Novell® Sentinel™

5.1.3

www.novell.com

Volume I – GUIDE D'INSTALLATION

07/07/06

Novell®

Mentions légales

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 pour ce produit ou d'autres produits Novell et pour obtenir des mises à jour, voir www.novell.com/documentation.

Marques de Novell

Pour connaître les marques commerciales Novell, voir la liste de marques déposées et marques de service de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Éléments tiers

Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.

Mentions légales tiers

Sentinel 5 peut contenir les technologies tiers suivantes :

- Apache Axis and Apache Tomcat, Copyright © 1999 to 2005, Apache Software Foundation. Pour plus d'informations, exclusions de garantie et limitations, voir http://www.apache.org/licenses/
- ANTLR. Pour plus d'informations, exclusions de garantie et limitations, voir http://www.antlr.org
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Pour plus d'informations, exclusions de garantie et limitations, voir http://www.bouncycastle.org.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, utility package. Copyright © Doug Lea. Utilisé sans les classes CopyOnWriteArrayList et ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, incorporant les travaux de droits d'auteur suivants : mars.cpp by Brian Gladman and Sean Woods. Pour plus d'informations, exclusions de garantie et limitations, voir 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 de Lesser GNU Public License. Pour plus d'informations, exclusions de garantie et limitations, voir http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, sous licence de Lesser General Public License disponible à l'adresse : 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 and/or Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Pour plus d'informations, exclusions de garantie et limitations, voir http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

  Java 2 Platform 2 peut aussi contenir les produits tiers suivants :

  - CoolServlets © 1999
  - DES and 3xDES © 2000 by 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 marque commerciale de Bigelow and Holmes.
- Taligent, Inc.
- IBM, dont certaines portions sont disponibles à l'adresse : http://oss.software.ibm.com/icu4j/

Pour plus d'informations sur ces technologies de fabricant tiers et leurs exclusions de garantie et limitations associées, voir : http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Pour plus d'informations, exclusions de garantie et limitations, voir http://www.java.sun.com/products/javabeans/glasgow/jaf.html et cliquez sur téléchargement > licence.
- JavaMail. Copyright © Sun Microsystems, Inc. Pour plus d'informations, exclusions de garantie et limitations, voir http://www.java.sun.com/products/javamail/downloads/index.html et cliquez sur téléchargement > licence.
- Java Ace, by Douglas C. Schmidt and his research group at Washington University and Tao (with ACE wrappers) by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine and Vanderbilt University. Copyright © 1993-2005. Pour plus d'informations, exclusions de garantie et limitations, voir http://www.cs.wustl.edu/~schmidt/ACE-copying.html et http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html.
- Java Authentication and Authorization Service Modules, sous licence de Lesser General Public License Pour plus d'informations, exclusions de garantie et limitations, voir http://free.tagish.net/jaas/index.jsp.
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Pour plus d'informations, exclusions de garantie et limitations, voir http://www.java.sun.com/products/javawebstart/download-jnlp.html et cliquez sur téléchargement > licence.
- Java Service Wrapper. Portions dont les droits d'auteurs sont protégés : Copyright © 1999, 2004 Tanuki Software and Copyright © 2001 Silver Egg Technology. Pour plus d'informations, exclusions de garantie et limitations, voir http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE. Copyright © 2002 to 2005, JIDE Software, Inc.
- jTDS, sous licence de Lesser GNU Public License. Pour plus d'informations, exclusions de garantie et limitations, voir http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, sous licence de Lesser GNU Public License. Pour plus d'informations, exclusions de garantie et limitations, voir http://web.ukonline.co.uk/mseries.
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Les portions du code ont les droits d'auteur protégés par divers organismes, qui se réservent tous les droits. Copyright © 1989, 1991, 1992 by Carnegie Mellon University; Copyright © 1996, 1998 to 2000, the Regents of the University of California; Copyright © 2001 to 2003 Networks Associates Technology, Inc.; Copyright © 2001 to 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. and Copyright © 2003 to 2004, Sparta, Inc. Pour plus d'informations, exclusions de garantie et limitations, voir http://net-snmp.sourceforge.net.
- The OpenSSL Project. Copyright © 1998-2004. the Open SSL Project. Pour plus d'informations, exclusions de garantie et limitations, voir http://www.openssl.org.
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, ancienne Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Sous licence de Apache Software License. Pour plus d'informations, exclusions de garantie et limitations, voir http://skinlf.dev.java.net/.
- Sonic Software Corporation. Copyright © 2003-2004. Le logiciel SSC contient un logiciel de sécurité sous licence de RSA Security, Inc.
- Tinyxml. Pour plus d'informations, exclusions de garantie et limitations, voir http://grinninglizard.com/tinyxmldocs/index.html

REMARQUE : Au moment de la publication de cette documentation les liens ci-dessus étaient actifs. Si éventuellement vous constatez que l'un des liens ci-dessus est interrompu ou que l'une des pages Web liées est inactive, veuillez contacter Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Préface

La documentation technique Sentinel est un guide d'opérations et de références générales. Cette documentation est destinée aux professionnels de la sécurité de l'information. Le texte de cette documentation a été conçu pour servir de source de référence sur Enterprise Security Management System de Sentinel. Une documentation supplémentaire est disponible sur le portail Web Sentinel :

La documentation technique Sentinel est composée de cinq volume différents. À savoir :

- Volume I – Guide d'installation Sentinel™ 5
- Volume II – Guide de l'utilisateur Sentinel™ 5
- Volume III – Guide de l'utilisateur de Sentinel™ 5 Wizard.
- Volume IV – Guide de référence de l'utilisateur Sentinel™ 5
- Volume V – Guide du logiciel d'intégration tiers Sentinel™

Volume I – Guide d'installation Sentinel

Ce guide explique comment installer les éléments suivants :

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

Volume II – Guide de l'utilisateur Sentinel

Ce guide traite des thèmes suivants :

- Opération de console Sentinel
- Fonctions Sentinel
- Architecture Sentinel
- Communication Sentinel
- Arrêt/Démarrage de Sentinel
- Estimation de la vulnérabilité
- Contrôle d'évènements
- Filtrage d'évènements
- Corrélation d'évènements
- Gestionnaire de données Sentinel
- Configuration d'évènements pour la pertinence des activités
- Service d'assignation
- Création de rapports historiques
- Gestion d'hôte de Wizard
- Incidents
- Cas
- Gestion d'utilisateur
- Processus de travail

Volume III – Guide de l'utilisateur de Wizard

Ce guide traite des thèmes suivants :

- Opération du générateur de collecteurs de Wizard
- Gestionnaire de collecteurs de Wizard
- Collecteurs
- Gestion d'hôte de Wizard
- Construction et maintenance de collecteurs

Volume IV – Guide de référence de l’utilisateur Sentinel

Ce guide traite des thèmes suivants :

- Langue de script de Wizard
- Commandes d’analyse de Wizard
- Fonctions administratives de Wizard
- Meta-balises de Wizard et de Sentinel
- Autorisations d’utilisateur
- Moteur de corrélation Sentinel
- Options de ligne de commande de corrélation
- Schéma de la base de données Sentinel

Volume V – Guide du logiciel d'intégration tiers Sentinel

- Remedy
- HP OpenView Operations
- HP Service Desk

Sommaire

1 Introduction

REMARQUE : le terme « agent » est échangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Ce guide va vous accompagner lors de l'installation de base. Le *guide de l'utilisateur Sentinel™ 5* contient une architecture et des procédures administratives et opérationnelles plus détaillées.

