVT_USR contenant les informations sur les utilisateurs des événements.

Nom de la colonne	Type de données	Commentaire
USER_ID	bigint	Identificateur de l'utilisateur
USER_NAME	varchar(255)	Nom de l'utilisateur
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour
USER_ID	bigint	Identificateur de l'utilisateur

EXTERNAL_DATA_RPT_V

Cette vue fait référence à la table EXTERNAL_DATA contenant les données externes.

Nom de la colonne	Type de données	Commentaire
EXTERNAL_DATA_ID	int	Identificateur des données externes
SOURCE_NAME	varchar(50)	Nom de la source
SOURCE_DATA_ID	varchar(255)	Identificateur des données sources
EXTERNAL_DATA	text	Données externes
EXTERNAL_DATA_TYPE	varchar(10)	Type de données externes
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

HIST_EVENTS_RPT_V

Cette vue contient les événements historiques (événements restaurés des archives).

HIST_INCIDENTS_RPT_V

Cette vue contient les incidents (incidents restaurés des archives).

IMAGES_RPT_V

Cette vue fait référence à la table IMAGES contenant les informations sur les images du système.

Nom de la colonne	Type de données	Commentaire
NAME	VARCHAR(128)	Nom de l'image

Nom de la colonne	Type de données	Commentaire
TYPE	VARCHAR(64)	Type d'image
DATA	TEXT	Données de l'image
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

INCIDENTS_ASSETS_RPT_V

Cette vue fait référence à la table INCIDENTS_ASSETS contenant les informations sur les actifs concernés par les incidents créés dans la console Sentinel.

Nom de la colonne	Type de données	Commentaire
INC_ID	INT	Identificateur de l'incident - numéro de séquence
ASSET_ID	uniqueidentifier	UUID (Universal Unique Identifier) de l'actif
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

INCIDENTS_EVENTS_RPT_V

Cette vue fait référence à la table INCIDENTS_EVENTS contenant les informations sur les événements des incidents créés dans la console Sentinel.

Nom de la colonne	Type de données	Commentaire
INC_ID	INT	Identificateur de l'incident - numéro de séquence
EVT_ID	uniqueidentifier	UUID (Universal Unique Identifier) de l'événement
EVT_TIME	DATETIME	Heure de l'événement
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

INCIDENTS_RPT_V

Cette vue fait référence à la table INCIDENTS contenant les informations détaillées sur les incidents créés dans la console Sentinel.

Nom de la colonne	Type de données	Commentaire
INC_ID	INT	Identificateur de l'incident - numéro de séquence
NAME	VARCHAR(255)	Nom de l'incident
SEVERITY	INT	Degré de gravité de l'incident
STT_ID	INT	ID de l'état de l'incident
SEVERITY_RATING	VARCHAR(32)	Moyenne de tous les degrés de gravité des événements liés à un incident
VULNERABILITY_RATING	VARCHAR(32)	Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
CRITICALITY_RATING	VARCHAR(32)	Réservé pour utilisation ultérieure par Sentinel. Si vous utilisez ce champ pour d'autres fins, vous risquez de perdre les informations qu'il contient lors de l'utilisation de la fonctionnalité à laquelle il est destiné.
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour
INC_DESC	varchar(4000)	Description de l'incident
INC_PRIORITY	int	Priorité de l'incident
INC_CAT	varchar(255)	Catégorie de l'incident
INC_RES	varchar(4000)	Résolution de l'incident

INCIDENTS_VULN_RPT_V

Cette vue fait référence à la table INCIDENTS_VULN contenant les informations sur la vulnérabilité des incidents créés dans la console Sentinel.

Nom de la colonne	Type de données	Commentaire
INC_ID	INT	Identificateur de l'incident - numéro de séquence
VULN_ID	uniqueidentifier	UUID (Universal Unique Identifier) de la vulnérabilité
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

L_STAT_RPT_V

Cette vue fait référence à la table L_STAT contenant les statistiques.

Nom de la colonne	Type de données	Commentaire
RES_NAME	VARCHAR(32)	Nom de la ressource
STATS_NAME	VARCHAR(32)	Nom de la statistique
STATS_VALUE	VARCHAR(32)	Valeur de la statistique
OPEN_TOT_SECS	NUMBER	Nombre de secondes depuis 1970.

LOGS_RPT_V

Cette vue fait référence à la table LOGS_RPT contenant les informations de consignation.

Table LOGS		
Nom de la colonne	**Type de données**	**Commentaire**
LOG_ID	NUMBER	Numéro de séquence
TIME	DATE	Date du journal
MODULE	VARCHAR(64)	Module auquel est destiné le fichier journal
TEXT	VARCHAR(4000)	Texte du journal

NETWORK_IDENTITY_RPT_V

Cette vue fait référence à la table NETWORK_IDENTITY_LKUP contenant les informations sur l'identité de réseau des actifs.

Nom de la colonne	Type de données	Commentaire
NETWORK_IDENTITY_CD	varchar(5)	Code d'identité du réseau
NETWORK_IDENTITY_NAME	varchar(255)	Nom de l'identité du réseau
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ORGANIZATION_RPT_V

Cette vue fait référence à la table ORGANIZATION contenant les informations sur les organisations (actifs).

Nom de la colonne	Type de données	Commentaire
ORGANIZATION_ID	uniqueidentifier	Identificateur de l'organisation
ORGANIZATION_NAME	varchar(100)	Nom de l'organisation
CUSTOMER_ID	bigint	Identificateur du client
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la

Nom de la colonne	Type de données	Commentaire
		dernière mise à jour

PERSON_RPT_V

Cette vue fait référence à la table PERSION contenant les informations sur les personnes (actifs).

Nom de la colonne	Type de données	Commentaire
PERSON_ID	uniqueidentifier	Identificateur de la personne
FIRST_NAME	varchar(255)	Prénom
LAST_NAME	varchar(255)	Nom
CUSTOMER_ID	bigint	Identificateur du client
PHONE_NUMBER	varchar(50)	Numéro de téléphone
EMAIL_ADDRESS	varchar(255)	Adresse électronique
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

PHYSICAL_ASSET_RPT_V

Cette vue fait référence à la table PHYSICAL_ASSET contenant les informations sur les actifs physiques.

Nom de la colonne	Type de données	Commentaire
PHYSICAL_ASSET_ID	uniqueidentifier	Identificateur de l'actif physique
CUSTOMER_ID	int	Identificateur du client
LOCATION_ID	bigint	Identificateur de l'emplacement
HOST_NAME	varchar(255)	Nom de l'hôte
IP_ADDRESS	int	Adresse IP
NETWORK_IDENTITY_CD	varchar(5)	Code d'identité du réseau
MAC_ADDRESS	varchar(100)	Adresse MAC
RACK_NUMBER	varchar(50)	Numéro de rack
ROOM_NAME	varchar(100)	Nom de la salle
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

○PRODUCT_RPT_V

Cette vue fait référence à la table PRDT contenant les informations produit des actifs.

Nom de la colonne	Type de données	Commentaire
PRODUCT _ID	bigint	Identificateur du produit
PRODUCT _NAME	varchar(255)	Nom du produit

Nom de la colonne	Type de données	Commentaire
PRODUCT _VERSION	varchar(100)	Version du produit
VENDOR _ID	bigint	Identificateur du fournisseur
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

ROLE_RPT_V

Cette vue fait référence à la table ROLE_LKUP contenant les informations sur les rôles des utilisateurs (actifs).

Nom de la colonne	Type de données	Commentaire
ROLE_CODE	varchar(5)	Code du rôle
ROLE_NAME	varchar(255)	Nom du rôle
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

SENSITIVITY_RPT_V

Cette vue fait référence à la table SENSITIVITY_LKUP contenant les informations de sensibilité des actifs.

Nom de la colonne	Type de données	Commentaire
SENSITIVITY_CODE	varchar(5)	Code de sensibilité de l'actif
SENSITIVITY_NAME	varchar(50)	Nom relatif à la sensibilité de l'actif
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID utilisateur
MODIFIED_BY	int	ID utilisateur

STATES_RPT_V

Cette vue fait référence à la table STATES qui contient les définitions des états définis par les applications ou le contexte.

Nom de la colonne	Type de données	Commentaire
STT_ID	INT	ID de l'état - numéro de séquence
CONTEXT	VARCHAR(64)	Contexte de l'état, à savoir cas, incident, utilisateur
NAME	VARCHAR(64)	Nom de l'état
TERMINAL_FLAG	VARCHAR(1)	Indique si l'état de l'incident est résolu
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour

Nom de la colonne	Type de données	Commentaire
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
CREATED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour

Vue UNASSIGNED_INCIDENTS_RPT_V

Cette vue fait référence aux tables CASES et INCIDENTS qui rapportent les cas non attribués.

Nom	Type de données
INC_ID	INT
NAME	VARCHAR(255)
SEVERITY	INT
STT_ID	INT
SEVERITY_RATING	VARCHAR(32)
VULNERABILITY_RATING	VARCHAR(32)
CRITICALITY_RATING	VARCHAR(32)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT
INC_DESC	VARCHAR(4000)
INC_PRIORITY	INT
INC_CAT	VARCHAR(255)
INC_RES	VARCHAR(4000)

USERS_RPT_V

Cette vue fait référence à la table USERS qui répertorie l'ensemble des utilisateurs de l'application. Des utilisateurs de base de données seront également créés pour permettre l'utilisation d'outils de rapports tiers.

Nom de la colonne	Type de données	Commentaire
USR_ID	INT	Identificateur de l'utilisateur - numéro de séquence
NAME	VARCHAR(64)	Nom d'utilisateur court et unique utilisé pour la connexion
CNT_ID	INT	ID du contact - numéro de séquence
STT_ID	INT	ID de l'état. Le statut est actif ou inactif.
DESCRIPTION	VARCHAR(512)	Commentaires
DATE_CREATED	DATETIME	Date d'insertion
DATE_MODIFIED	DATETIME	Date de la dernière mise à jour
CREATED_BY	INT	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	INT	ID de l'utilisateur à l'origine de la dernière mise à jour
PERMISSIONS	VARCHAR(4000)	Autorisations actuellement attribuées à l'utilisateur Sentinel

Nom de la colonne	Type de données	Commentaire
FILTER	VARCHAR(128)	Filtre de sécurité actuellement attribué à l'utilisateur Sentinel
UPPER_NAME	VARCHAR(64)	Nom d'utilisateur en majuscules
DOMAIN_AUTH_IND	Bit	Indication de l'authentification de domaine

VENDOR_RPT_V

Cette vue fait référence à la table VNDR contenant les informations relatives aux fournisseurs de produits associés aux actifs.

Nom de la colonne	Type de données	Commentaire
VENDOR_ID	bigint	Identificateur du fournisseur
VENDOR_NAME	varchar(255)	Nom du fournisseur
DATE_CREATED	datetime	Date d'insertion
DATE_MODIFIED	datetime	Date de la dernière mise à jour
CREATED_BY	int	ID de l'utilisateur à l'origine de l'insertion
MODIFIED_BY	int	ID de l'utilisateur à l'origine de la dernière mise à jour

VULN_CALC_SEVERITY_RPT_V

Cette vue fait référence aux tables VULN_RSRC et VULN pour le calcul du taux de gravité de la vulnérabilité d'eSecurity en fonction des vulnérabilités actuelles.

Nom de la colonne	Type de données
RSRC_ID	uniqueidentifier
IP	VARCHAR(32)
HOST_NAME	VARCHAR(255)
CRITICALITY	int
ASSIGNED_VULN_SEVERITY	int
VULN_COUNT	Nombre de vulnérabilités pour la ressource spécifiée
CALC_SEVERITY	Gravité calculée en fonction des valeurs ASSIGNED_VULN_SEVERITY et CRITICALITY

VULN_CODE_RPT_V

Cette vue fait référence à la table VULN_CODE contenant les codes de vulnérabilité standard tels que les CAN et les CVE de Mitre.

Nom de la colonne	Type de données
VULN_CODE_ID	VARCHAR(36)
VULN_ID	VARCHAR(36)
VULN_CODE_TYPE	VARCHAR(64)
VULN_CODE_VALUE	VARCHAR(255)
URL	VARCHAR(512)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME

Nom de la colonne	Type de données
CREATED_BY	INT
MODIFIED_BY	INT

VULN_INFO_RPT_V

Cette vue fait référence à la table VULN_INFO contenant les informations supplémentaires rapportées au cours d'une analyse.

Nom de la colonne	Type de données
VULN_INFO_ID	VARCHAR(36)
VULN_ID	VARCHAR(36)
VULN_INFO_TYPE	VARCHAR(36)
VULN_INFO_VALUE	VARCHAR(2000)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_RPT_V

Cette vue fait référence à la table VULN contenant les informations relatives au système analysé. Chaque scanner dispose de sa propre entrée pour chacun des systèmes.

Nom de la colonne	Type de données
VULN_ID	VARCHAR(36)
RSRC_ID	VARCHAR(36)
PORT_NAME	VARCHAR(64)
PORT_NUMBER	INT
NETWORK_PROTOCOL	INT
APPLICATION_PROTOCOL	VARCHAR(64)
ASSIGNED_VULN_SEVERITY	INT
COMPUTED_VULN_SEVERITY	INT
VULN_DESCRIPTION	CLOB
VULN_SOLUTION	CLOB
VULN_SUMMARY	VARCHAR(1000)
BEGIN_EFFECTIVE_DATE	DATETIME
END_EFFECTIVE_DATE	DATETIME
DETECTED_OS	VARCHAR(64)
DETECTED_OS_VERSION	VARCHAR(64)
SCANNED_APP	VARCHAR(64)
SCANNED_APP_VERSION	VARCHAR(64)
VULN_USER_NAME	VARCHAR(64)
VULN_USER_DOMAIN	VARCHAR(64)
VULN_TAXONOMY	VARCHAR(1000)
SCANNER_CLASSIFICATION	VARCHAR(255)
VULN_NAME	VARCHAR(300)
VULN_MODULE	VARCHAR(64)

Nom de la colonne	Type de données
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_RSRC_RPT_V

Cette vue fait référence à la table VULN_RSRC contenant toutes les ressources analysées au cours d'une analyse donnée.

Nom de la colonne	Type de données
RSRC_ID	VARCHAR(36)
SCANNER_ID	VARCHAR(36)
IP	VARCHAR(32)
HOST_NAME	VARCHAR(255)
LOCATION	VARCHAR(128)
DEPARTMENT	VARCHAR(128)
BUSINESS_SYSTEM	VARCHAR(128)
OPERATIONAL_ENVIRONMENT	VARCHAR(64)
CRITICALITY	INT
REGULATION	VARCHAR(128)
REGULATION_RATING	VARCHAR(64)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_RSRC_SCAN_RPT_V

Cette vue fait référence à la table VULN_RSRC_SCAN contenant toutes les ressources analysées au cours d'une analyse donnée.

Nom de la colonne	Type de données
RSRC_ID	VARCHAR(36)
SCAN_ID	VARCHAR(36)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_SCAN_RPT_V

Cette vue fait référence à la table qui contient les informations relatives aux analyses.