Ce guide part du principe que vous êtes déjà familiarisé avec la sécurité de réseaux, l'administration de bases de données, les systèmes d'exploitation Windows et UNIX.

Conventions utilisées

Remarques et avertissements

REMARQUE : les remarques fournissent des informations supplémentaires qui peuvent être utiles.

ATTENTION : les avertissements fournissent des informations supplémentaires qui peuvent vous éviter d'endommager ou de perdre des données sur votre système.

Commandes

Les commandes apparaissent en police Courier. Par exemple :

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

Présentation de Sentinel 5

Sentinel 5 élève le niveau d'exigence quant à une solution de gestion d'informations de sécurité. Sentinel 5 comprend des capacités de gestion d'informations de sécurité standard

comme collecter, regrouper, relier et afficher les données d’évènements. Il vous permet aussi de donner une réponse décisive et adaptée à certains incidents, en automatisant et en mettant en oeuvre des processus d'identification et de résolution d'incidents.

Les fonctionnalités clés du Sentinel 5 sont iTRAC™, Active Views™ et iSCALE™. Elles vous permettent de gérer, mesurer et d'assurer votre conformité de façon plus efficace. Avec Sentinel 5, vous pouvez :

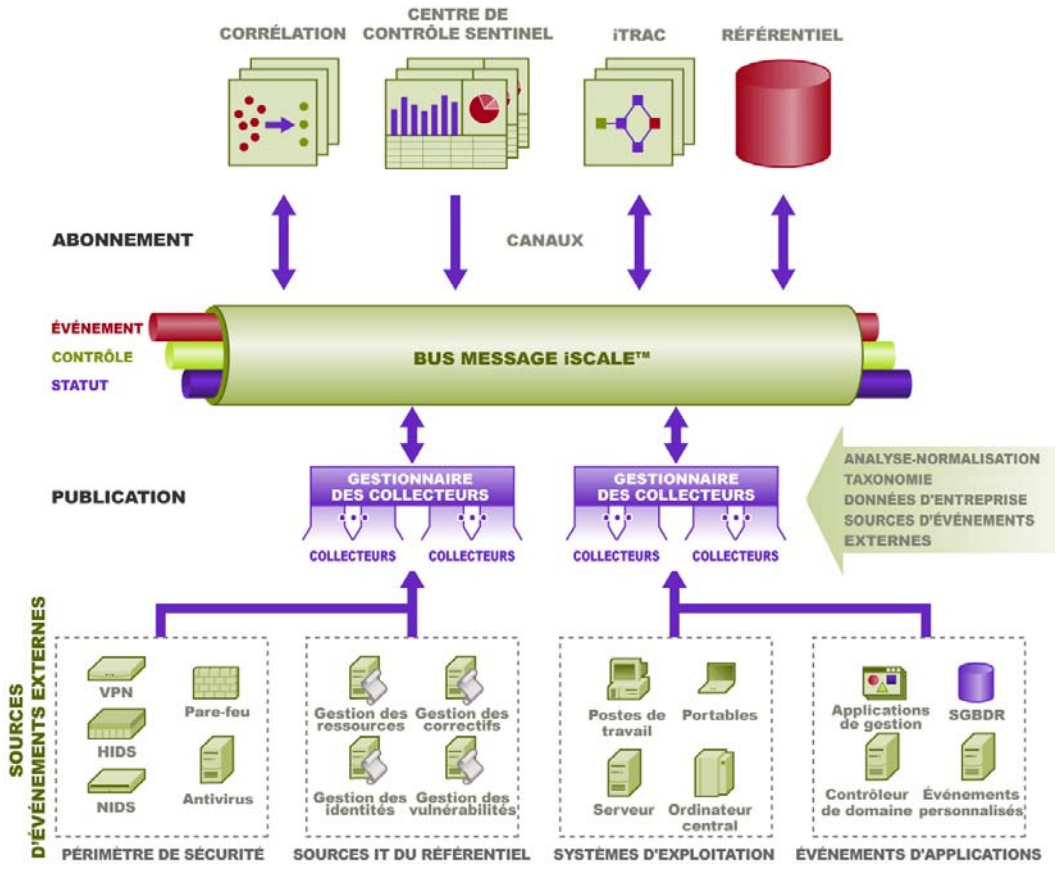
- obtenir la visibilité et le contrôle nécessaires pour gérer votre environnement de sécurité de façon plus avantageuse sur le plan financier.
- détecter et résoudre plus rapidement les incidents, en réduisant les coûts d'exploitation.
- fournir les rapports et mesures appropriés pour une évaluation permanente de votre position en matière de sécurité et conformité
- accomplir et contrôler la conformité avec les normes internes et légales.

Obtenir plus de résultats avec vos ressources actuelles en éliminant des processus manuels.

Le Sentinel 5 comprend plusieurs composants qui travaillent ensemble pour constituer la solution leader sur le marché.

- Sentinel Control Center
- Serveur Sentinel
- Sentinel Advisor
- gestionnaire de données Sentinel
- Sentinel Wizard
  - générateur de collecteurs de l’assistant
  - gestionnaire de collecteurs de l’assistant
  - moteur d’assistant

Vous trouverez ci-dessous l'**architecture conceptuelle** du produit Sentinel 5, qui présente les composants de Sentinel assurant la gestion de la sécurité.



Modules du produit Sentinel

Sentinel 5 est composé de trois modules principaux – Sentinel Control Center, Sentinel Wizard (générateur de collecteurs e gestionnaire de collecteurs) et Sentinel Advisor.

Sentinel Control Center

Sentinel Control Center fournit un tableau de bord intégré de gestion de la sécurité qui permet aux analystes d'identifier rapidement les nouvelles tendances ou menaces, de manipuler et d'interagir en temps réel avec l'information graphique et de répondre aux incidents.
Les fonctionnalités clés de Sentinel Control Center comprennent :

- Active Views – diagnostics et visualisation en temps réel
- Incidents – création et gestion d'incidents
- Admin.– définition et gestion des règles de corrélation
- iTRAC – gestion de processus pour documenter, appliquer et suivre les processus de résolution d'incidents
- Création de rapport – rapports et métriques historiques

Sentinel Wizard

Sentinel Wizard collecte les données des périphériques source et fournit un flux d'évènements plus riche en ajoutant une classification, une détection d'exploit et une pertinence des activités dans le flux de données, avant que l'évènement ne soit relié, analysé et transmis à la base

de données. Un flux d'évènements plus riche signifie que les données sont reliées au contexte d'activités demandé, pour identifier et réparer les menaces et violations internes ou externes des normes. Dans toute configuration, un ou plusieurs assistants peuvent être développés, ce qui donne aux clients la possibilité de développer les composants de produit dans leur infrastructure sur la base de leur topologie réseau.

L'assistant Sentinel Wizard vous permet de développer et de personnaliser des collecteurs, de façon efficace. Cela permet à Sentinel de collecter des données à partir de plusieurs périphériques différents dans une entreprise. Ces périphériques consistent en (mais ne sont pas limités à) :

- systèmes de détection d'intrusion (hôte)
- systèmes de détection d'intrusion (réseau)
- pare-feux
- systèmes d'exploitation
- surveillance de stratégie
- authentification
- routeurs & commutateurs
- VPN
- anti-Virus
- serveurs Web
- bases de données
- macro-ordinateur
- estimation de la vulnérabilité
- services Annuaire
- gestion réseau
- systèmes propriétaires

Les principaux composants de Sentinel Wizard comprennent :

- collecteur – un récepteur qui collecte et normalise les évènements non traités (bruts) à partir des périphériques et des systèmes de sécurité.
- Collector Engine – composant traitant la logique de modèle pour chaque port.
- Gestionnaire de collecteurs – le composant de l'interface dorsale qui gère les collecteurs et les messages sur l'état du système et qui réalise le filtrage global des évènements.
- Générateur de collecteurs – une application indépendante qui vous permet de construire et de configurer des collecteurs.

Sentinel Advisor

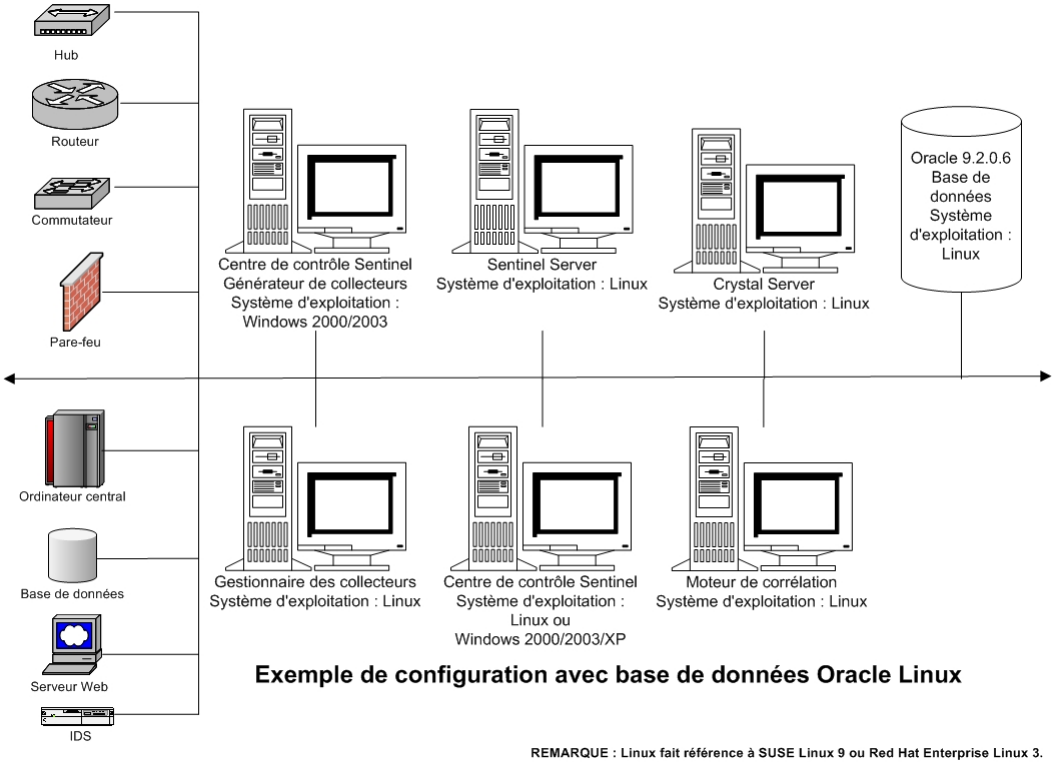
Sentinel Advisor est un module ajouté facultatif qui compare les données d'alerte en temps réel de Sentinel avec les vulnérabilités et les informations de solution déjà connues.

Configuration type

Vous trouverez ci-dessous les configurations types du produit Sentinel 5, qui présentent la façon dont la gestion de la sécurité est assurée. Votre application peut être différente, en fonction du lieu et du mode de votre installation.

REMARQUE : pour plus d'informations concernant les EPS (évènements par seconde), plates-formes, RAM, espace nécessaire sur le disque dur et UC, voir le *chapitre 2 – Bonnes pratiques*.

Plates-formes prises en charge pour le serveur Sentinel sous Linux



Exemple de configuration avec base de données Oracle Linux

REMARQUE : Pour des systèmes d'exploitation spécifiques, consultez les tableaux suivants :

Serveur Sentinel		
SE	**Version**	**Niveau de correctif**
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	Mise à jour 5 ES (x86)

Base de données		
Base de données	**Version**	**Niveau de correctif**
Oracle 64 bits Enterprise Edition	9i	▪ 9.2.0.6 2617419 ou ▪ 9.2.0.7

REMARQUE : Pour plus d'informations concernant le correctif critique 2617419, voir le site Web Oracle et le Novell Customer Portal.

Sentinel Control Center (interface utilisateur)		
SE	**Version**	**Niveau de correctif**
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Mises à jour 5 ES (x86)
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