Nom de la colonne	Type de données
SCAN_ID	VARCHAR(36)
SCANNER_ID	VARCHAR(36)
SCAN_TYPE	VARCHAR(10)
SCAN_START_DATE	DATETIME
SCAN_END_DATE	DATETIME

Nom de la colonne	Type de données
CONSOLIDATION_SERVER	VARCHAR(64)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_SCAN_VULN_RPT_V

Cette vue fait référence à la table VULN_SCAN_VULN contenant les vulnérabilités détectées au cours des analyses.

Nom de la colonne	Type de données
SCAN_ID	VARCHAR(36)
VULN_ID	VARCHAR(36)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

VULN_SCANNER_RPT_V

Cette vue fait référence à la table VULN_SCANNER contenant les informations relatives aux scanners recherchant les vulnérabilités.

Nom de la colonne	Type de données
SCANNER_ID	VARCHAR(36)
PRODUCT_NAME	VARCHAR(100)
PRODUCT_VERSION	VARCHAR(64)
SCANNER_TYPE	VARCHAR(64)
VENDOR	VARCHAR(100)
SCANNER_INSTANCE	VARCHAR(64)
DATE_CREATED	DATETIME
DATE_MODIFIED	DATETIME
CREATED_BY	INT
MODIFIED_BY	INT

A Liste de contrôle pour dépannage de Sentinel

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

Cette liste vous permet de déterminer le type de problème auquel vous êtes confronté. En la complétant, vous gagnerez du temps pour résoudre les problèmes les plus courants. Dans le cas de problèmes plus complexes, le fait d'avoir déjà rassemblé ces informations évite de procéder à un deuxième diagnostic.

Point de contrôle	**Informations**	**Exemple**
Version de Novell :		Version 5.1.3
Système d'exploitation et plate-forme du produit Novell :		Windows 2003 Server Service Pack 1
Système d'exploitation et plate-forme de la base de données :		Microsoft SQL Server 2000 Service Pack 3a
Configuration matérielle du serveur Sentinel Processeur Mémoire Autre		5 Go de mémoire vive (RAM) 4 unités centrales 3,0 GHz
Configuration matérielle du serveur de la base de données Processeur Mémoire Autre (en cas de matériel distinct)		8 Go de mémoire vive (RAM) 4 unités centrales 3,0 GHz
Configuration de stockage de la base de données (stockage en réseau, SAN, stockage local, etc.)		Stockage local avec sauvegarde externe
Système d'exploitation et configuration du serveur de création de rapports (Crystal Server)		Crystal Reports XI Windows 2003 Server Service Pack 1 Authentification Windows

REMARQUE : en fonction de la configuration (ou de la distribution) de votre système Sentinel, il se peut que vous ayez besoin d'ajouter des entrées au tableau ci-dessus. Par exemple, vous devrez peut-être fournir des informations supplémentaires pour le service DAS, Advisor, le Centre de contrôle Sentinel, le Générateur de collecteurs et la couche communication.

1. Recherchez le problème qui vous concerne sur le portail d'assistance aux utilisateurs :
   - S'agit-il d'un problème connu avec une solution palliative ?
   - S'agit-il d'un problème corrigé dans le dernier correctif ou hotfix ?
   - S'agit-il d'un problème qu'il est prévu de corriger dans une prochaine version ?
2. Déterminez la nature du problème.
   - Peut-il être reproduit ? Quelles sont les différentes étapes ayant abouti à ce problème ?
   - Quelle action pourrait être à l'origine du problème ?
   - S'agit-il d'un problème périodique ?
3. Déterminez la gravité du problème.
   - Le système fonctionne-t-il toujours ?
4. Précisez l'environnement et les systèmes concernés.
   - Quelles sont les versions du produit et des plates-formes concernées ?
   - Le problème concerne-t-il également des composants non standard ou personnalisés ?
   - S'agit-il d'un environnement à taux élevé d'événements ?
   - À quelle fréquence les événements sont-ils collectés ?
   - Quelle est la fréquence d'insertion des événements dans la base de données ?
   - Combien de personnes utilisent le système simultanément ?
   - Le serveur de création de rapports Crystal est-il utilisé ? Quand les rapports sont-ils exécutés ?
   - Faites-vous appel à la corrélation ? Combien de règles sont déployées ?

   Rassemblez les fichiers de configuration, les fichiers journaux et les informations système en vue d'une éventuelle communication. Pour connaître l'emplacement des fichiers journaux, consultez le chapitre 2 du guide d'installation de Sentinel qui répertorie les pratiques recommandées.
5. Vérifiez l'état de fonctionnement de votre système.
   - Parvenez-vous à vous connecter à la console Sentinel ?
   - Les événements sont-ils générés, puis insérés dans la base de données ? (Si elle est toujours configurée, exécutez la commande SendOneEvent et recherchez les événements.)
   - Parvenez-vous à afficher les événements sur la console Sentinel ?
   - Les événements peuvent-ils être extraits de la base de données à l'aide d'une requête rapide ?
   - Vérifiez la quantité de mémoire vive utilisée, l'espace disque, l'activité des processus, l'utilisation de l'unité centrale et la connexion réseau des hôtes concernés.
   - Vérifiez que tous les processus Sentinel nécessaires sont en cours d'exécution. Des scripts tels que hp_checkprocess sur Solaris peuvent supprimer de la liste nos processus et leur statut. Dans un environnement Windows, vous pouvez utiliser le gestionnaire des tâches Microsoft.
   - Vérifiez si des fichiers de vidage figurent dans les sous-répertoires ESEC_HOME. Si tel est le cas, indiquez de quelle mémoire il s'agit. (cd $ESEC_HOME, par exemple. –name core -print)

- Vérifiez l'accès Internet de sqlplus net. Vérifiez l'espace des tables.
- Assurez-vous que le courtier Sonic est en cours d'exécution. La connexion peut être vérifiée à l'aide de la console de gestion Sonic. Assurez-vous que les différentes connexions sont actives au niveau des processus Novell. Assurez-vous qu'aucun fichier de verrouillage n'empêche Sonic de se lancer. Vous pouvez éventuellement lancer la commande telnet vers ce serveur sur le port Sonic (par exemple, telnet sentinel.company.com 10012).
- Vérifiez si Watchdog s'exécute sur le serveur (ps –ef | grep watchdog).
- Vérifiez si les processus Wizard fonctionnent. Le Gestionnaire des collecteurs est-il en cours d'exécution ? Le Gestionnaire des collecteurs est-il signalé comme actif dans le Générateur de collecteurs ou dans la console Sentinel ? Les collecteurs s'exécutent-t-ils ? Combien d'entre eux sont exécutés sur chaque ordinateur ? Quels sont les connecteurs utilisés (fichier, processus, syslog, pare-feu, journal des événements, etc.) ? Dans quelles proportions utilisent-ils les ressources système ?

6. Avez-vous noté un problème avec la base de données ?
   - Parvenez-vous à vous connecter à la base de données à l'aide de sqlplus ?
   - La base de données permet-elle un login sqlplus dans dans le schéma ESEC à l'aide du compte Novell dba ?

     Parvenez-vous à effectuer une requête sur l'une des tables ?
   - Parvenez-vous à lancer une instruction select sur l'une des tables de la base de données ?
   - Vérifiez les pilotes JDBC, leur emplacement ainsi que leurs paramètres de chemin d'accès aux classes.
   - Si vous utilisez Oracle, vos pilotes sont-ils dotés de la fonction de partitionnement (entrez « select * from v$version; »). Le cas échéant, l'utilisent-ils ?
   - Un administrateur assure-t-il la maintenance de la base de données ? Si tel n'est pas le cas, quelqu'un d'autre s'en charge-t-il ?
   - L'administrateur a-t-il modifié la base de données ?
   - Le Gestionnaire de données Sentinel (SDM) est-il utilisé pour la maintenance du partitionnement et pour archiver/supprimer les partitions en vue de libérer de l'espace dans la base de données ?
   - À l'aide de SDM, identifiez la partition active ? Est-ce PMAX?
7. Vérifiez si les paramètres d'environnement du produit sont corrects.
   - Vérifiez les scripts de shell de login utilisateur, les variables d'environnement, les configurations et les paramètres java home.
   - Les variables d'environnement sont-elle définies pour exécuter la bonne JVM ?
   - Vérifiez que les autorisations adéquates sont associées aux dossiers du produit installé.
   - Vérifiez si des travaux cron génèrent des interférences avec les fonctionnalités de notre produit.
   - Si le produit est installé sur des points de montage NFS, assurez-vous du bon fonctionnement des points de montage NFS et des services NFS/NIS.

8. Peut-il y avoir des fuites de mémoire ?
   - Recherchez les statistiques d'utilisation de la mémoire, ainsi que les processus qui l'utilise.
   - Rassemblez les valeurs de débit d'événements par collecteur.
   - Exécutez la commande prstat sur Solaris. Vous obtiendrez les statistiques relatives à l'exécution des processus.
   - Dans Windows, vous pouvez vérifier la taille des processus et le nombre de handles dans le gestionnaire des tâches.

   Si le problème persiste, vous pouvez à présent le faire remonter. Il pourra alors vous être proposé :
   - des améliorations ;
   - des correctifs ;
   - une solution palliative.

B Configuration du compte de connexion du service Sentinel en tant que service réseau NT AUTHORITY\ NetworkService

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

L'objectif du présent document est de fournir une description détaillée de la procédure à suivre pour configurer le compte de connexion du service Sentinel en tant que service réseau NT AUTHORITY\NetworkService et non en tant que compte d'utilisateur du domaine. Cette configuration ne s'est révélée opérationnelle que sous Windows 2003.

Un service doit se connecter à un compte pour accéder aux ressources et aux objets du système d'exploitation. Si vous sélectionnez un compte qui n'est pas autorisé à se connecter en tant que service, le snap-in des services accorde automatiquement à ce compte les droits d'utilisateur requis pour se connecter en tant que service sur l'ordinateur que vous administrez. Néanmoins, cette procédure ne garantit pas que le service pourra démarrer correctement. Il est fortement recommandé de sélectionner la case à cocher **Password never expires** (**Le mot de passe n'expire jamais**) dans les propriétés des comptes d'utilisateur servant à la connexion en tant que service et de définir des mots de passe sécurisés pour ces comptes. Si la stratégie de verrouillage du compte est activée et que le compte est verrouillé, le service ne pourra pas fonctionner correctement.

Le tableau ci-dessous donne une description des différents comptes de connexion du service et de la façon dont ils doivent être utilisés.

Compte de connexion	Description
Compte système local (Local System)	Le compte système local (Local System) est très intéressant car il dispose d'autorisations d'accès à tout le système, y compris au service d'annuaire des contrôleurs de domaine. Si un service se connecte au compte système local sur un contrôleur de domaine, il a accès à l'intégralité du domaine. Par défaut, certains services se connectent au compte système local. Ne modifiez pas cette configuration par défaut. Le compte système local est un compte local prédéfini utilisé pour démarrer un service et pour lui fournir des éléments de sécurité. Le nom de ce compte est NT AUTHORITY\System. Aucun mot de passe n'est défini pour ce compte. Si un mot de passe est entré, il l'ignore. Le compte système local est un compte disposant d'autorisations d'accès à tout le système, y compris au service d'annuaire des contrôleurs de domaine. Étant donné qu'il se comporte de la même façon qu'un ordinateur sur le réseau, il peut accéder aux ressources réseau.

Compte de connexion	Description
Compte de service local (Local Service)	Le compte de service local (Local Service) est un compte intégré particulier, semblable à un compte d'utilisateur authentifié. Il dispose des mêmes autorisations d'accès aux ressources et aux objets que les membres du groupe Users (utilisateurs). Ce niveau d'accès, limité, permet de protéger le système en cas de violation de certains services ou processus. Les services s'exécutant sur ce compte accèdent aux ressources réseau en tant que session nulle, sans références d'utilisateur. Le compte de service local est un compte local prédéfini utilisé pour démarrer un service et pour lui fournir des éléments de sécurité. Le nom de ce compte est NT AUTHORITY\LocalService. Il dispose d'autorisations d'accès limitées à l'ordinateur local ainsi que d'autorisations d'accès anonyme aux ressources réseau.
Compte de service réseau (Network Service)	Le compte de service réseau (Network Service) est un compte intégré particulier, semblable à un compte d'utilisateur authentifié. Il dispose des mêmes autorisations d'accès aux ressources et aux objets que les membres du groupe Users (utilisateurs). Ce niveau d'accès, limité, permet de protéger le système en cas de violation de certains services ou processus. Les services s'exécutant sur ce compte accèdent aux ressources réseau à l'aide des références du compte de l'ordinateur. Le compte de service réseau est un compte local prédéfini utilisé pour démarrer un service et pour lui fournir des éléments de sécurité. Le nom de ce compte est NT AUTHORITY\\NetworkService. Il dispose d'autorisations d'accès limitées à l'ordinateur local ainsi que d'autorisations d'accès authentifié (en tant que compte de l'ordinateur) aux ressources réseau.

L'exécution d'un service dans le cadre d'un compte de connexion d'utilisateur présente plusieurs inconvénients :

1. Le compte doit être créé avant d'exécuter le service. Si le programme d'installation du service crée le compte, il doit être exécuté sur un compte disposant des droits d'administration nécessaires à la création de comptes dans le service d'annuaire.
2. Les noms et mots de passe du compte de service sont stockés sur chaque ordinateur où le service est installé. Si le mot de passe défini pour un compte de service sur un ordinateur donné est modifié ou n'est plus valable, le service ne démarre pas sur cet ordinateur tant que le mot de passe du service n'est pas redéfini en fonction. Il est recommandé d'utiliser le service local ou le service réseau à la place d'un compte qui requiert un mot de passe : la gestion des mots de passe s'en trouve simplifiée.
3. Si un compte de service est renommé, verrouillé, désactivé ou supprimé, le service ne démarre pas sur l'ordinateur concerné tant que le compte n'est pas défini correctement.

En raison de ces inconvénients, Novell a testé l'exécution du service Sentinel sous le compte NT AUTHORITY\NetworkService. En effet, le compte NT AUTHORITY\LocalService ne dispose pas des privilèges requis puisque les processus DAS (Data Access Service) doivent être en mesure de communiquer avec le serveur de base de données sur le réseau.