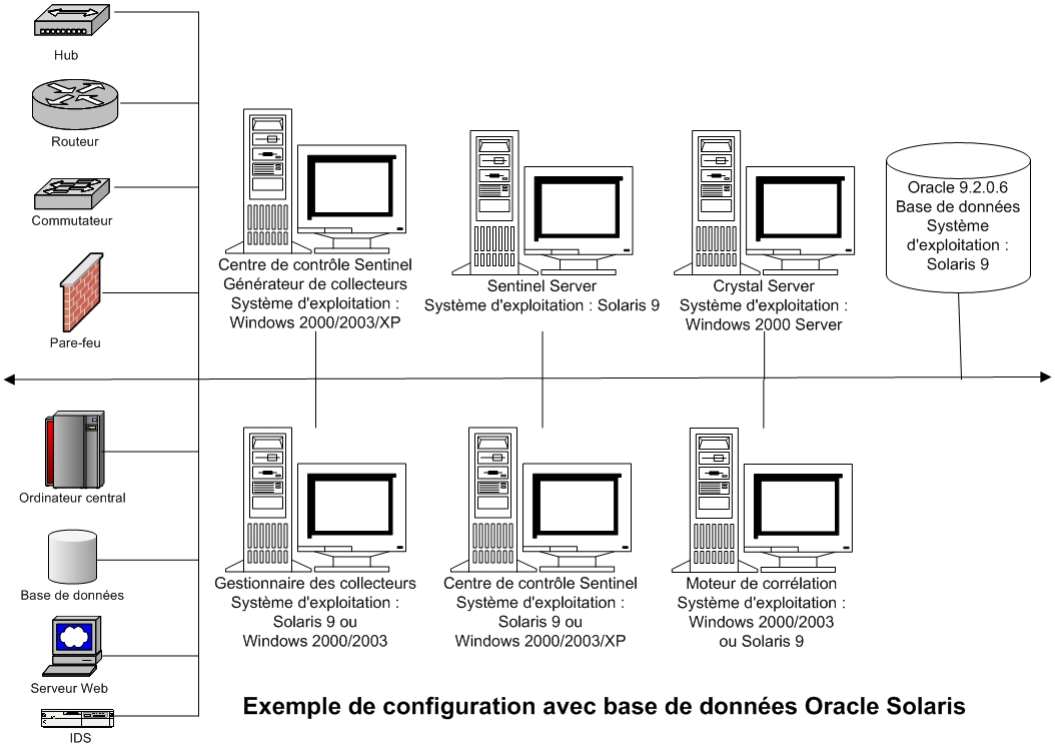
Générateur de collecteurs		
SE	**Version**	**Niveau de correctif**
Windows	2000	SP4
Windows	2003	SP1

Gestionnaire de collecteurs		
SE	**Version**	**Niveau de correctif**
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Solaris 9- grappe de correctifs recommandée DATE : 03/05/05
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Mises à jour 5 ES (x86)

Serveur Crystal (Deux versions au choix [Linux (SLES/Red Hat) et Windows])			
Version Crystal	**SE**	**Version SE**	**Niveau de correctif SE**
Crystal BusinessObjects Enterprise™ 11	SuSE Linux Enterprise Server 9 (SLES 9)	9	
Crystal BusinessObjects Enterprise™ 11	Red Hat Enterprise Linux	3	3 Mises à jour 5 ES (x86)
Crystal BusinessObjects Enterprise™ 11	Windows avec MS SQL 2000. Sentinel 5 ne prend pas en charge MSDE.	Windows 2003 Server	SP1

REMARQUE : Sentinel 5 ne prend pas en charge Crystal XI sur Windows® 2000 Server et MSDE.

Plates-formes prises en charge pour le serveur Sentinel sur Solaris



Exemple de configuration avec base de données Oracle Solaris

REMARQUE : Pour des systèmes d'exploitation spécifiques, consultez les tableaux suivants :

Serveur Sentinel		
SE	**Version**	**Niveau de correctif**
Solaris Enterprise Edition	9	Solaris 9- grappe de correctifs recommandée DATE : 03/05/05

Base de données		
Base de données	**Version**	**Niveau de correctif**
Oracle 64 bits	9i	▪ 9.2.0.6 2617419 ou ▪ 9.2.0.7

REMARQUE : pour plus d'informations concernant le correctif critique 2617419, voir le site Web Oracle et le Novell Customer Portal.

Sentinel Control Center (interface utilisateur)		
SE	**Version**	**Niveau de correctif**
Solaris	9	Solaris 9- grappe de correctifs recommandée DATE : 03/05/05
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1
Générateur de collecteurs		
SE	**Version**	**Niveau de correctif**
Windows	2000	SP4
Windows	2003	SP1

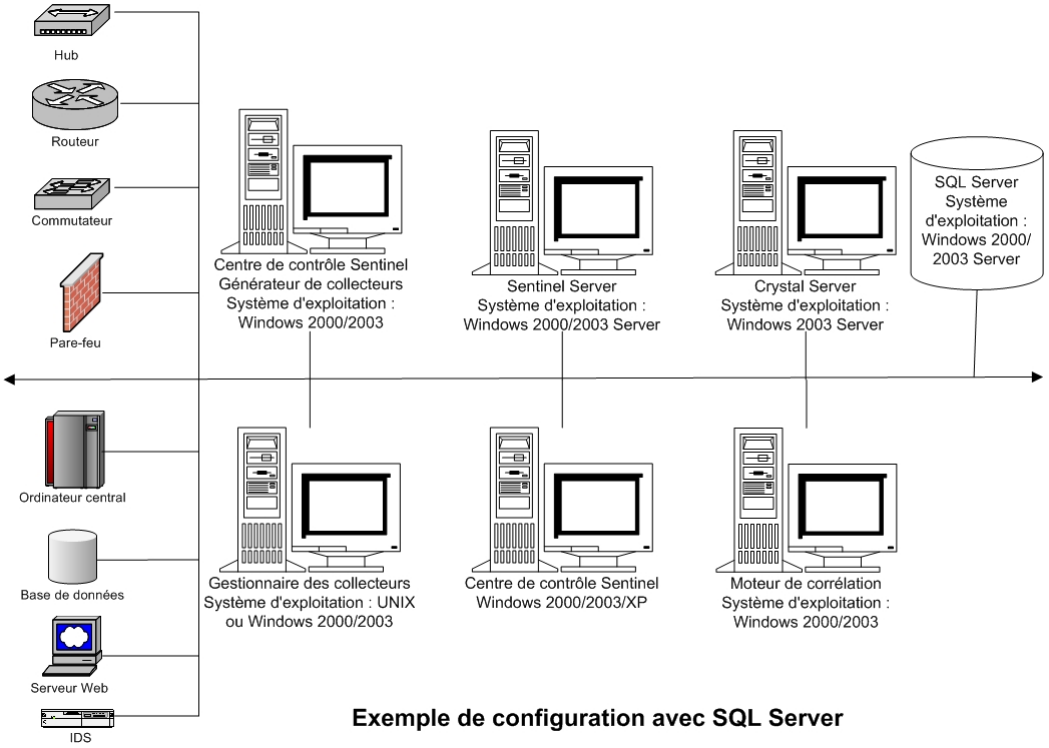
Générateur de collecteurs		
SE	**Version**	**Niveau de correctif**
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Solaris 9 - grappe de correctifs recommandée DATE : 03/05/05
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Mises à jour 5 ES (x86)

Serveur Crystal			
Version Crystal	**SE**	**Version SE**	**Niveau de correctif SE**
Crystal BusinessObjects Enterprise™ 11	Windows avec MS SQL 2000. Sentinel 5 ne prend pas en charge MSDE.	Windows 2003 Server	SP1

REMARQUE : Crystal Reports v9 est pris en charge sur Sentinel v5.1 et les versions antérieures ainsi que sur Sentinel v5.1.1 SP1 et les versions ultérieures. Il n'est pas pris en charge sur Sentinel v5.1.1 sans SP1. Si vous utilisez Crystal Reports v9 et Sentinel v5.1.1, vous devez appliquer Sentinel v5.1.1 Service Pack 1 ou la mise à niveau vers v5.1.2 ou v5.1.3.

REMARQUE : Sentinel 5 ne prend pas en charge Crystal XI sur Windows® 2000 Server.

Plates-formes prises en charges pour le serveur Sentinel sous Windows



Exemple de configuration avec SQL Server

REMARQUE : Pour des systèmes d'exploitation spécifiques, consultez les tableaux suivants :

Serveur Sentinel		
SE	**Version**	**Niveau de correctif**
Windows	2000 Server - Enterprise Edition	SP4
Windows	2003 Server - Enterprise Edition	SP1

Base de données		
Base de données	**Version**	**Niveau de correctif**
SQL Server	2000 Enterprise	SP3a
SQL Server	2005 Enterprise (Sentinel v5.1.1 SP1 et versions ultérieures)	

Sentinel Control Center (interface utilisateur)		
SE	**Version**	**Niveau de correctif**
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

Générateur de collecteurs		
SE	**Version**	**Niveau de correctif**
Windows	2000	SP4
Windows	2003	SP1

Gestionnaire de collecteurs		
SE	**Version**	**Niveau de correctif**
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Solaris 9 - grappe de correctifs recommandée DATE : 03/05/05
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Mises à jour 5 ES (x86)

Serveur Crystal			
Version Crystal	**SE**	**Version SE**	**Niveau de correctif SE**
Crystal BusinessObjects Enterprise™ 11	Windows avec MS SQL 2000. Sentinel 5 ne prend pas en charge MSDE.	Windows 2003 Server	SP1

REMARQUE : Crystal Reports v9 est pris en charge sur Sentinel v5.1 et les versions antérieures ainsi que sur Sentinel v5.1.1 SP1 et les versions ultérieures. Il n'est pas pris en charge sur Sentinel v5.1.1 sans SP1. Si vous utilisez Crystal Reports v9 et Sentinel v5.1.1, vous devez appliquer Sentinel v5.1.1 Service Pack 1 ou la mise à niveau vers v5.1.2 ou v5.1.3.

REMARQUE : Sentinel 5 ne prend pas en charge Crystal XI sur Windows® 2000 Server.

Autres références Novell

Les manuels suivants sont disponibles avec les CD d'installation Sentinel.

- Guide d'installation Sentinel™
- Guide de l'utilisateur Sentinel™
- Guide de l'utilisateur Sentinel™ Wizard
- Guide de références de l'utilisateur Sentinel™
- Guide du logiciel d'intégration tiers Sentinel™
- Notes de publication

Contacter Novell

- Site Web : http://www.novell.com
- Support technique Novell : http://www.novell.com/support/index.html
- Support technique international Novell : http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Support automatique : http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Pour obtenir un support technique 24h/24, appelez le 800-858-4000

2 Bonnes pratiques

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Ce chapitre traite des bonnes pratiques et des recommandations pour mieux utiliser Sentinel. Les thèmes traités sont les suivants :

- bonnes pratiques d'installation
  - configuration matérielle requise
  - configuration de pile de disques
  - configuration de réseaux
  - installation d'Oracle pour MS SQL Server
  - correctifs de la base de données Sentinel
  - paramètres Kernel recommandés pour UNIX
  - paramètres de configuration lors de la création de votre propre instance de la base de données
  - installation de Sentinel
  - maximisation de la création de rapport d'évènements pour Crystal Reports
  - rapports fournis par Sentinel
  - conseils pour le développement de Crystal Reports personnalisé
- maintenance des bonnes pratiques
  - analyse des bases de données
  - vérification de l'état de santé des bases de données
  - Archivage automatique des données et ajout des partitions (seulement Windows)
  - moteur de corrélation
  - journal de transactions
  - et emplacement des journaux

Bonnes pratiques d'installation

Vous trouverez ci-dessous les taux de performance des attributs spécifiques de Sentinel.

Attribut	Taux	Commentaires
▪ EPS pour insertion BD d'évènements	1250	L'insertion dépend des règles de corrélation et du service d'assignation
▪ EPS pour chaque gestionnaire de collecteurs	350	
▪ EPS par collecteur (Checkpoint, Win2K, etc.)	300	

Attribut	Taux	Commentaires
▪ Nombre maximum de collecteurs pris en charge par un gestionnaire de collecteurs	10	
▪ Nombre de règles déployées par moteur de corrélation	20-80	EPS bas(150 EPS) = 80 EPS haut (1 250 EPS) = 20
▪ Nombre d'Active Views™ par Sentinel	35 - 50	
▪ Nombre maximum d'utilisateurs simultanés	20	
▪ Nombre maximum de vues par Sentinel Control Center	10	
▪ Nombre maximum d'assignations par Sentinel	10	
▪ Taille maximale de chaque assignation	10 Mo	
▪ Nombre maximum de lignes par assignation	350 k	

La spécification de référence de l'unité centrale est basée sur :

- Windows - 3.2 GHz Xeon
- SuSE Linux - 3.2 GHz Xeon
- Solaris - 1.1 GHz Sparc-3
- Linux - 3.2 GHz Xeon

La configuration est destinée aux systèmes d'exploitation suivants :

- Windows 2000 Server avec SP4
- Windows 2003 Server avec SP1
- SuSE Linux Enterprise Server 9 (SLES 9)
- Solaris 9 avec correctifs avec la version générique_112233-11 de grappe de correctifs recommandée
- Red Hat Enterprise Linux 3 Mise à jour 5 ES (x86)

La base de données est une des suivantes :

- MSSQL 2000 avec SP3a
- Oracle 9i Enterprise Edition 9.2.0.6 ou 9.2.0.7 avec partitionnement

Configuration simple – indépendante (utilisation démo)

Cette installation installe tous les composants (y compris la base de données) sur une seule plate-forme. Elle sert surtout à des fins de démonstration. Elle n'est pas recommandée pour une utilisation réelle. La configuration matérielle requise est la suivante :

Composants	Minimum		Recommandé	
	RAM (Go)	Unité centrale	RAM (Go)	Unité centrale
Machine 1 ▪ tous les composants Sentinel ▪ gestionnaires de collecteurs ▪ collecteurs ▪ base de données ▪ pile de disques	2	2	4	2

Composants	Minimum		Recommandé	
	RAM (Go)	Unité centrale	RAM (Go)	Unité centrale
Machine 1 Pour Windows : ▪ Crystal Server ▪ générateur de collecteurs Pour Linux : ▪ Crystal Server	2	2	4	2
Machine 2 (pour installations UNIX seulement) Pour Solaris : ▪ Crystal Server ▪ générateur de collecteurs (Windows) Pour Linux : ▪ générateur de collecteurs (Windows)	1.0	1	2.0	2

Preuve de concept (POC) – Configuration indépendante

Cette installation installe tous les composants, sauf la base de données, sur une seule plate-forme. Cette configuration est normalement utilisée comme preuve de concept afin de tester la fonctionnalité sous des chargements normaux. Dans ce cas, la base de données est sur une autre machine séparée du reste de Sentinel.