Pour configurer NT AUTHORITY\NetworkService en tant que compte de connexion du service Sentinel

Pour configurer NT AUTHORITY\NetworkService en tant que compte de connexion du service Sentinel, procédez comme suit :

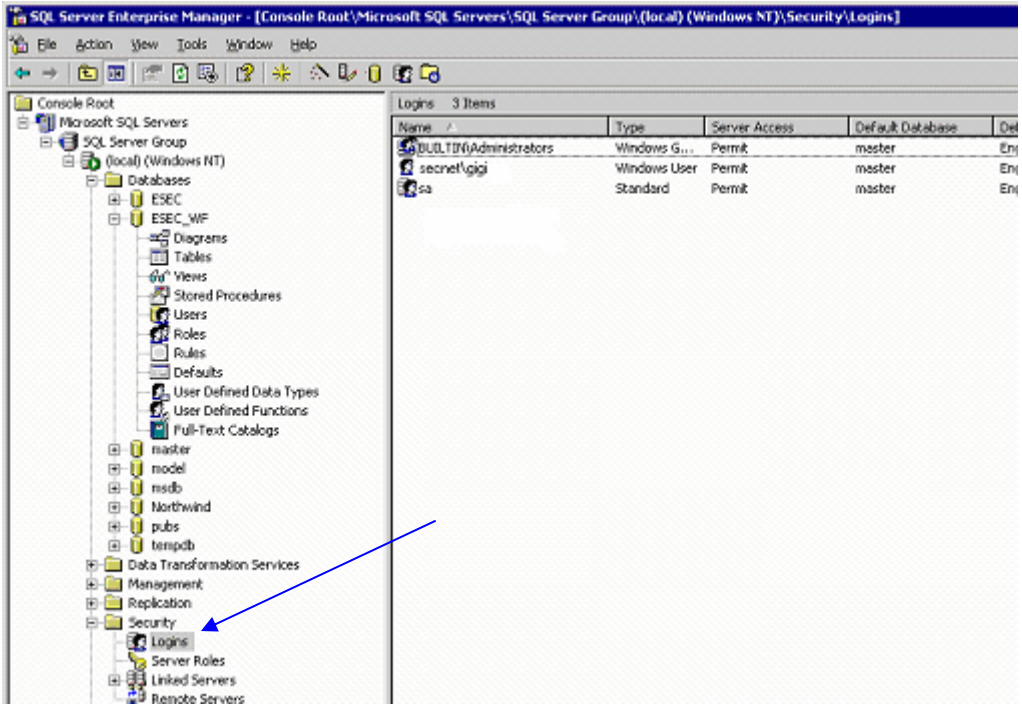
- Ajoutez la machine qui exécute le service Sentinel en tant que compte de connexion dans les instances de base de données ESEC et ESEC_WF (à effectuer sur la machine où se trouvent les bases de données).
- Définissez NT AUTHORITY\NetworkService en tant que compte de connexion pour le service Sentinel (à effectuer à distance, sur votre machine).
- Configurez le démarrage du service Sentinel (à effectuer à distance, sur votre machine).

Ajout du service Sentinel en tant que compte de connexion dans les instances de base de données ESEC et ESEC_WF

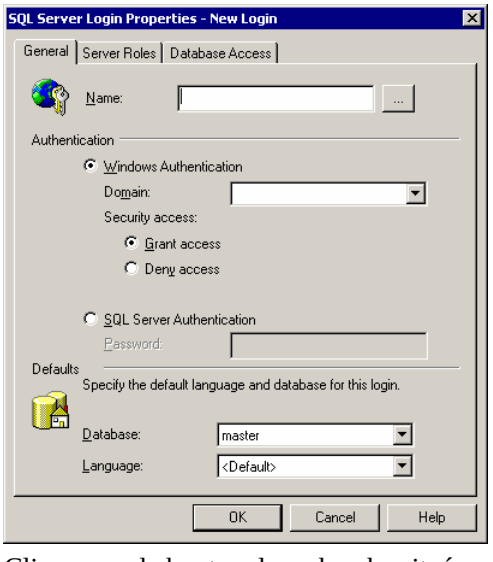
Pour ajouter un compte de connexion d'une machine distante sur le serveur de base de données

REMARQUE : dans la procédure suivante, l'exemple choisi est celui de l'ajout du compte secnet\case1 en tant que compte de connexion sur le serveur de base de données.

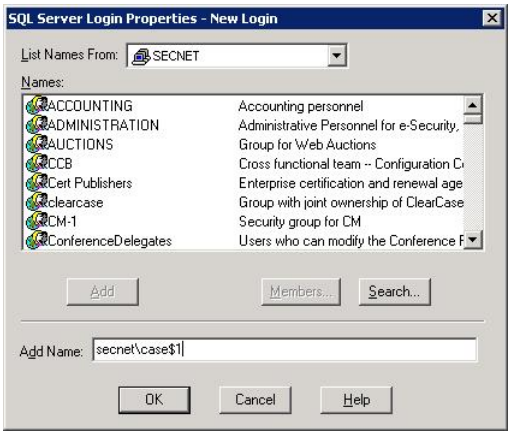
1. Sur la machine où se trouvent les bases de données, ouvrez SQL Server Enterprise Manager. Dans le volet de navigation, sous SQL Server Group, développez le dossier Security (Sécurité) et sélectionnez Logins (Connexions).



2. Cliquez avec le bouton droit sur *Logins* (Connexions) > *New login*… (Nouvelle connexion)

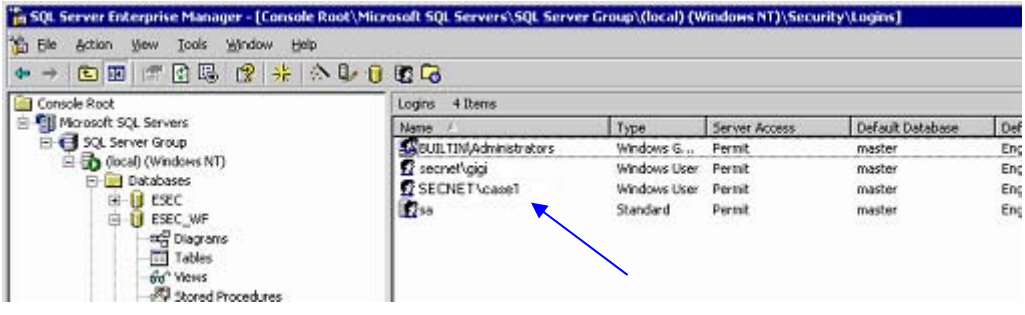


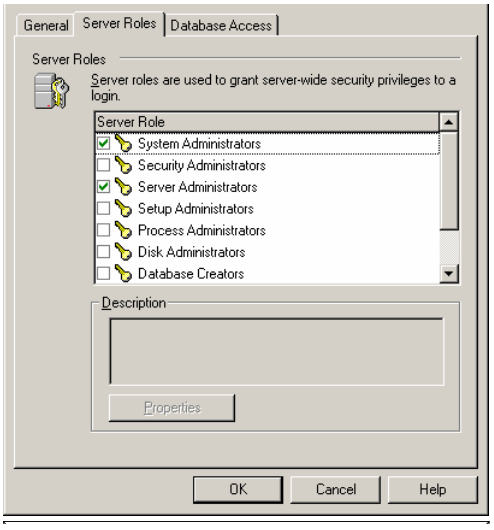
3. Cliquez sur le bouton de recherche situé en regard du champ Name (Nom). La fenêtre suivante s'affiche :

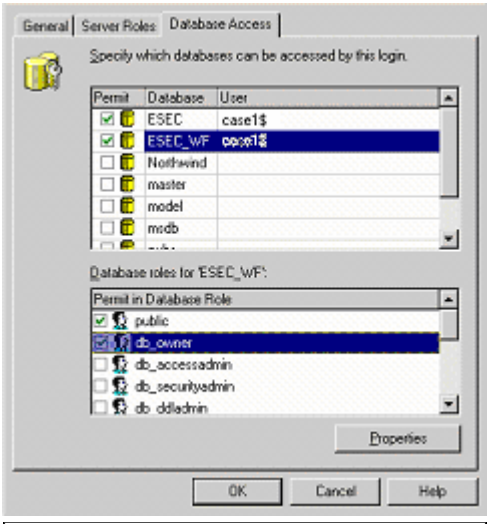


Dans le champ Add Name (Ajouter un nom), tapez un nom de domaine ainsi qu'un nom d'utilisateur (exemple : secnet\case1$). Il s'agit de la machine <nom de domaine>\<nom de la machine>$ que vous ajoutez en tant que compte de connexion sur le serveur de base de données. Cliquez sur *OK*.

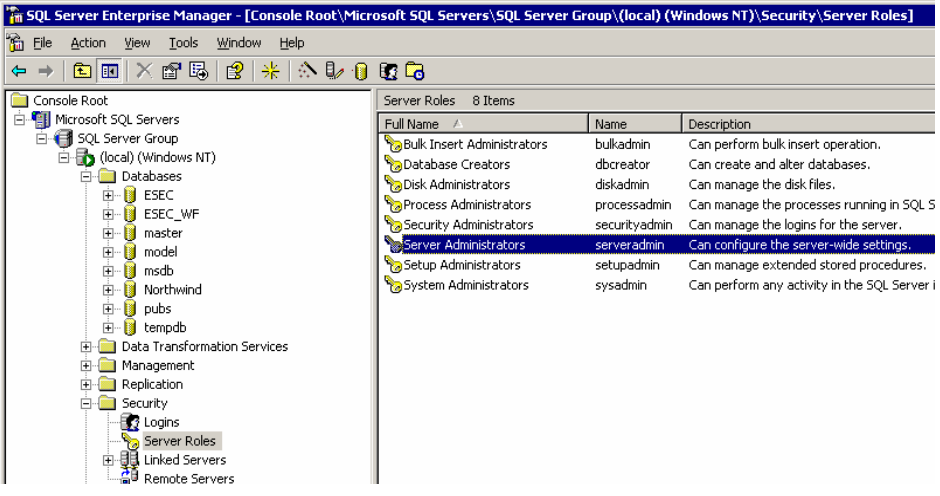
4. Cliquez avec le bouton droit sur le nom ([<nom de domaine>\<nom de la machine>$]) de la machine que vous ajoutez en tant que compte de connexion, puis sur Properties (Propriétés), et modifiez les rôles du serveur ainsi que l'accès à la base de données. Sélectionnez System Administrators (Administrateurs système) et Server Administrators (Administrateurs du serveur) en tant que Server Roles (Rôles du serveur). Définissez l'accès à la base de données ESEC sur « public » (public) et « db_owner » (propriétaire de la base). Définissez l'accès à la base de données ESEC sur « public » et « db_owner ».

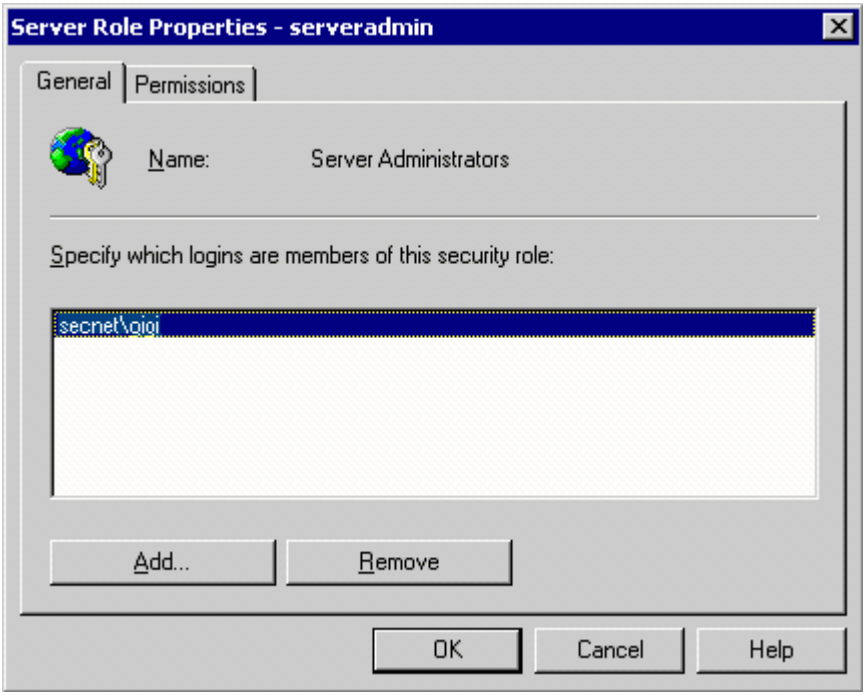




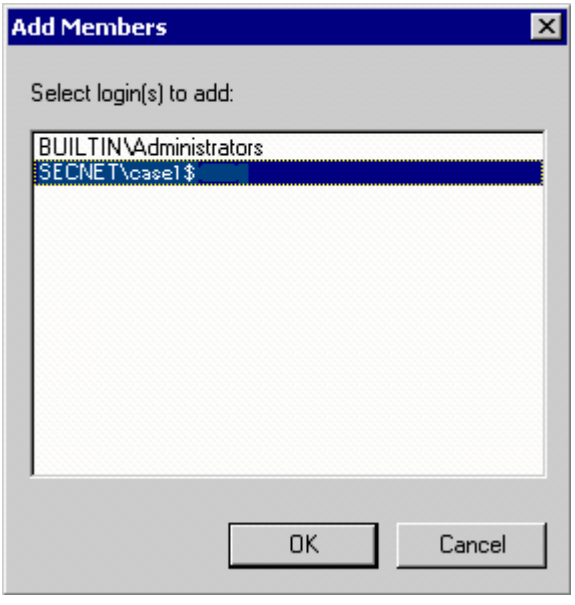


5. Sous Server Roles (Rôles du serveur), sélectionnez Server Administrators (Administrateurs du serveur) et cliquez avec le bouton droit sur *Properties* (Propriétés).





6. Cliquez sur le bouton *Add* (Ajouter).

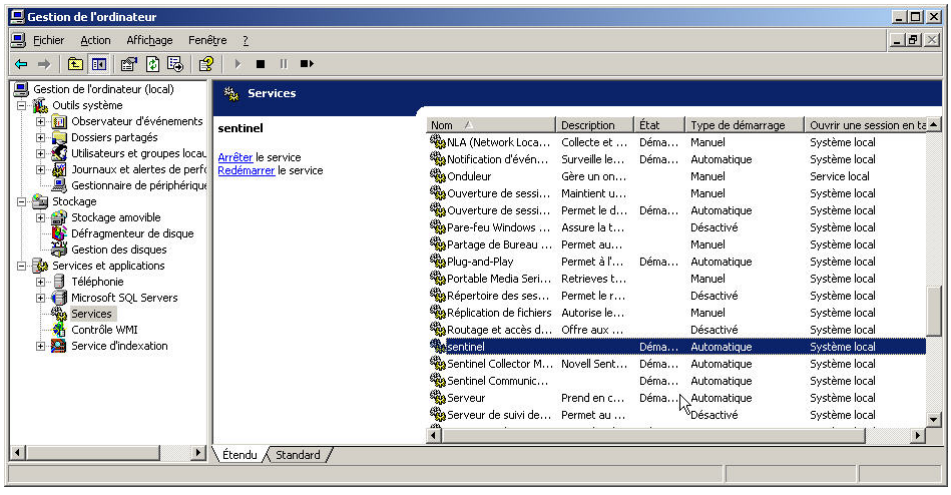


Cliquez sur OK. Secnet\case1$ est ajouté.

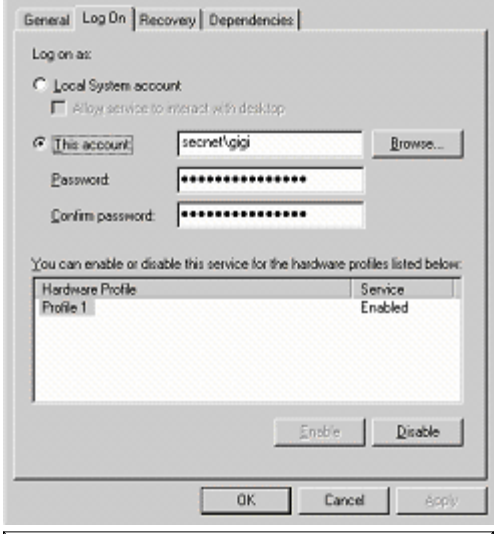
Configuration de NT AUTHORITY\NetworkService en tant que compte de connexion pour le service Sentinel

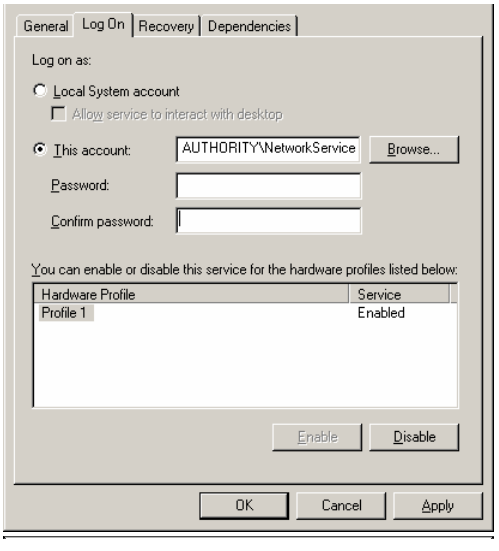
Pour configurer NT AUTHORITY\NetworkService en tant que compte de connexion pour le service Sentinel

1. Sur la machine que vous souhaitez connecter à la base de données, cliquez sur *Start* (Démarrer) > *Programs* (Programmes) > *Administrative Tools* (Outils d'administration) > *Services*.