Composants	Minimum		Recommandé	
	RAM (Go)	Unité centrale	RAM (Go)	Unité centrale
Machine 1 ▪ tous les composants Sentinel ▪ gestionnaires de collecteurs ▪ collecteurs Pour Windows : ▪ Crystal Server ▪ générateur de collecteurs Pour Linux : ▪ Crystal Server	4.0	2	4	4
Machine 2 ▪ base de données ▪ pile de disques	4	2	4	4

Composants	Minimum		Recommandé	
	RAM (Go)	Unité centrale	RAM (Go)	Unité centrale
Machine 3 (pour installations UNIX seulement) Pour Solaris : ▪ Crystal Server ▪ générateur de collecteurs (Windows) Sur Linux : ▪ générateur de collecteurs (Windows)	2.0	2	4.0	2

Production – Configuration distribuée

Une configuration distribuée est une installation personnalisée destinée aux systèmes standard et Enterprise.

Comme Sentinel possède 8 composants différents en plus de Crystal Reports, de nombreuses configurations différentes peuvent être construites. Vous trouverez ci-dessous deux configurations différentes.

Comme les bases de données dépendent des E/S, il est recommandé de placer la base de données sur une machine séparée. Le serveur BD requiert un tableau de stockage à grande vitesse qui correspond à la configuration requise des E/S, en fonction des taux d'insertion d'évènements.

Les hôtes distribués doivent être connectés aux autres hôtes du serveur Sentinel via un seul commutateur à grande vitesse (GIGE), afin d'éviter des encombrements de trafic des réseaux.

Production – Configuration distribuée (Option 1)

Configuration de 4 machines

Composants	Minimum		Recommandé	
	RAM (Go)	Unité centrale	RAM (Go)	Unité centrale
Machine 1 ▪ moteur de corrélation ▪ DAS ▪ iSCALE (Bus de Messages) ▪ Advisor	4.0	4	8.0	8
Machine 2 ▪ gestionnaire de collecteurs ▪ collecteurs	1.0	2	2.0	2
Machine 3 ▪ Crystal Server	2.0	2	4.0	4
Machine 4 ▪ base de données ▪ pile de disques	4	4	16	8

Production – Configuration distribuée (Option 2)

Configuration de 5 machines

Composants	Minimum RAM (Go)	Minimum Unité centrale	Recommandé RAM (Go)	Recommandé Unité centrale
Machine 1 ▪ DAS ▪ iSCALE (Bus de Messages) ▪ Advisor	4.0	4	8.0	8
Machine 2 ▪ moteur de corrélation	1.0	2	2.0	2
Machine 3 ▪ gestionnaire de collecteurs ▪ collecteurs	1.0	2	2.0	2
Machine 4 ▪ Crystal Server	2.0	2	4.0	4
Machine 5 ▪ base de données ▪ pile de disques	4	4	16	8

Stratégie de support de correctifs

Sentinel certifie les correctifs de systèmes d'exploitation et de bases de données dans un délai de 60 jours après qu'ils ont été libérés.

Recommandations matérielles

Serveur Sentinel Moteur de corrélation			
EPS	**RAM**	**Espace**	**Unité centrale**
250	2 Go	72 Go	Windows - 2 x 3.0 GHz XeonSuSE Linux ou Redhat Linux - 2 x 3.0 GHz Xeon Solaris - V280 2 x 1.1 GHz Ultra Sparc III
500	4 Go	72 Go	Windows - 4 x 3.0 GHz Xeon SuSE Linux ou Redhat Linux - 4 x 3.0 GHz Xeon Solaris - V480 4 x 1.1 GHz Ultra Sparc III
1000+	8 Go	72 Go	Windows - 8 x 3.0 GHz Xeon SuSE Linux ou Redhat Linux - 8 x 3.0 GHz Xeon Solaris - V880 8 x 1.1 GHz Ultra Sparc III

Gestionnaire de collecteurs			
EPS	**RAM**	**Espace**	**Unité centrale**
250	2 Go	36 Go	Windows - 2 x 3.0 GHz Xeon SuSE Linux ou Redhat Linux - 2 x 3.0 GHz Xeon Solaris - V280 2 x 1.1 GHz Ultra Sparc III
350+	4 Go	36 Go	Windows - 4 x 3.0 GHz Xeon SuSE Linux ou Redhat Linux - 4 x 3.0 GHz Xeon Solaris - V480 4 x 1.1 GHz Ultra Sparc III

Sentinel Control Center Générateur de collecteurs (seulement Windows) Gestionnaire de données Sentinel		
RAM	**Espace**	**Unité centrale**
2 Go	15 Go	Windows 2000 or 2003 - 2 x 3.0 GHz Xeon Windows XP (seulement Control Center) - 2 x 3.0 GHz Xeon SuSE Linux ou Redhat Linux - 2 x 3.0 GHz Xeon Sun Solaris 9 - V280 2 x 1.1 GHz Ultra Sparc III

Base de données			
EPS	**RAM**	**Espace**	**Unité centrale**
250	8 Go	500 Go	Windows - 4 x 3.0 GHz Xeon SuSE Linux ou Redhat Linux - 4 x 3.0 GHz Xeon Solaris - V480 4 x 1.1 GHz Ultra Sparc III
500	12 Go	1.0 To	Windows - 4 x 3.0 GHz Xeon SuSE Linux ou Redhat Linux - 4 x 3.0 GHz Xeon Solaris - V880 6 x 1.1 GHz Ultra Sparc III
1000+	16 Go	2,0 To	Windows - 8 x 3.0 GHz Xeon SuSE Linux ou Redhat Linux - 8 x 3.0 GHz Xeon Solaris - V880 8 x 1.1 GHz Ultra Sparc III

Configuration de pile de disques

Le serveur Novell Sentinel 5 dans une configuration de production requiert un pile de disques à grande vitesse pour la base de données et les hôtes sentinel. Cette section tente d'englober les recommandations de configuration type d’un disque (RAID). Vous trouverez ci-dessous les composants principaux affectés par la performance du matériel de disque :

- Composant de base de données (MSSQL/Oracle) : Le taux d’évènements par seconde (EPS) et les fonctions de recherche (performance rapide de recherche/Crystal) sont affectés.
- DAS-RT (Data Access Service Real Time Component) : La fonction Active View est affectée.
- Regroupement DAS : Le nombre de résumés qui peuvent être activés est influencé.

Conditions minimales pour l'installation Enterprise (1000 EPS ou plus)

La configuration minimum recommandée est l'utilisation de RAID 5. RAID 5 peut être le plus rentable. Cette configuration favorise la rentabilité, au détriment de la performance et de la redondance. Veuillez notez que ce ne sont que des recommandations à utiliser comme guide. La majorité des installations d'entreprise de production à grande échelle requiert une analyse plus détaillée des conditions requises de vitesse, de débit et de redondance.

- RAID Groupe 1 – BD (données, index, journaux des transactions, etc.)
- RAID Groupe 2 – DAS du serveur Sentinel (Data dir, Temp DIR*)
- disques minimums : 13 par groupe de RAID
- Type de disque : 12 k+ RPM, Fiber Channel ou SCSI
- LUN 1 (RAID Groupe 1) : 5 Go – 144 Go+ par disque
- LUN 2 (RAID Groupe 2) : 5 Go – 144 Go+ par disque

Configuration optimale

Pour une configuration optimale de performance et de redondance, un RAID 1+0 peut être utilisé avec les mêmes paramètres que ci-dessus. Cependant, d'autres groupes RAID et LUN peuvent s'avérer nécessaires selon les orientations indiquées ci-dessus, afin d'atteindre un degré plus élevé de parallélisme et de E/S pour certaines bases de données.

REMARQUE : Voir la section Installation Sentinel pour obtenir des instructions concernant la façon de cibler le REP TEMP DAS sur un emplacement différent.

Exemple d'une configuration de stockage pour une installation MS SQL

Cet exemple utilise le sous-système EMC^2 CLARiiON avec :

- 1 To de stockage
- 60 unités , 36 Go, 15 K RPM

Groupes RAID

Pile	Groupe RAID	Nombre d'unités	Unités assignées (bus-enclosure-disk)	Nom
1	0	8	0-0-13, 0-0-14, 1-0-13, 1-0-14, 2-0-13, 2-0-14, 3-0-13, 3-0-13	RAID Groupe 0
1	1	8	0-0-11, 0-0-12, 1-0-11, 1-0-12, 2-0-11, 2-0-12, 3-0-11, 3-0-12	RAID Groupe 1
1	2	8	0-0-9, 0-0-10, 1-0-9, 1-0-10, 2-0-9, 2-0-10, 3-0-9, 3-0-10	RAID Groupe 2
1	3	8	0-0-7, 0-0-8, 1-0-7, 1-0-8, 2-0-7, 2-0-8, 3-0-7, 3-0-8	RAID Groupe 3
1	4	8	0-0-5, 0-0-6, 1-0-5, 1-0-6, 2-0-5, 2-0-6, 3-0-5, 3-0-6	RAID Groupe 4
1	5	8	0-0-3, 0-0-4, 1-0-3, 1-0-4, 2-0-3, 2-0-4, 3-0-3, 3-0-4	RAID Groupe 5
1	6	12	0-0-0, 0-0-1, 0-0-2, 1-0-0, 1-0-1, 1-0-2, 2-0-0, 2-0-1, 2-0-2, 3-0-0, 3-0-1, 3-0-2	RAID Groupe 6

Assignations LUN

Pile	LUN	Type de RAID	Groupe RAID	Taille (Go)	Processeur de stockage	Nom
1	0	0	0	263	A	LUN 0
1	1	0	1	263	B	LUN 1
1	2	0	2	263	A	LUN 2
1	3	0	3	263	B	LUN 3
1	4	0	4	263	A	LUN 4
1	5	0	5	214	B	LUN 5
1	6	0	6	160	A	LUN 6
1	7	0	6	160	B	LUN 7

Groupes de stockage

Pile	Groupe de stockage	LUN	Hôte	Lettre d'unité	Nom
1	Sentinel	0	E2P0 (E3P0)	E :	SQLData1
1	Sentinel	1	E2P0 (E3P0)	F :	SQLData2
1	Sentinel	2	E2P0 (E3P0)	G :	SQLData3
1	Sentinel	3	E2P0 (E3P0)	H :	SQLData4
1	Sentinel	4	E2P0 (E3P0)	I :	SQLIndex1
1	Sentinel	5	E2P0 (E3P0)	J :	SQLIndex2
1	Sentinel	6	E2P0 (E3P0)	L :	SQLLog
1	Sentinel	7	E2P0 (E3P0)	T :	TempDB

Exemple d'une configuration de stockage pour une configuration Oracle

volume 1	RAID 1	Accueil Oracle
volume 2	RAID 1	journal de répétitions du membre a
volume 3	RAID 1	journal de répétitions du membre b
volume 4	RAID 0+1 ou RAID 5	espaces de table d'annulation et temporaire
volume 5	RAID 0+1 ou RAID 5	espaces de table de données Sentinel
volume 6	RAID 0+1 ou RAID 5	espaces de table d'index Sentinel
volume 7	RAID 0+1 ou RAID 5	espaces de table de données récapitulatifs Sentinel
volume 8	RAID 0+1 ou RAID 5	espaces de table d'index récapitulatifs Sentinel
volume 9	RAID 1	fichiers journaux de stockage

Configuration de réseaux

Composants sur le serveur Sentinel : Ils devraient être connectés les uns aux autres via un seul commutateur de 1 Go. Ils incluent la base de données, le serveur de communication, l'Advisor, les services de base Sentinel, le moteur de corrélations et le DAS.

Sentinel Control Center, le générateur de collecteurs et les services de collecteurs (gestionnaire de collecteurs) : Ils doivent être connectés au serveur Sentinel via des commutateurs FULL DUPLEX d'au moins 100 Mbits.

Installation d'Oracle et de MS SQL Server

REMARQUE : la majorité des paramètres d'installation de la base de données peut être modifiée après l'installation de la base de données via Enterprise Manager ou une ligne de commande.

1. Pour des raisons de performance, si vous installez en RAID et si l'environnement RAID le permet, les journaux suivants doivent être installés sur le disque d'écriture disponible le plus rapide.
   - journal de répétitions (Oracle)
   - journal de transactions (MS SQL)
2. Pour déterminer plus précisément la taille de la base de données, au début vous pouvez commencer par une petite base de données et agrandir sa taille une fois que le système est prêt et en cours exécution depuis peu. Ainsi, vous pouvez observer la croissance de la base de données en fonction du taux d'insertion d'évènements, pour déterminer l'espace requis du système pour la base de données.
3. À des fins de récupération, il est recommandé d'effectuer des sauvegardes régulièrement planifiées de la base de données.
4. Pour l'installation Oracle, le programme d'installation Sentinel par défaut désactive l'archivage de consignations. À des fins de récupération de la base de données, il est fortement recommandé d'activer l'archivage de consignations après l'installation et avant de commencer à recevoir les données d'évènements de production. Vous devriez aussi programmer la sauvegarde des archives de consignations pour libérer de l'espace dans le journal de stockage cible, sinon la base de données ne va plus accepter d'évènements lorsque le journal de stockage cible aura atteint sa capacité maximale.
5. Pour des raisons de performance, les emplacements de stockage doivent cibler des emplacements différents pour éviter des contentions E/S.
   - Répertoire de données Répertoire d'index récapitulatifs
   - Répertoire de journaux (seulement MS SQL)
   - Répertoire d'espaces de table temporaires et annulés (seulement Oracle)
   - Répertoire de journaux de répétitions du membre A (seulement Oracle)
   - Répertoire de journaux de répétitions du membre B (seulement Oracle)

Correctifs de la base de données Sentinel

Seulement pour MS SQL, lorsque les correctifs de la base de données Sentinel sont appliqués, le programme d'installation ne fait qu'ajouter de nouveaux index à *_P_MAX. Les partitions déjà existantes ne sont pas mises à jour. Vous devez ajouter manuellement les index aux partitions déjà existantes si vous voulez que les nouveaux index améliorent la performance des recherches exécutées sur les partitions existantes.