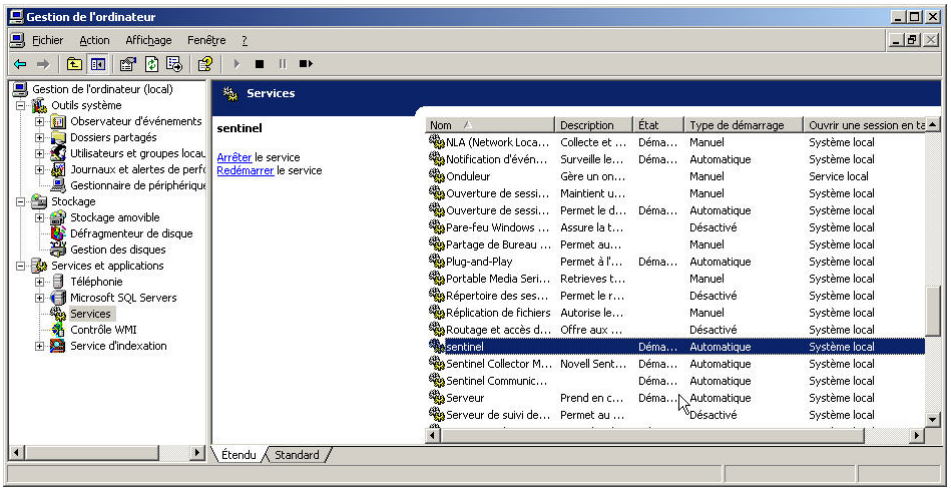


2. Arrêtez le service Sentinel. Cliquez avec le bouton droit et sélectionnez *Properties* (Propriétés), puis cliquez sur l'onglet *Log On* (Ouvrir une session).
3. Cliquez sur This Account (Ce compte) et dans le champ correspondant, entrez NT AUTHORITY\NetworkService. Effacez les informations contenues dans les champs Password (Mot de passe) et Confirm Password (Confirmer le mot de passe).





Cliquez sur *OK*. La fenêtre des services de Sentinel doit indiquer Network Service (Service réseau) dans la colonne Log On As (Ouvrir une session en tant que).



Configuration du service Sentinel pour le démarrage

Pour que le service Sentinel démarre correctement, le compte NT AUTHORITY\NetworkService doit disposer d'une autorisation d'accès en écriture à %ESEC_HOME%. D'après la documentation Microsoft, le compte NetworkService dispose des privilèges suivants :

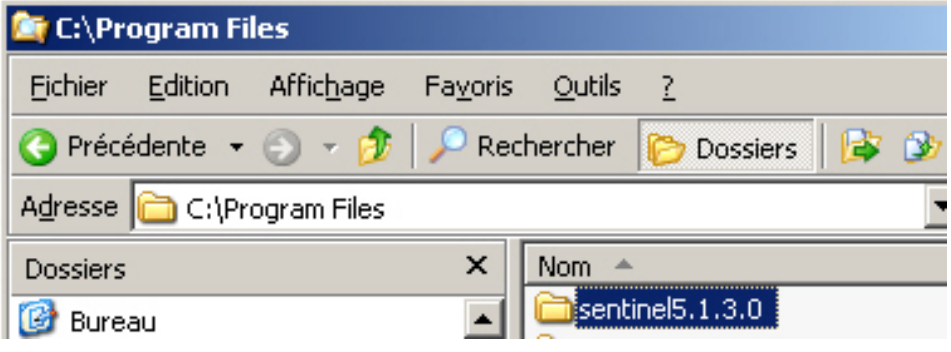
- SE_AUDIT_NAME
- SE_CHANGE_NOTIFY_NAME
- SE_UNDOCK_NAME
- Tous les privilèges attribués à des utilisateurs, authentifiés ou pas

Il vous faut accorder des autorisations d'accès en écriture au groupe Users (utilisateurs) pour le répertoire %ESEC_HOME%.

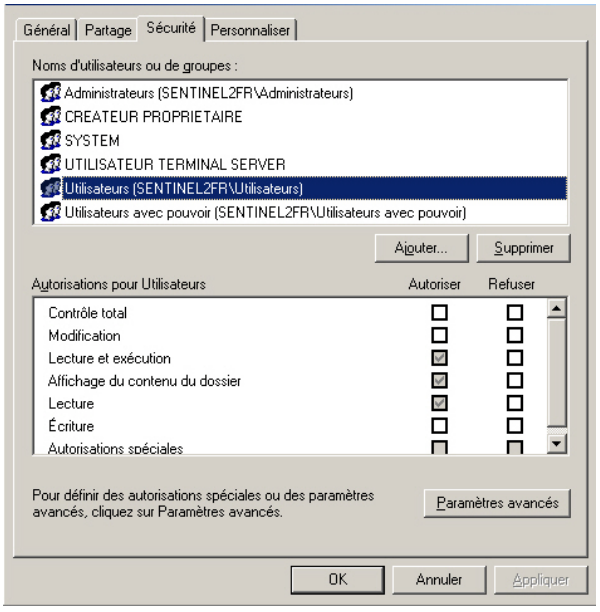
Pour configurer le service Sentinel pour le démarrage

Ouvrez l'Explorateur de Windows et accédez au répertoire %ESEC_HOME%.

1. Cliquez avec le bouton droit sur le dossier parent Sentinel (appelé « sentinel5.1.3 »), sélectionnez *Properties* (Propriétés), puis cliquez sur l'onglet *Security* (Sécurité).



2. Cliquez sur le groupe Users (utilisateurs). Donnez à ce groupe les autorisations d'accès suivantes : Read&Execute (Lecture et exécution), List Folder Contents (Affichage du contenu du dossier), Read (Lecture), Write (Écriture).



Cliquez sur *OK*.

Dans la fenêtre des services, redémarrez le service Sentinel

C Autorisations d'accès, rôles et utilisateurs de la base de données Sentinel

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

L'objectif du présent document est de dresser la liste des utilisateurs et des rôles de la base de données Sentinel en détaillant leurs autorisations d'accès.

Instance de la base de données Sentinel

ESEC

Utilisateurs :

- esecadm
- esecapp
- esecdba
- esecrpt
- autres utilisateurs

REMARQUE : les utilisateurs susmentionnés sont créés dans le Gestionnaire d'utilisateurs. Pour connaître le détail des autorisations d'accès, reportez-vous à la section « Utilisateurs de la base de données Sentinel ».

Rôles :

- ESEC_APP : autorisations d'accès identiques à celles de db_owner.
- ESEC_ETL : ce rôle n'est pas utilisé pour le moment. Il est réservé à de futures mises à jour. Pour connaître le détail des autorisations d'accès, reportez-vous à la section Rôles de la base de données Sentinel.
- ESEC_USER : pour connaître le détail des autorisations d'accès, reportez-vous à la section Rôles de la base de données Sentinel.

ESEC_WF

- Utilisateurs : esecapp : pour connaître le détail des autorisations d'accès, reportez-vous à la section Utilisateurs de la base de données Sentinel.
- Rôles : ESEC_APP : pour connaître le détail des autorisations d'accès, reportez-vous à la section Rôles de la base de données Sentinel.

Utilisateurs de la base de données Sentinel

Summary (Récapitulatif)

Nom d'utilisateur	Nom du groupe	Nom de connexion	Nom par défaut de la base de données
esecadm	ESEC_USER	esecadm	ESEC
esecapp	ESEC_APP	esecapp	ESEC
esecapp	ESEC_ETL	esecapp	ESEC

esecdba	db_owner	esecdba	ESEC
esecrpt	ESEC_USER	esecrpt	ESEC

esecadm

Nom de connexion	Nom de la base de données	Nom d'utilisateur	Alias utilisé
esecadm	ESEC	ESEC_USER	MemberOf
esecadm	ESEC	esecadm	User (Utilisateur)

esecapp

Nom de connexion	Nom de la base de données	Nom d'utilisateur	Alias utilisé
esecapp	ESEC	ESEC_APP	MemberOf
esecapp	ESEC	ESEC_ETL	MemberOf
esecapp	ESEC	esecapp	User (Utilisateur)
esecapp	ESEC_WF	ESEC_APP	MemberOf
esecapp	ESEC_WF	esecapp	User (Utilisateur)

esecdba

Nom de connexion	Nom de la base de données	Nom d'utilisateur	Alias utilisé
esecdba	ESEC	db_owner	MemberOf
esecdba	ESEC	esecdba	User (Utilisateur)

esecrpt

Nom de connexion	Nom de la base de données	Nom d'utilisateur	Alias utilisé
esecrpt	ESEC	ESEC_USER	MemberOf
esecrpt	ESEC	esecrpt	User (Utilisateur)

Rôles de la base de données Sentinel

Summary (Récapitulatif)

- ESEC_APP : rôle de base de données pour ESEC et ESEC_WF. Il dispose des mêmes autorisations d'accès que db_owner. Pour connaître le détail des autorisations d'accès, reportez-vous à la section ESEC_APP.
- ESEC_ETL : rôle de base de données pour l'instance ESEC. Ce rôle n'est pas utilisé pour le moment. Il est réservé à un développement ultérieur. Pour connaître le détail des autorisations d'accès, reportez-vous à la section Rôles de la base de données Sentinel.
- ESEC_USER : rôle de l'instance ESEC. Pour connaître le détail des autorisations d'accès, reportez-vous à la section Rôles de la base de données Sentinel.

ESEC_APP

Dans l'instance ESEC, ESEC_APP dispose des mêmes autorisations d'accès que db_owner. Le rôle ESEC_APP permet d'effectuer les activités de tous les rôles de la base de données ainsi que des activités de maintenance et de configuration dans la base de données. Les autorisations d'accès de ce rôle couvrent tous les autres rôles définis de manière fixe dans la base de données.

Ces autorisations d'accès sont celles dont dispose le rôle ESEC_APP dans l'instance ESEC_WF.

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_APP	Activities	193 SELECT	U Table utilisateur
ESEC_APP	Activities	195 INSERT	U Table utilisateur
ESEC_APP	Activities	196 DELETE	U Table utilisateur
ESEC_APP	Activities	197 UPDATE	U Table utilisateur
ESEC_APP	ActivityData	193 SELECT	U Table utilisateur
ESEC_APP	ActivityData	195 INSERT	U Table utilisateur
ESEC_APP	ActivityData	196 DELETE	U Table utilisateur
ESEC_APP	ActivityData	197 UPDATE	U Table utilisateur
ESEC_APP	ActivityStateEventAudits	193 SELECT	U Table utilisateur
ESEC_APP	ActivityStateEventAudits	195 INSERT	U Table utilisateur
ESEC_APP	ActivityStateEventAudits	196 DELETE	U Table utilisateur
ESEC_APP	ActivityStateEventAudits	197 UPDATE	U Table utilisateur
ESEC_APP	ActivityStates	193 SELECT	U Table utilisateur
ESEC_APP	ActivityStates	195 INSERT	U Table utilisateur
ESEC_APP	ActivityStates	196 DELETE	U Table utilisateur
ESEC_APP	ActivityStates	197 UPDATE	U Table utilisateur
ESEC_APP	AndJoinTable	193 SELECT	U Table utilisateur
ESEC_APP	AndJoinTable	195 INSERT	U Table utilisateur
ESEC_APP	AndJoinTable	196 DELETE	U Table utilisateur
ESEC_APP	AndJoinTable	197 UPDATE	U Table utilisateur

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_APP	AssignmentEventAudits	193 SELECT	U Table utilisateur
ESEC_APP	AssignmentEventAudits	195 INSERT	U Table utilisateur
ESEC_APP	AssignmentEventAudits	196 DELETE	U Table utilisateur
ESEC_APP	AssignmentEventAudits	197 UPDATE	U Table utilisateur
ESEC_APP	AssignmentsTable	193 SELECT	U Table utilisateur
ESEC_APP	AssignmentsTable	195 INSERT	U Table utilisateur
ESEC_APP	AssignmentsTable	196 DELETE	U Table utilisateur
ESEC_APP	AssignmentsTable	197 UPDATE	U Table utilisateur
ESEC_APP	Counters	193 SELECT	U Table utilisateur
ESEC_APP	Counters	195 INSERT	U Table utilisateur
ESEC_APP	Counters	196 DELETE	U Table utilisateur
ESEC_APP	Counters	197 UPDATE	U Table utilisateur
ESEC_APP	CreateProcessEventAudits	193 SELECT	U Table utilisateur
ESEC_APP	CreateProcessEventAudits	195 INSERT	U Table utilisateur
ESEC_APP	CreateProcessEventAudits	196 DELETE	U Table utilisateur
ESEC_APP	CreateProcessEventAudits	197 UPDATE	U Table utilisateur
ESEC_APP	DataEventAudits	193 SELECT	U Table utilisateur
ESEC_APP	DataEventAudits	195 INSERT	U Table utilisateur
ESEC_APP	DataEventAudits	196 DELETE	U Table utilisateur
ESEC_APP	DataEventAudits	197 UPDATE	U Table utilisateur
ESEC_APP	Deadlines	193 SELECT	U Table utilisateur
ESEC_APP	Deadlines	195 INSERT	U Table utilisateur
ESEC_APP	Deadlines	196 DELETE	U Table utilisateur
ESEC_APP	Deadlines	197 UPDATE	U Table utilisateur
ESEC_APP	EventTypes	193 SELECT	U Table

Nom du rôle	Nom de l'objet	Opération	Type
			utilisateur
ESEC_APP	EventTypes	195 INSERT	U Table utilisateur
ESEC_APP	EventTypes	196 DELETE	U Table utilisateur
ESEC_APP	EventTypes	197 UPDATE	U Table utilisateur
ESEC_APP	GroupGroupTable	193 SELECT	U Table utilisateur
ESEC_APP	GroupGroupTable	195 INSERT	U Table utilisateur
ESEC_APP	GroupGroupTable	196 DELETE	U Table utilisateur
ESEC_APP	GroupGroupTable	197 UPDATE	U Table utilisateur
ESEC_APP	GroupTable	193 SELECT	U Table utilisateur
ESEC_APP	GroupTable	195 INSERT	U Table utilisateur
ESEC_APP	GroupTable	196 DELETE	U Table utilisateur
ESEC_APP	GroupTable	197 UPDATE	U Table utilisateur
ESEC_APP	GroupUser	193 SELECT	U Table utilisateur
ESEC_APP	GroupUser	195 INSERT	U Table utilisateur
ESEC_APP	GroupUser	196 DELETE	U Table utilisateur
ESEC_APP	GroupUser	197 UPDATE	U Table utilisateur
ESEC_APP	GroupUserPackLevelParticipant	193 SELECT	U Table utilisateur
ESEC_APP	GroupUserPackLevelParticipant	195 INSERT	U Table utilisateur
ESEC_APP	GroupUserPackLevelParticipant	196 DELETE	U Table utilisateur
ESEC_APP	GroupUserPackLevelParticipant	197 UPDATE	U Table utilisateur
ESEC_APP	GroupUserProcLevelParticipant	193 SELECT	U Table utilisateur
ESEC_APP	GroupUserProcLevelParticipant	195 INSERT	U Table utilisateur
ESEC_APP	GroupUserProcLevelParticipant	196 DELETE	U Table utilisateur
ESEC_APP	GroupUserProcLevelParticipant	197 UPDATE	U Table utilisateur
ESEC_APP	LockTable	193 SELECT	U Table utilisateur

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_APP	LockTable	195 INSERT	U Table utilisateur
ESEC_APP	LockTable	196 DELETE	U Table utilisateur
ESEC_APP	LockTable	197 UPDATE	U Table utilisateur
ESEC_APP	NewEventAuditData	193 SELECT	U Table utilisateur
ESEC_APP	NewEventAuditData	195 INSERT	U Table utilisateur
ESEC_APP	NewEventAuditData	196 DELETE	U Table utilisateur
ESEC_APP	NewEventAuditData	197 UPDATE	U Table utilisateur
ESEC_APP	NextXPDLVersions	193 SELECT	U Table utilisateur
ESEC_APP	NextXPDLVersions	195 INSERT	U Table utilisateur
ESEC_APP	NextXPDLVersions	196 DELETE	U Table utilisateur
ESEC_APP	NextXPDLVersions	197 UPDATE	U Table utilisateur
ESEC_APP	NormalUser	193 SELECT	U Table utilisateur
ESEC_APP	NormalUser	195 INSERT	U Table utilisateur
ESEC_APP	NormalUser	196 DELETE	U Table utilisateur
ESEC_APP	NormalUser	197 UPDATE	U Table utilisateur
ESEC_APP	ObjectId	193 SELECT	U Table utilisateur
ESEC_APP	ObjectId	195 INSERT	U Table utilisateur
ESEC_APP	ObjectId	196 DELETE	U Table utilisateur
ESEC_APP	ObjectId	197 UPDATE	U Table utilisateur
ESEC_APP	OldEventAuditData	193 SELECT	U Table utilisateur
ESEC_APP	OldEventAuditData	195 INSERT	U Table utilisateur
ESEC_APP	OldEventAuditData	196 DELETE	U Table utilisateur
ESEC_APP	OldEventAuditData	197 UPDATE	U Table utilisateur
ESEC_APP	PackLevelParticipant	193 SELECT	U Table utilisateur
ESEC_APP	PackLevelParticipant	195 INSERT	U Table

Nom du rôle	Nom de l'objet	Opération	Type
			utilisateur
ESEC_APP	PackLevelParticipant	196 DELETE	U Table utilisateur
ESEC_APP	PackLevelParticipant	197 UPDATE	U Table utilisateur
ESEC_APP	PackLevelXPDLApp	193 SELECT	U Table utilisateur
ESEC_APP	PackLevelXPDLApp	195 INSERT	U Table utilisateur
ESEC_APP	PackLevelXPDLApp	196 DELETE	U Table utilisateur
ESEC_APP	PackLevelXPDLApp	197 UPDATE	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppDetail	193 SELECT	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppDetail	195 INSERT	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppDetail	196 DELETE	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppDetail	197 UPDATE	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	193 SELECT	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	195 INSERT	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	196 DELETE	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	197 UPDATE	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppUser	193 SELECT	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppUser	195 INSERT	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppUser	196 DELETE	U Table utilisateur
ESEC_APP	PackLevelXPDLAppTAAppUser	197 UPDATE	U Table utilisateur
ESEC_APP	PackLevelXPDLAppToolAgentApp	193 SELECT	U Table utilisateur
ESEC_APP	PackLevelXPDLAppToolAgentApp	195 INSERT	U Table utilisateur
ESEC_APP	PackLevelXPDLAppToolAgentApp	196 DELETE	U Table utilisateur
ESEC_APP	PackLevelXPDLAppToolAgentApp	197 UPDATE	U Table utilisateur
ESEC_APP	ProcessData	193 SELECT	U Table utilisateur
ESEC_APP	ProcessData	195 INSERT	U Table utilisateur

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_APP	ProcessData	196 DELETE	U Table utilisateur
ESEC_APP	ProcessData	197 UPDATE	U Table utilisateur
ESEC_APP	ProcessDefinitions	193 SELECT	U Table utilisateur
ESEC_APP	ProcessDefinitions	195 INSERT	U Table utilisateur
ESEC_APP	ProcessDefinitions	196 DELETE	U Table utilisateur
ESEC_APP	ProcessDefinitions	197 UPDATE	U Table utilisateur
ESEC_APP	Processus	193 SELECT	U Table utilisateur
ESEC_APP	Processus	195 INSERT	U Table utilisateur
ESEC_APP	Processus	196 DELETE	U Table utilisateur
ESEC_APP	Processus	197 UPDATE	U Table utilisateur
ESEC_APP	ProcessRequesters	193 SELECT	U Table utilisateur
ESEC_APP	ProcessRequesters	195 INSERT	U Table utilisateur
ESEC_APP	ProcessRequesters	196 DELETE	U Table utilisateur
ESEC_APP	ProcessRequesters	197 UPDATE	U Table utilisateur
ESEC_APP	ProcessStateEventAudits	193 SELECT	U Table utilisateur
ESEC_APP	ProcessStateEventAudits	195 INSERT	U Table utilisateur
ESEC_APP	ProcessStateEventAudits	196 DELETE	U Table utilisateur
ESEC_APP	ProcessStateEventAudits	197 UPDATE	U Table utilisateur
ESEC_APP	ProcessStates	193 SELECT	U Table utilisateur
ESEC_APP	ProcessStates	195 INSERT	U Table utilisateur
ESEC_APP	ProcessStates	196 DELETE	U Table utilisateur
ESEC_APP	ProcessStates	197 UPDATE	U Table utilisateur
ESEC_APP	ProcLevelParticipant	193 SELECT	U Table utilisateur
ESEC_APP	ProcLevelParticipant	195 INSERT	U Table utilisateur
ESEC_APP	ProcLevelParticipant	196 DELETE	U Table

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_APP	ProcLevelParticipant	197 UPDATE	U Table utilisateur
ESEC_APP	ProcLevelXPDLApp	193 SELECT	U Table utilisateur
ESEC_APP	ProcLevelXPDLApp	195 INSERT	U Table utilisateur
ESEC_APP	ProcLevelXPDLApp	196 DELETE	U Table utilisateur
ESEC_APP	ProcLevelXPDLApp	197 UPDATE	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppDetail	193 SELECT	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppDetail	195 INSERT	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppDetail	196 DELETE	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppDetail	197 UPDATE	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	193 SELECT	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	195 INSERT	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	196 DELETE	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	197 UPDATE	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppUser	193 SELECT	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppUser	195 INSERT	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppUser	196 DELETE	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppTAAppUser	197 UPDATE	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppToolAgentApp	193 SELECT	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppToolAgentApp	195 INSERT	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppToolAgentApp	196 DELETE	U Table utilisateur
ESEC_APP	ProcLevelXPDLAppToolAgentApp	197 UPDATE	U Table utilisateur
ESEC_APP	ResourcesTable	193 SELECT	U Table utilisateur
ESEC_APP	ResourcesTable	195 INSERT	U Table utilisateur
ESEC_APP	ResourcesTable	196 DELETE	U Table utilisateur

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_APP	ResourcesTable	197 UPDATE	U Table utilisateur
ESEC_APP	StateEventAudits	193 SELECT	U Table utilisateur
ESEC_APP	StateEventAudits	195 INSERT	U Table utilisateur
ESEC_APP	StateEventAudits	196 DELETE	U Table utilisateur
ESEC_APP	StateEventAudits	197 UPDATE	U Table utilisateur
ESEC_APP	ToolAgentApp	193 SELECT	U Table utilisateur
ESEC_APP	ToolAgentApp	195 INSERT	U Table utilisateur
ESEC_APP	ToolAgentApp	196 DELETE	U Table utilisateur
ESEC_APP	ToolAgentApp	197 UPDATE	U Table utilisateur
ESEC_APP	ToolAgentAppDetail	193 SELECT	U Table utilisateur
ESEC_APP	ToolAgentAppDetail	195 INSERT	U Table utilisateur
ESEC_APP	ToolAgentAppDetail	196 DELETE	U Table utilisateur
ESEC_APP	ToolAgentAppDetail	197 UPDATE	U Table utilisateur
ESEC_APP	ToolAgentAppDetailUser	193 SELECT	U Table utilisateur
ESEC_APP	ToolAgentAppDetailUser	195 INSERT	U Table utilisateur
ESEC_APP	ToolAgentAppDetailUser	196 DELETE	U Table utilisateur
ESEC_APP	ToolAgentAppDetailUser	197 UPDATE	U Table utilisateur
ESEC_APP	ToolAgentAppUser	193 SELECT	U Table utilisateur
ESEC_APP	ToolAgentAppUser	195 INSERT	U Table utilisateur
ESEC_APP	ToolAgentAppUser	196 DELETE	U Table utilisateur
ESEC_APP	ToolAgentAppUser	197 UPDATE	U Table utilisateur
ESEC_APP	ToolAgentUser	193 SELECT	U Table utilisateur
ESEC_APP	ToolAgentUser	195 INSERT	U Table utilisateur
ESEC_APP	ToolAgentUser	196 DELETE	U Table utilisateur
ESEC_APP	ToolAgentUser	197 UPDATE	U Table

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_APP	UserGroupTable	193 SELECT	U Table utilisateur
ESEC_APP	UserGroupTable	195 INSERT	U Table utilisateur
ESEC_APP	UserGroupTable	196 DELETE	U Table utilisateur
ESEC_APP	UserGroupTable	197 UPDATE	U Table utilisateur
ESEC_APP	UserPackLevelParticipant	193 SELECT	U Table utilisateur
ESEC_APP	UserPackLevelParticipant	195 INSERT	U Table utilisateur
ESEC_APP	UserPackLevelParticipant	196 DELETE	U Table utilisateur
ESEC_APP	UserPackLevelParticipant	197 UPDATE	U Table utilisateur
ESEC_APP	UserProcLevelParticipant	193 SELECT	U Table utilisateur
ESEC_APP	UserProcLevelParticipant	195 INSERT	U Table utilisateur
ESEC_APP	UserProcLevelParticipant	196 DELETE	U Table utilisateur
ESEC_APP	UserProcLevelParticipant	197 UPDATE	U Table utilisateur
ESEC_APP	UserTable	193 SELECT	U Table utilisateur
ESEC_APP	UserTable	195 INSERT	U Table utilisateur
ESEC_APP	UserTable	196 DELETE	U Table utilisateur
ESEC_APP	UserTable	197 UPDATE	U Table utilisateur
ESEC_APP	XPDLApplicationPackage	193 SELECT	U Table utilisateur
ESEC_APP	XPDLApplicationPackage	195 INSERT	U Table utilisateur
ESEC_APP	XPDLApplicationPackage	196 DELETE	U Table utilisateur
ESEC_APP	XPDLApplicationPackage	197 UPDATE	U Table utilisateur
ESEC_APP	XPDLApplicationProcess	193 SELECT	U Table utilisateur
ESEC_APP	XPDLApplicationProcess	195 INSERT	U Table utilisateur
ESEC_APP	XPDLApplicationProcess	196 DELETE	U Table utilisateur
ESEC_APP	XPDLApplicationProcess	197 UPDATE	U Table utilisateur

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_APP	XPDLData	193 SELECT	U Table utilisateur
ESEC_APP	XPDLData	195 INSERT	U Table utilisateur
ESEC_APP	XPDLData	196 DELETE	U Table utilisateur
ESEC_APP	XPDLData	197 UPDATE	U Table utilisateur
ESEC_APP	XPDLHistory	193 SELECT	U Table utilisateur
ESEC_APP	XPDLHistory	195 INSERT	U Table utilisateur
ESEC_APP	XPDLHistory	196 DELETE	U Table utilisateur
ESEC_APP	XPDLHistory	197 UPDATE	U Table utilisateur
ESEC_APP	XPDLHistoryData	193 SELECT	U Table utilisateur
ESEC_APP	XPDLHistoryData	195 INSERT	U Table utilisateur
ESEC_APP	XPDLHistoryData	196 DELETE	U Table utilisateur
ESEC_APP	XPDLHistoryData	197 UPDATE	U Table utilisateur
ESEC_APP	XPDLParticipantPackage	193 SELECT	U Table utilisateur
ESEC_APP	XPDLParticipantPackage	195 INSERT	U Table utilisateur
ESEC_APP	XPDLParticipantPackage	196 DELETE	U Table utilisateur
ESEC_APP	XPDLParticipantPackage	197 UPDATE	U Table utilisateur
ESEC_APP	XPDLParticipantProcess	193 SELECT	U Table utilisateur
ESEC_APP	XPDLParticipantProcess	195 INSERT	U Table utilisateur
ESEC_APP	XPDLParticipantProcess	196 DELETE	U Table utilisateur
ESEC_APP	XPDLParticipantProcess	197 UPDATE	U Table utilisateur
ESEC_APP	XPDLReferences	193 SELECT	U Table utilisateur
ESEC_APP	XPDLReferences	195 INSERT	U Table utilisateur
ESEC_APP	XPDLReferences	196 DELETE	U Table utilisateur
ESEC_APP	XPDLReferences	197 UPDATE	U Table utilisateur
ESEC_APP	XPDLS	193 SELECT	U Table

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_APP	XPDLS	195 INSERT	U Table utilisateur
ESEC_APP	XPDLS	196 DELETE	U Table utilisateur
ESEC_APP	XPDLS	197 UPDATE	U Table utilisateur

ESEC_ETL

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_ETL	ACTVY	193 SELECT	U Table utilisateur
ESEC_ETL	ACTVY_NAMESPACE	193 SELECT	U Table utilisateur
ESEC_ETL	ACTVY_PARM	193 SELECT	U Table utilisateur
ESEC_ETL	ACTVY_REF	193 SELECT	U Table utilisateur
ESEC_ETL	ACTVY_REF_PARM_VAL	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_ALERT	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_ALERT_CVE	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_ALERT_PRODUCT	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_ATTACK	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_ATTACK_ALERT	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_ATTACK_CVE	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_ATTACK_MAP	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_ATTACK_PLUGIN	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_CREDIBILITY	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_FEED	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_PRODUCT	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_PRODUCT_SERVICE_PACK	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_PRODUCT_VERSION	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_SEVERITY	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_SUBALERT	193 SELECT	U Table

Nom du rôle	Nom de l'objet	Opération	Type
			utilisateur
ESEC_ETL	ADV_URGENCY	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_VENDOR	193 SELECT	U Table utilisateur
ESEC_ETL	ADV_VULN_PRODUCT	193 SELECT	U Table utilisateur
ESEC_ETL	ANNOTATIONS	193 SELECT	U Table utilisateur
ESEC_ETL	ASSET	193 SELECT	U Table utilisateur
ESEC_ETL	ASSET_CTGRY	193 SELECT	U Table utilisateur
ESEC_ETL	ASSET_HOSTNAME	193 SELECT	U Table utilisateur
ESEC_ETL	ASSET_IP	193 SELECT	U Table utilisateur
ESEC_ETL	ASSET_LOC	193 SELECT	U Table utilisateur
ESEC_ETL	ASSET_VAL_LKUP	193 SELECT	U Table utilisateur
ESEC_ETL	ASSET_X_ENTITY_X_ROLE	193 SELECT	U Table utilisateur
ESEC_ETL	ASSOCIATIONS	193 SELECT	U Table utilisateur
ESEC_ETL	ATTACHMENTS	193 SELECT	U Table utilisateur
ESEC_ETL	CONFIGS	193 SELECT	U Table utilisateur
ESEC_ETL	CONTACTS	193 SELECT	U Table utilisateur
ESEC_ETL	CORRELATED_EVENTS_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	CORRELATED_EVENTS_P_MIN	193 SELECT	U Table utilisateur
ESEC_ETL	CRIT_LKUP	193 SELECT	U Table utilisateur
ESEC_ETL	CUST	193 SELECT	U Table utilisateur
ESEC_ETL	ENTITY_TYP_LKUP	193 SELECT	U Table utilisateur
ESEC_ETL	ENV_IDENTITY_LKUP	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_ARCHIVE_CONFIG	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_ARCHIVE_LOG_FILES	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_ARCHIVE_LOGS	193 SELECT	U Table utilisateur

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_ETL	ESEC_DB_PATCHES	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_DB_VERSION	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_DISPLAY	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_PARTITION_CONFIG	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_PARTITIONS_TEMP	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_PORT_REFERENCE	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_PROTOCOL_REFERENCE	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_SDM_LOCK	193 SELECT	U Table utilisateur
ESEC_ETL	ESEC_SEQUENCE	193 SELECT	U Table utilisateur
ESEC_ETL	EVENTS_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	EVENTS_P_MIN	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_AGENT	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_ASSET	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	195 INSERT	U Table utilisateur
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	196 DELETE	U Table utilisateur
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	197 UPDATE	U Table utilisateur
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MIN	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	195 INSERT	U Table utilisateur
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	196 DELETE	U Table utilisateur
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	197 UPDATE	U Table utilisateur
ESEC_ETL	EVT_DEST_SMRY_1_P_MIN	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	195 INSERT	U Table

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	196 DELETE	U Table utilisateur
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	197 UPDATE	U Table utilisateur
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MIN	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_NAME	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_NAME	195 INSERT	U Table utilisateur
ESEC_ETL	EVT_NAME	196 DELETE	U Table utilisateur
ESEC_ETL	EVT_NAME	197 UPDATE	U Table utilisateur
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	195 INSERT	U Table utilisateur
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	196 DELETE	U Table utilisateur
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	197 UPDATE	U Table utilisateur
ESEC_ETL	EVT_PORT_SMRY_1_P_MIN	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_PRTCL	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_RSRC	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	195 INSERT	U Table utilisateur
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	196 DELETE	U Table utilisateur
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	197 UPDATE	U Table utilisateur
ESEC_ETL	EVT_SEV_SMRY_1_P_MIN	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	195 INSERT	U Table utilisateur
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	196 DELETE	U Table utilisateur
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	197 UPDATE	U Table utilisateur
ESEC_ETL	EVT_SRC_SMRY_1_P_MIN	193 SELECT	U Table utilisateur

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_ETL	EVT_TXNMY	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_USR	193 SELECT	U Table utilisateur
ESEC_ETL	EVT_USR	195 INSERT	U Table utilisateur
ESEC_ETL	EVT_USR	196 DELETE	U Table utilisateur
ESEC_ETL	EVT_USR	197 UPDATE	U Table utilisateur
ESEC_ETL	EXT_DATA	193 SELECT	U Table utilisateur
ESEC_ETL	HIST_CORRELATED_EVENTS_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	HIST_EVENTS_P_MAX	193 SELECT	U Table utilisateur
ESEC_ETL	IMAGES	193 SELECT	U Table utilisateur
ESEC_ETL	INCIDENTS	193 SELECT	U Table utilisateur
ESEC_ETL	INCIDENTS_ASSETS	193 SELECT	U Table utilisateur
ESEC_ETL	INCIDENTS_EVENTS	193 SELECT	U Table utilisateur
ESEC_ETL	INCIDENTS_VULN	193 SELECT	U Table utilisateur
ESEC_ETL	L_STAT	193 SELECT	U Table utilisateur
ESEC_ETL	LOGS	193 SELECT	U Table utilisateur
ESEC_ETL	MD_CONFIG	193 SELECT	U Table utilisateur
ESEC_ETL	MD_EVT_FILE_STS	193 SELECT	U Table utilisateur
ESEC_ETL	MD_EVT_FILE_STS	195 INSERT	U Table utilisateur
ESEC_ETL	MD_EVT_FILE_STS	196 DELETE	U Table utilisateur
ESEC_ETL	MD_EVT_FILE_STS	197 UPDATE	U Table utilisateur
ESEC_ETL	MD_SMRY_STS	193 SELECT	U Table utilisateur
ESEC_ETL	MD_SMRY_STS	195 INSERT	U Table utilisateur
ESEC_ETL	MD_SMRY_STS	196 DELETE	U Table utilisateur
ESEC_ETL	MD_SMRY_STS	197 UPDATE	U Table utilisateur
ESEC_ETL	MD_VIEW_CONFIG	193 SELECT	U Table

Nom du rôle	Nom de l'objet	Opération	Type
			utilisateur
ESEC_ETL	NETWORK_IDENTITY_LKUP	193 SELECT	U Table utilisateur
ESEC_ETL	OBJ_STORE	193 SELECT	U Table utilisateur
ESEC_ETL	ORGANIZATION	193 SELECT	U Table utilisateur
ESEC_ETL	PERSON	193 SELECT	U Table utilisateur
ESEC_ETL	PHYSICAL_ASSET	193 SELECT	U Table utilisateur
ESEC_ETL	PRDT	193 SELECT	U Table utilisateur
ESEC_ETL	ROLE_LKUP	193 SELECT	U Table utilisateur
ESEC_ETL	SENSITIVITY_LKUP	193 SELECT	U Table utilisateur
ESEC_ETL	STATES	193 SELECT	U Table utilisateur
ESEC_ETL	USERS	193 SELECT	U Table utilisateur
ESEC_ETL	VNDR	193 SELECT	U Table utilisateur
ESEC_ETL	VULN	193 SELECT	U Table utilisateur
ESEC_ETL	VULN_CODE	193 SELECT	U Table utilisateur
ESEC_ETL	VULN_INFO	193 SELECT	U Table utilisateur
ESEC_ETL	VULN_RSRC	193 SELECT	U Table utilisateur
ESEC_ETL	VULN_RSRC_SCAN	193 SELECT	U Table utilisateur
ESEC_ETL	VULN_SCAN	193 SELECT	U Table utilisateur
ESEC_ETL	VULN_SCAN_VULN	193 SELECT	U Table utilisateur
ESEC_ETL	VULN_SCANNER	193 SELECT	U Table utilisateur
ESEC_ETL	WORKFLOW_DEF	193 SELECT	U Table utilisateur
ESEC_ETL	WORKFLOW_INFO	193 SELECT	U Table utilisateur

ESEC_USER

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_USER	ADV_ALERT_CVE_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_ALERT_PRODUCT_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_ALERT_RPT_V	193 SELECT	V Vue

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_USER	ADV_ATTACK_ALERT_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_ATTACK_CVE_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_ATTACK_MAP_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_ATTACK_PLUGIN_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_ATTACK_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_CREDIBILITY_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_FEED_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_PRODUCT_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_PRODUCT_SERVICE_PACK_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_PRODUCT_VERSION_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_SEVERITY_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_SUBALERT_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_URGENCY_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_VENDOR_RPT_V	193 SELECT	V Vue
ESEC_USER	ADV_VULN_PRODUCT_RPT_V	193 SELECT	V Vue
ESEC_USER	ANNOTATIONS_RPT_V	193 SELECT	V Vue
ESEC_USER	ASSET_CATEGORY_RPT_V	193 SELECT	V Vue
ESEC_USER	ASSET_HOSTNAME_RPT_V	193 SELECT	V Vue
ESEC_USER	ASSET_IP_RPT_V	193 SELECT	V Vue
ESEC_USER	ASSET_LOCATION_RPT_V	193 SELECT	V Vue
ESEC_USER	ASSET_RPT_V	193 SELECT	V Vue
ESEC_USER	ASSET_VALUE_RPT_V	193 SELECT	V Vue
ESEC_USER	ASSET_X_ENTITY_X_ROLE_RPT_V	193 SELECT	V Vue
ESEC_USER	ASSOCIATIONS_RPT_V	193 SELECT	V Vue
ESEC_USER	ATTACHMENTS_RPT_V	193 SELECT	V Vue
ESEC_USER	CONFIGS_RPT_V	193 SELECT	V Vue
ESEC_USER	CONTACTS_RPT_V	193 SELECT	V Vue
ESEC_USER	CORRELATED_EVENTS	193 SELECT	V Vue
ESEC_USER	CORRELATED_EVENTS_RPT_V	193 SELECT	V Vue
ESEC_USER	CORRELATED_EVENTS_RPT_V1	193 SELECT	V Vue
ESEC_USER	CRITICALITY_RPT_V	193 SELECT	V Vue
ESEC_USER	CUST_RPT_V	193 SELECT	V Vue
ESEC_USER	ENTITY_TYPE_RPT_V	193 SELECT	V Vue
ESEC_USER	ENV_IDENTITY_RPT_V	193 SELECT	V Vue
ESEC_USER	ESEC_DISPLAY_RPT_V	193 SELECT	V Vue
ESEC_USER	ESEC_PORT_REFERENCE_RPT_V	193 SELECT	V Vue
ESEC_USER	ESEC_PROTOCOL_REFERENCE_RPT_V	193 SELECT	V Vue
ESEC_USER	ESEC_SEQUENCE_RPT_V	193 SELECT	V Vue
ESEC_USER	esec_toBase	224 EXECUTE	NULL
ESEC_USER	esec_toDecimal	224 EXECUTE	NULL
ESEC_USER	esec_toIpChar	224 EXECUTE	NULL
ESEC_USER	EVENTS	193 SELECT	V Vue
ESEC_USER	EVENTS_ALL_RPT_V	193 SELECT	V Vue
ESEC_USER	EVENTS_ALL_RPT_V1	193 SELECT	V Vue
ESEC_USER	EVENTS_ALL_V	193 SELECT	V Vue
ESEC_USER	EVENTS_RPT_V	193 SELECT	V Vue
ESEC_USER	EVENTS_RPT_V1	193 SELECT	V Vue

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_USER	EVENTS_RPT_V2	193 SELECT	V Vue
ESEC_USER	EVT_AGENT_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_ASSET_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_DEST_EVT_NAME_SMRY_1	193 SELECT	V Vue
ESEC_USER	EVT_DEST_EVT_NAME_SMRY_1_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_DEST_SMRY_1	193 SELECT	V Vue
ESEC_USER	EVT_DEST_SMRY_1_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_DEST_TXNMY_SMRY_1	193 SELECT	V Vue
ESEC_USER	EVT_DEST_TXNMY_SMRY_1_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_NAME_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_PORT_SMRY_1	193 SELECT	V Vue
ESEC_USER	EVT_PORT_SMRY_1_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_PRTCL_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_RSRC_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_SEV_SMRY_1	193 SELECT	V Vue
ESEC_USER	EVT_SEV_SMRY_1_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_SRC_SMRY_1	193 SELECT	V Vue
ESEC_USER	EVT_SRC_SMRY_1_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_TXNMY_RPT_V	193 SELECT	V Vue
ESEC_USER	EVT_USR_RPT_V	193 SELECT	V Vue
ESEC_USER	EXTERNAL_DATA_RPT_V	193 SELECT	V Vue
ESEC_USER	HIST_CORRELATED_EVENTS	193 SELECT	V Vue
ESEC_USER	HIST_CORRELATED_EVENTS_RPT_V	193 SELECT	V Vue
ESEC_USER	HIST_EVENTS	193 SELECT	V Vue
ESEC_USER	HIST_EVENTS_RPT_V	193 SELECT	V Vue
ESEC_USER	IMAGES_RPT_V	193 SELECT	V Vue
ESEC_USER	INCIDENTS_ASSETS_RPT_V	193 SELECT	V Vue
ESEC_USER	INCIDENTS_EVENTS_RPT_V	193 SELECT	V Vue
ESEC_USER	INCIDENTS_RPT_V	193 SELECT	V Vue
ESEC_USER	INCIDENTS_VULN_RPT_V	193 SELECT	V Vue
ESEC_USER	L_STAT_RPT_V	193 SELECT	V Vue
ESEC_USER	LOGS_RPT_V	193 SELECT	V Vue
ESEC_USER	NETWORK_IDENTITY_RPT_V	193 SELECT	V Vue
ESEC_USER	ORGANIZATION_RPT_V	193 SELECT	V Vue
ESEC_USER	PERSON_RPT_V	193 SELECT	V Vue
ESEC_USER	PHYSICAL_ASSET_RPT_V	193 SELECT	V Vue
ESEC_USER	○PRODUCT_RPT_V	193 SELECT	V Vue
ESEC_USER	ROLE_RPT_V	193 SELECT	V Vue
ESEC_USER	SENSITIVITY_RPT_V	193 SELECT	V Vue
ESEC_USER	STATES_RPT_V	193 SELECT	V Vue
ESEC_USER	UNASSIGNED_INCIDENTS_RPT_V	193 SELECT	V Vue
ESEC_USER	USERS_RPT_V	193 SELECT	V Vue
ESEC_USER	VENDOR_RPT_V	193 SELECT	V Vue
ESEC_USER	VULN_CALC_SEVERITY_RPT_V	193 SELECT	V Vue
ESEC_USER	VULN_CODE_RPT_V	193 SELECT	V Vue
ESEC_USER	VULN_INFO_RPT_V	193 SELECT	V Vue
ESEC_USER	VULN_RPT_V	193 SELECT	V Vue

Nom du rôle	Nom de l'objet	Opération	Type
ESEC_USER	VULN_RSRC_RPT_V	193 SELECT	V Vue
ESEC_USER	VULN_RSRC_SCAN_RPT_V	193 SELECT	V Vue
ESEC_USER	VULN_SCAN_RPT_V	193 SELECT	V Vue
ESEC_USER	VULN_SCAN_VULN_RPT_V	193 SELECT	V Vue
ESEC_USER	VULN_SCANNER_RPT_V	193 SELECT	V Vue

Rôles du serveur Sentinel

Rôle serveur	Description	Utilisateur de Sentinel
sysadmin	Administrateurs système	esecdba
securityadmin	Administrateurs de sécurité	esecapp
serveradmin	Administrateurs du serveur	esecdba
setupadmin	Administrateurs de la configuration	
processadmin	Administrateurs des processus	
diskadmin	Administrateurs de disque	
dbcreator	Créateurs de la base de donnée	
bulkadmin	Administrateurs d'insertion en bloc	

Utilisateurs de la base de données d'authentification de domaine et autorisations d'accès correspondantes

Un utilisateur de domaine est associé à un utilisateur esecadm, esecapp, esecdba ou esecrpt en fonction de la configuration définie à l'installation. Ces utilisateurs de domaine disposent des mêmes privilèges que ceux mentionnés dans les sections précédentes de ce document

D Tableaux des autorisations requises pour les services Sentinel

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

Sentinel Server (moteur de corrélation)

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Autorisations requises	Précisions sur les autorisations requises
Sentinel Server	-	Sentinel/ WatchDog.exe	correlation_engine.exe	Le processus 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.	Accès au réseau et accès en lecture aux fichiers de configuration modifiés	Le serveur communique avec Sonic pour la configuration et la génération des processus d'événement et des événements corrélés. Un accès aux fichiers est requis lorsque vous utilisez un fichier de configuration modifié.

Gestionnaire des collecteurs

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Type de connecteur	Autorisations requises	Précisions sur les autorisations requises
Sentinel Wizard / Gestionnaire des collecteurs	-	Gestionnaire des collecteurs	agentengine.exe	Le processus du Gestionnaire de collecteur gère les moteurs du collecteur (il génère de façon dynamique les processus du moteur du collecteur), publie des messages sur le statut du système, filtre l'ensemble des événements et procède à des assignations de référence. Un processus du moteur du collecteur exécute les scripts d'un collecteur, ce qui permet de normaliser les événements non traités (bruts) provenant de périphériques et de systèmes de sécurité.	**REMARQUE** : le Gestionnaire des collecteurs requiert des autorisations d'accès différentes selon le type de connexion.		
					Serial : données lues sur un port série RS-232C	Accès en lecture/écriture à un port série	Le moteur du collecteur peut lire et écrire sur un port série
					Socket : connexion par socket TCP	Accès au réseau : accès en lecture/écriture à partir d'un socket réseau ; autorisation d'accès permettant de démarrer une connexion	Le moteur du collecteur démarre une connexion à un point limite du réseau et peut lire et écrire sur un socket.
					File New (fichier actualisé) : lit uniquement les données d'événement de sécurité qui ont été ajoutées au fichier après le démarrage du script (lit à partir de la fin du fichier).	Accès au fichier en lecture/écriture	Le moteur du collecteur lit les données du premier fichier spécifié et écrit dans le second.

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Type de connecteur	Autorisations requises	Précisions sur les autorisations requises	
					File All (tout le fichier) : lit toutes les données d'événement de sécurité d'un fichier.		Accès au fichier en lecture/écriture	Le moteur du collecteur lit les données du premier fichier spécifié et écrit dans le second.
					Persistent Process (processus permanent) : lance un processus permanent lorsque le port a démarré ; permet la communication entre le collecteur assigné à ce port et une application externe via des états de réception et de transmission ; s'exécute sans arrêt tant que le port est actif.		Autorisation d'exécution du processus permanent défini. Remarque : si vous utilisez EventLog.exe en tant que processus permanent pour les consignations NT utilisant WMI, une autorisation d'accès à WMI doit être accordée au Gestionnaire des collecteurs.	Le moteur du collecteur exécute le processus spécifié selon le niveau d'autorisation en cours.

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Type de connecteur	Autorisations requises	Précisions sur les autorisations requises	
					Transient Process (processus temporaire) : permet la communication entre le collecteur assigné à ce port et une application externe via des états de réception et de transmission. Un processus temporaire peut être démarré à plusieurs reprises.	Autorisation d'exécution du processus temporaire défini	Le moteur du collecteur exécute le processus spécifié selon le niveau d'autorisation en cours.	
					SNMP : reçoit des trappes SNMP v1, v2 et v3.	Accès au réseau : accès en lecture/écriture à partir d'un socket réseau	Le Gestionnaire des collecteurs envoie et reçoit des trappes SNMP.	
					Aucun	Néant	Néant	
Sentinel Wizard / Générateur de collecteurs	Générateur de collecteurs	-	agentbuilder.exe	Interface utilisateur permettant de créer, configurer et contrôler les collecteurs. Cette interface peut être utilisée pour exécuter des collecteurs locaux ou pour contrôler des collecteurs se trouvant sur les systèmes d'assistants distants.	Accès au fichier en lecture/écriture		Le Générateur de collecteurs lit et écrit des scripts de collecteur dans %WORKBENCH_HOME%/Elements.	
					Accès au fichier en lecture/écriture		Le Générateur de collecteurs lit et écrit dans des fichiers de configuration de port sous %WORKBENCH_HOME%/Agents.	

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Type de connecteur	Autorisations requises	Précisions sur les autorisations requises	
					Accès au fichier en lecture			Le Générateur de collecteurs est autorisé à accéder à %ESEC_HOME%/.uuid.
					Accès au réseau : accès en lecture/écriture à partir d'un socket réseau ; autorisation d'accès permettant de démarrer une connexion.			Le Générateur de collecteurs télécharge des collecteurs et reçoit des messages rendant compte de l'état du Gestionnaire des collecteurs.

Sentinel Communication

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Autorisations requises	Précisions sur les autorisations requises
iSCALE / MOM	SonicMQ	Serveur de communication Sentinel	sonicmf.exe	Pour Windows, le composant de communication Sentinel est considéré comme un service et apparaît sous le nom de iSCALE, intergiciel orienté message (MOM). Le composant iSCALE constitue un framework Java Message Service (JMS) destiné à la communication interprocessus. Les processus communiquent par l'intermédiaire d'un courtier responsable du routage et de la mise en mémoire tampon des messages. Plusieurs courtiers peuvent communiquer entre eux pour passer à travers des pare-feu ou équilibrer la charge. Les processus Sentinel utilisent un mécanisme de type publier/s'abonner pour communiquer entre eux. Cela permet à un processus de	Autorisations d'accès à la base de données, au répertoire d'installation (%ESEC_HOME%\3rdparty\SonicMQ) et aux fichiers intégrés de l'application	Sonic dispose d'un accès à la base de données, au répertoire d'installation (%ESEC_HOME%\3rdparty\SonicMQ) et aux fichiers intégrés à l'application.

				publier un message vers un sujet utilisé par plusieurs abonnés sans que le processus de publication ne sache quel processus s'est abonné. De même, les abonnés peuvent recevoir les messages publiés sans savoir quel sont les canaux Éditeur disponibles. Ce mécanisme permet de réduire les manipulations de configuration et de renforcer la stabilité et l'évolutivité du système. Par exemple, lorsqu'un nouvel assistant est ajouté au système, aucune configuration n'est requise au niveau de Sentinel. Le processus de publication publie les messages vers des sujets (canaux) tandis que les processus d'abonnement s'abonnent à ces sujets. Le courtier de messages se charge ensuite du routage des messages entre la publication et l'abonnement en fonction des sujets que ces deux processus ont enregistrés.		

Serveur de base de données (sans DAS)

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Autorisations requises	Précisions sur les autorisations requises
-	-	-	-	Configuration de la base de données Sentinel	-	Le pilote ODBC ou Oracle doit pointer vers la base de données Sentinel.

Serveur de base de données (avec DAS)

Pour un récapitulatif et une liste des autorisations d'accès de la base de données Sentinel, reportez-vous au document suivant :
Annexe A : Autorisations d'accès, rôles et utilisateurs de la base de données Sentinel

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Autorisations requises	Précisions sur les autorisations requises
-	-	-	-	Configuration de la base de données Sentinel	-	Le pilote ODBC ou Oracle doit pointer vers la base de données Sentinel.
Sentinel Server	-	Sentinel/ WatchDog.exe	das_binary	Opérations d'insertion d'événements corrélés ou pas	Accès au réseau ; une autorisation d'accès à la base de données est requise pour l'instance ESEC en tant que ESECAPP.	Le serveur communique avec le composant Sonic. Il communique également avec la base de données Sentinel par le biais de l'interface JDBC (Java DataBase Connectivity) lorsqu'il s'agit d'extraire des données et par l'intermédiaire d'ADO (ActiveX Data Object) lorsqu'il s'agit d'insérer des événements (uniquement si la stratégie de chargement ADO est configurée).

Pour un récapitulatif et une liste des autorisations d'accès de la base de données Sentinel, reportez-vous au document suivant :
Annexe A : Autorisations d'accès, rôles et utilisateurs de la base de données Sentinel

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Autorisations requises	Précisions sur les autorisations requises
			das_query	Toutes les autres opérations de base de données	Accès au réseau ; une autorisation d'accès à la base de données est requise pour l'instance ESEC en tant que ESECAPP ; des autorisations d'exécution des processus sont requises.	Le serveur communique avec le composant Sonic. Il communique également avec la base de données Sentinel par le biais de l'interface JDBC pour l'extraction de données.
			activity_container	Service d'exécution et de configuration des activités	Accès au réseau ; une autorisation d'accès à la base de données est requise pour l'instance ESEC en tant que ESECAPP ; des autorisations d'exécution des processus sont requises.	Le serveur communique avec le composant Sonic. Il communique également avec la base de données Sentinel par le biais de l'interface JDBC pour l'extraction de données et les opérations d'insertion.
			workflow_container	Configuration du service de workflow (iTRAC)	Accès au réseau ; une autorisation d'accès à la base de données est requise pour l'instance ESEC_WF en tant que ESECAPP ; des autorisations d'exécution des processus sont requises.	Le serveur communique avec le composant Sonic. Il communique également avec la base de données Sentinel par le biais de l'interface JDBC pour l'extraction de données et les opérations d'insertion.
			das_rt	Configuration de la fonction Active Views dans Sentinel Control Console	Accès au réseau ; une autorisation d'accès à la base de données est requise pour l'instance ESEC en tant que ESECAPP.	Le serveur communique avec le composant Sonic. Il communique également avec la base de données Sentinel par le biais de l'interface JDBC pour l'extraction de données.

Outils de création de rapports

Composant Sentinel	Application Sentinel	Service Sentinel	Processus Sentinel	Bref descriptif de la fonction	Autorisations requises	Précisions sur les autorisations requises
-	-	-	-	Outils de création de rapports fonctionnant avec Sentinel : Crystal Reports XI ou Crystal Enterprise 9 édition Standard	-	Le pilote ODBC ou Oracle doit pointer vers la base de données Sentinel.

Glossaire

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

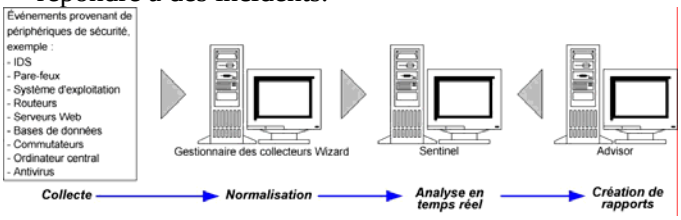
Création d'une règle de corrélation avancée	Permet de créer une règle de corrélation qui intègre toutes les fonctionnalités de la règle de corrélation simple et envoie un événement lorsque, dans un groupe d'événements, les événements n'ont pas les mêmes valeurs de balise META (exemple : capteur à l'intérieur ou à l'extérieur du pare-feu). 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 voudrait dire que l'attaque a réussi à traverser le pare-feu).
Advisor	Il s'agit d'un système intégré doté d'une base de données de vulnérabilités SecurityNexus capable de faire le lien entre les événements qui se produisent et les vulnérabilités connues.
Agent	Voir Collecteur
Générateur d'agents	Voir Générateur de collecteurs
Moteur d'agent	Voir Moteur du collecteur
Gestionnaire d'agents	Gestionnaire de collecteurs
Regroupement et normalisation d'événements	Le regroupement est le processus qui consiste à rassembler des éléments de données isolés peu importants pour les transformer en un seul élément de données d'importance supérieure. Individuellement, les différentes parties de l'événement telles que le nom de l'événement, la date à laquelle il s'est produit, les IP de source et de destination, l'UUID, le type de capteur, etc. n'ont pas nécessairement de signification particulière. Cependant, leur regroupement permet de créer un événement potentiellement intéressant puisqu'il permet de révéler l'existence d'une attaque sur le réseau, attaque pouvant déboucher sur l'utilisation abusive de l'actif d'une entreprise. La sauvegarde d'un événement dans son intégralité entraîne le stockage d'informations en double. Par exemple, dans un système ne fonctionnant pas par regroupement, lorsque dix événements identiques où seule la date diffère se produisent, ils sont tous les dix sauvegardés séparément alors que leurs éléments

	de données (nom de l'événement, type de capteur, etc.) sont parfaitement similaires. Le regroupement permet de sauvegarder tous les événements dont les éléments de données sont identiques une seule fois et d'en effectuer le décompte pendant une heure. Les données d'événements sont transformées, récapitulées et stockées dans des tables de récapitulatifs. Les rapports sur les récapitulatifs peuvent ensuite être exécutés en fonction de ces récapitulatifs précalculés, ce qui permet de réduire les conflits d'accès dus aux nombreuses requêtes lancées sur les tables d'événements en temps réel. Le moteur de regroupement d'événements récupère les données d'événements binaires, les transforme en événements de structure normalisée qu'il récapitule en fonction d'un ensemble de définitions récapitulées prédéfinies. Le moteur de regroupement d'événements traite les événements en temps quasi réel avec un impact minimal sur le système Sentinel fonctionnant en temps réel.
Analyse	Dans le Centre de contrôle Sentinel, l'option d'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. Ils apparaissent sur les onglets Analyse et Advisor de la barre du navigateur du Centre de contrôle.
Gestion des actifs	L'objectif de la gestion des actifs est de relier un ou plusieurs événements à des actifs et à des informations sur la vulnérabilité et, ainsi, de constituer une méthode efficace de protection des actifs d'une entreprise. Il existe deux types d'actifs : les actifs physiques et les actifs logiciels. Les actifs physiques correspondent au matériel informatique tandis que les actifs logiciels sont les services et les applications.
Séquences de retour à l'état antérieur	Voir Séquences
Règle de corrélation de base	Cette règle permet de sélectionner une balise META pour créer une règle de corrélation capable de compter le nombre de fois que certaines 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, tels qu'un système de détection d'intrusion ou un pare-feu.

Données d'entreprise Voir Service d'assignation

CorrelatedEventUUID Identificateur de l'événement corrélé généré par la règle qui s'est déclenchée.

Collecteur Un collecteur est un récepteur qui récupère et normalise des événements bruts provenant de périphériques et de systèmes de sécurité, et qui génère des événements normalisés. Ces événements peuvent ensuite faire l'objet de corrélations et de rapports et être utilisés pour répondre à des incidents.



Il existe trois niveaux de collecteur :

- les collecteurs pris en charge (T1)
- les collecteurs documentés (T2)
- les collecteurs d'exemples (T3)

Ils sont constitués des fichiers suivants :

- fichiers de modèle
- fichiers de paramètres
- fichiers de recherche
- fichiers d'assignation

Générateur de collecteurs Interface graphique permettant de créer des collecteurs fonctionnant selon des règles. Ces collecteurs doivent récupérer, filtrer et normaliser des données provenant de sources diverses et communiquer de manière sécurisée les informations importantes à Sentinel Server de sorte qu'elles puissent être utilisées pour surveiller le trafic.

Moteur du collecteur Traite la logique de modèle pour chaque port et exécute le port correspondant à ce modèle.

Gestionnaire des collecteurs Interface dorsale de l'assistant qui gère les collecteurs et les messages de statut du système.

Corrélation	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. Grâce à la corrélation, les tendances ou les modèles qui se dessinent pour des événements de niveau inférieur et conçus pour fonctionner en-dessous des seuils de sécurité peuvent être repérés de manière plus efficace. Sentinel propose cinq types de règles de corrélation. Ces types sont les suivants : ▪ Liste de surveillance ▪ Corrélation de base ▪ Corrélation avancée ▪ RuleLg de format libre
Moteur de corrélation	Le moteur de corrélation analyse les événements entrants pour y rechercher des modèles pertinents et examiner plus en détails les événements de corrélation afin de déterminer les éléments qui ont déclenché la règle.
Processus Correlation Engine (correlation_engine)	Le processus 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 Data Access Service (DAS)	Le processus DAS (Data Access Service) constitue le service de persistance de Sentinel Server et fournit une interface de bus message (iSCALE) à la base de données. Il permet un accès régi par les données à la base de données principale. Le service DAS reçoit les requêtes XML 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 au format XML. Il prend en charge les requêtes d'extraction d'événement pour l'interrogation rapide et la hiérarchisation vers le bas vers les événements, les requêtes d'extraction des informations de vulnérabilité et des informations Advisor et les requêtes de manipulation des informations de configuration. 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.
das_aggregation.xml	Fichier utilisé lors de l'opération de regroupement.

das_binary.xml	Fichier utilisé pour les opérations d'insertion d'événements corrélés ou non.
das_itrac.xml	Fichier utilisé pour l'exécution et la configuration du service d'activités ainsi que pour la configuration du service de flux de travail.
das_query.xml	Indique les paramètres de configuration pour le processus DAS (Data Access Service), un composant de la base de données Sentinel.
das_rt.xml	Indique la configuration de la fonction Actives Views dans le centre de contrôle Sentinel.
Contrôleur des données	Voir Processus Data Synchronizer
Processus Data Synchronizer (contrôleur des données)	Le processus data_synchronizer gère les modifications de données de configuration apportées par les 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.
Événement	Un événement est une action ou une occurrence détectée par un périphérique de sécurité (événement externe) ou un processus de sécurité (événement interne). Les événements peuvent être liés à la sécurité, aux performances ou aux informations. Un événement externe peut être une attaque détectée par un système de détection d'intrusion, une connexion réussie signalée par un système d'exploitation ou une situation définie par le client (par exemple, un utilisateur qui accède à un fichier). Les événements internes sont des événements liés aux informations système. Ils peuvent indiquer un changement dans l'état d'un processus (l'arrêt d'un port, par exemple).

Configuration d'événements

La configuration d'un événement fait partie du service d'assignation et permet d'activer les éléments suivants :

- le contrôle de la conformité aux réglementations ;
- la conformité à la stratégie ;
- l'attribution d'une priorité aux réponses ;
- l'analyse des données de sécurité en fonction des activités de l'entreprise ;
- le renforcement des responsabilités.

La configuration des événements consiste à assigner des noms à des intitulés existants. Par exemple, elle permet de renommer la balise Ct2 pour qu'elle apparaisse sous le nom de City. Ces modifications se répercutent sur les filtres et les règles de corrélation.

Numéro d'ID d'événement

Numéro assigné à un événement.

Normalisation d'événements

Voir Regroupement

Routeur d'événements

Le routeur d'événements effectue l'assignation, la transformation et le filtrage des événements.

Événement en temps réel

Le traitement en temps réel est une fonctionnalité permettant de surveiller les événements à mesure qu'ils se produisent et de lancer des requêtes relatives à ces événements. Vous pouvez les surveiller au moyen d'une table ou d'un graphique 3-D.

Détection d'exploitation

Voir Service d'assignation

Moteur de filtre

Voir Processus Event Performance

Filtres

Les filtres Sentinel permettent de traiter des données en fonction de critères spécifiques relatifs à des événements entrant dans le système et à des utilisateurs du système. Plusieurs niveaux de filtrage sont disponibles :

- Collecteur : appliqué par script à l'aide du Générateur de collecteurs.
- Filtre global : appliqué à tous les événements générés par tous les assistants du système. Seuls les événements passant par les filtres globaux sont envoyés vers tous les processus Sentinel.
- Filtre de sécurité : appliqué aux utilisateurs actifs. Ces filtres limitent les événements auxquels un utilisateur actif peut accéder. Ils sont assignés par l'administrateur.
- Filtre d'affichage : appliqué aux vues de l'interface. Ces filtres permettent à l'utilisateur de définir ses propres fenêtres d'événement pour une analyse en temps réel. Ils sont appliqués par chaque utilisateur.

Les types de filtre sont au nombre de deux :

- Public : il s'agit de filtres qui 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.
- Privé : il s'agit de filtres propres à l'utilisateur. Ce sont des filtres d'affichage, partageables, à condition de disposer de l'autorisation View Private Filters (Affichage de filtres privés).

Moteur de filtre

Voir Processus Event Performance

Incidents

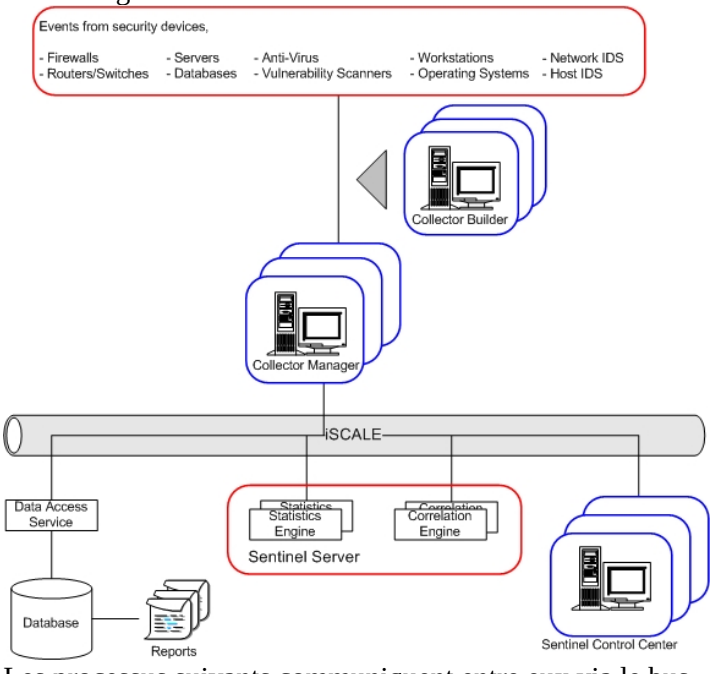
Regroupements des événements en ensembles présentant un intérêt particulier (un groupe d'événements similaires ou un ensemble d'événements différents qui correspondent à un sujet particulier, par exemple une attaque).

Événements internes

Voir Événements système

iSCALE™

Le bus message fournit un framework Java Message Service (JMS) destiné à la communication interprocessus. Les processus communiquent par l'intermédiaire d'un courtier responsable du routage et de la mise en mémoire tampon des messages. Plusieurs courtiers peuvent communiquer entre eux pour passer à travers des pare-feu ou équilibrer la charge.



Les processus suivants communiquent entre eux via le bus message.

- Watchdog
- Event Performance (moteur de filtre)
- Event Counts Over Time (moteur de statistiques)
- Data Synchronizer (contrôleur des données)
- Correlation Engine
- RuleLg Checker (vérificateur de règle de corrélation)
- Data Access Service (DAS)
- Query Manager

iTRAC™

iTRAC implique l'automatisation des procédures et permet de faire face à des incidents. Sentinel propose un système de gestion des flux de travail qui permet d'automatiser le processus SANS Incident Handling dans le cadre de procédures. Les éléments constitutifs principaux du système iTRAC sont les suivants :

- Worklist Handler : application utilisée pour passer d'une activité à l'autre.
- Activity Builder : application utilisée pour personnaliser le système iTRAC.
- Process Monitor : dispositif qui surveille les activités (étapes) nécessaires au bon déroulement d'un processus.

Fichiers de recherche

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

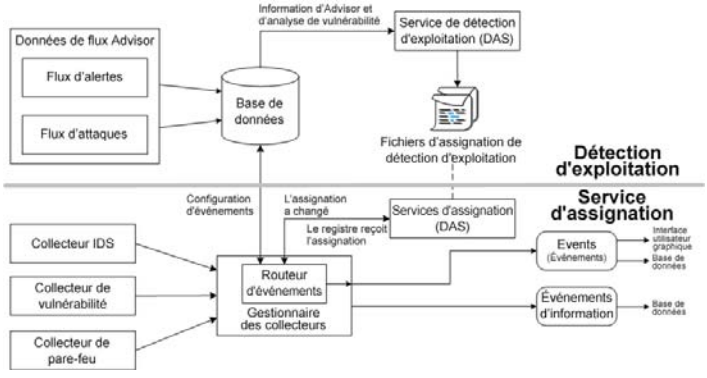
Éventuellement, des commandes d'analyse peuvent être associées à la chaîne recherchée. Ces commandes d'analyse sont exécutées si une correspondance est trouvée.

Fichiers d'assignation

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

Service d'assignation

Le service d'assignation Sentinel active des notifications entraînant une action immédiate pour des attaques subies par des systèmes vulnérables. Il fournit un lien en temps réel entre les événements et les résultats d'analyse de vulnérabilité, de sorte que les utilisateurs sont automatiquement et immédiatement informés lors d'attaques tentant d'exploiter les systèmes vulnérables. En améliorant ainsi considérablement l'efficacité de la réponse aux incidents, la disponibilité des systèmes critiques se trouve renforcée et le coût de la sécurité réduit.



Intergiciel orienté message (MOM)

Voir iSCALE™

MOM (Message Oriented Middleware)

Voir iSCALE™

Métadonnées

Les métadonnées sont des informations sur les données, des noms de variables prédéfinies pour les métadonnées. Par exemple, l'IP source d'une attaque est stocké dans la balise META SourceIP et les noms de produit sont stockés dans la balise META ProductName. Les données utilisées pour renseigner les balises META sont soit extraites des données d'événement soit définies dans le cadre du traitement du collecteur.

Balise META

Les balises META stockent les métadonnées.

Fichiers de paramètres

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

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

Les valeurs d'un fichier de paramètres peuvent être :

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

Commande d'analyse

Dans le module Wizard, cette commande est une interface de script de niveau élevé qui permet de manipuler les données. L'analyse consiste à décomposer un événement composant par composant.

Port

Dans le module Wizard, les ports permettent au collecteur de localiser les données d'événement de sécurité sur le réseau, car ils fournissent l'adresse IP de la source ainsi que d'autres informations (périphérique de sécurité [routeur, IDS, commutateur, etc.]). Chaque ligne de la table de configuration exécute un script de collecteur par source d'événement.

Processus Query Manager (query_manager)

Le processus query_manager reçoit les requêtes d'interrogation rapide et de hiérarchisation vers le bas du Centre de contrôle Sentinel et les transmet à la base de données par l'intermédiaire du processus DAS. Les requêtes du Centre de contrôle Sentinel déterminent les événements requis au moyen de critères ou d'un filtre. Si un filtre est utilisé, le Gestionnaire des requêtes extrait la définition du filtre et convertit le filtre au format XML. Le processus envoie ensuite la requête à la base de données. Les filtres ne peuvent pas tous être convertis au format XML. 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 au format XML, le Gestionnaire des requêtes convertit ce qu'il peut, puis génère un critère XML moins restrictif qui renvoie un surensemble 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.

Requête rapide

Voir Query Manager

Rx Buffer

Élément constitutif du Gestionnaire des collecteurs. Par défaut, il a une capacité de 50 000 événements. Le tampon de réception est un paramètre modifiable. Sa taille minimale est de 5 000 événements.

Pointeur Rx Buffer

Le pointeur Rx Buffer pointe vers les octets de données du tampon de réception. Avant chaque évaluation de chaîne de décision, le pointeur est réinitialisé sur sa valeur d'origine (normalement zéro).

Processus RuleLg Checker (rulelg_checker)

Le processus rulelg_checker valide les 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.

Fichier de script

Dans le module Wizard, le fichier de script est un fichier compilé (*.asd) qui contient le fichier de modèle du collecteur, le fichier de paramètres, le fichier de recherche et le fichier d'assignation.

Centre de contrôle Sentinel

Le Centre de contrôle Sentinel est la console de gestion centrale permettant d'afficher les récapitulatifs d'événement, les rapports d'historique, les événements en temps réel du filtre et de créer des incidents. Ce centre permet : d'afficher les événements en temps réel ; d'obtenir une présentation système des modifications survenues dans les activités déclenchées au moyen de paramètres définis dans les collecteurs ; d'administrer les filtres ; de générer des rapports ; de gérer les règles de corrélation, les filtres globaux et les événements de sécurité via les incidents.

Sentinel Server

Sentinel Server reçoit les informations d'événements normalisées récupérées par les collecteurs auprès du Gestionnaire des collecteurs Wizard. Il établit des corrélations entre les événements pour rechercher des modèles pertinents, identifier des menaces et des rapports en fonction des données en temps réel ainsi que des informations d'historique qui peuvent être consultées dans le Centre de contrôle Sentinel.

Séquences (démarrage et retour à l'état antérieur)

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

- Type de connexion
- Nom du processus
- Informations de socket
- Informations SNMP
- Nom des fichiers d'entrée/sortie
- Nom du collecteur

Séquences de démarrage

Voir Séquences

Moteur de statistiques

Voir Processus Event Counts Over Time

Événements 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 d'état du système. Ils signalent les cas où un utilisateur se connecte ou ne parvient pas à s'authentifier, 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.

Fichiers de modèle

Pour les collecteurs, vous pouvez créer des modèles, y insérer des états, modifier et supprimer ces modèles. Ces derniers déterminent la façon dont les enregistrements sont traités. La plupart des décisions concernant les modèles ont à voir avec le type des enregistrements utilisés et leur format. Il existe un fichier de modèle équivalent à ces fichiers qui porte l'extension .tem.

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

Lors de son insertion dans un modèle, un état se voit assigner un numéro qu'il conserve, quel que soit son emplacement dans le modèle par la suite.

Visualisation des vulnérabilités

Cette fonctionnalité est une représentation graphique des données d'événements en temps réel relatives à des systèmes vulnérables. Vous pouvez l'activer pour un événement en cours ou pour un événement qui s'est produit à l'heure spécifiée.

Processus Watchdog

Watchdog est un processus Sentinel qui gère tous les autres processus Sentinel. Si un processus autre que Watchdog s'arrête, Watchdog le redémarre.

Règle de corrélation Liste de surveillance	Permet d'indiquer une chaîne de texte que le moteur de corrélation doit rechercher dans toutes les balises META de chaque événement entrant. Cette règle peut par exemple rechercher l'adresse IP source d'un pirate informatique et générer une alerte chaque fois que cette adresse IP est repérée dans un message d'événement.
Assistant	Le Générateur et le Gestionnaire de collecteurs sont des assistants.
Hôtes de l'assistant	Toute machine sur laquelle le Gestionnaire des collecteurs a été installé.
Flux de travail	Voir iTRAC™