Paramètres Kernel recommandés pour UNIX

Vous trouverez ci-dessous des suggestions de valeurs minimums. Pour plus d'informations, voir la documentation concernant Oracle et le système.

Valeurs minimums des paramètres Kernel pour Linux

Pour plus d'informations sur la façon d'afficher et de définir les paramètres Kernel sous Linux, voir le *Chapitre 3, Installation de Sentinel 5 pour Oracle – Préinstallation d'Oracle sous Linux*.

```
shmmax=2147483648 (valeur minimum)
shmmni=4096
semmns=32000
semmni=1024
semmsl=1024
semopm=100
```

Valeurs minimums des paramètres Kernel pour Solaris

Vérifiez les paramètres Kernel pour Oracle dans /etc/system et configurez les éléments suivants :

```
shmmax=4294967295
shmmin=1
shmseg=50
shmmni=400
semmns=14000
semmni=1024
semmsl=1024
shmopm=100
shmvmx=32767
```

Paramètres de configuration lors de la création de votre propre instance de la base de données

Vous trouverez ci-dessous les paramètres recommandés lors de la création de votre propre instance de base de données. Les paramètres peuvent variés en fonction de la configuration et des conditions du système requises.

Dans l'instance Oracle, vous devez créer :

- les paramètres d'initialisation Oracle (ces valeurs varient en fonction de la taille et de la configuration du système)
- Paramètres de configuration d'espaces de tables requis par Sentinel pour Solaris et Linux.

Paramètres minimaux recommandés pour la configuration	
Paramètres	**Taille (octets ou tout autre indiqué)**
db_cache_size	1 Go
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 Mo
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAIRE
hash_join_enabled	VRAI
optimizer_index_caching	50
optimizer_index_cost_adj	55

Taille minimale recommandée pour les espaces de table		
Espace de table	**Taille exemple**	**Remarques**
REDO	3 x 100 M	▪ Valeur minimale. Vous devez créer des journaux de répétition plus grands si vous avez un EPS élevé.
SYSTEM	500 M	▪ Valeur minimum
TEMP	1 G	▪ Valeur minimum
UNDO	1 G	▪ Valeur minimum
ESENTD	5 G	▪ Valeur minimum ▪ Pour des données d'évènements
ESENTD2	500 M	▪ Valeur minimum ▪ Données pour configuration, actifs, vulnérabilité et associations (extension automatique activée)
ESENTWFD	250 M	▪ Pour données iTRAC (extension automatique activée)
ESENTWFX	250 M	▪ Pour index iTRAC (extension automatique activée)
ESENTX	3 G	▪ Valeur minimum ▪ Pour index d'évènements
ESENTX2	500 M	▪ Valeur minimum ▪ Index pour configuration, actifs, vulnérabilité et associations (extension automatique activée)
SENT_ADVISORD	200 M	▪ Valeur minimum ▪ Pour données Advisor (extension automatique activée)

Taille minimale recommandée pour les espaces de table		
Espace de table	**Taille exemple**	**Remarques**
SENT_ADVISORX	100 M	▪ Valeur minimum ▪ Pour index Advisor (extension automatique activée)
SENT_LOBS	100 M	▪ Valeur minimum ▪ Pour grands objets de base de données (extension automatique activée)
SENT_SMRYD	3 G	▪ Valeur minimum ▪ Pour regroupement, données récapitulatives
SENT_SMRYX	2 G	▪ Valeur minimum ▪ Pour regroupement, index récapitulatif

Installation de Sentinel

Pour des raisons de performance et de sauvegarde, lors de l'installation de Sentinel, vous devriez considérer les éléments suivants.

1. Si vous effectuez une nouvelle installation de Sentinel sur un ordinateur sur lequel une version précédente de Sentinel avait été installée, il est VIVEMENT recommandé de supprimer certains fichiers et paramètres de système de l'installation précédente. Si ces fichiers ne sont pas éliminés, la toute nouvelle installation peut échouer. Vous devriez le faire sur chaque machine où vous exécutez une nouvelle installation. Pour plus d'informations sur les fichiers à éliminer, voir *annexe E*.
2. La performance des vues actives et des assignations peut s'améliorer de façon significative en ciblant le répertoire temporaire des processus DAS_RT et DAS_Query vers un disque plus rapide (par ex, une pile de disque). Pour cibler le répertoire temporaire de ces processus vers un disque plus rapide, effectuez les tâches suivantes sur la machine où le DAS est installé :
   a. Créez un répertoire sur le disque rapide pour placer les fichiers temporaires. Si vous êtes sur UNIX, ce répertoire doit être accessible en écriture par l'utilisateur esecadm et le groupe esec et leur appartenir.
   b. Faites une copie de sauvegarde du fichier %ESEC_HOME%\configuration.xml.
   c. Ouvrez le fichier %ESEC_HOME%\configuration.xml dans un éditeur de texte :
   d. Pour les procesuss DAS_RT et DAS_Query, ajouter l'argument JVM java.io.tmpdir, en le configurant vers le répertoire que vous venez de créer.
   e. Pour effectuer cette modification au processus DAS_RT, cherchez la ligne contenant le texte

      ```
      -Dsrv_name=DAS_RT
      ```

      et ajoutez l'argument

      ```
      -Djava.io.tmpdir=<repertoire_tmp>
      ```

      juste après. Vous trouverez ci-dessous un exemple de l'aspect que la ligne doit avoir (vos arguments –Xmx, -Xms et –XX peuvent être différents) :

      ```
      <composant du processus ="DAS"
         image="&amp;quot;$(ESEC_JAVA_HOME)/java&amp;quot; -server -
         Dsrv_name=DAS_RT -Djava.io.tmpdir=D:\Temp2 -Xmx310m
         -Xms103m -XX:+UseParallelGC -Xss128k -Xrs -
      ```

```
Desecurity.dataobjects.config.file=/xml/BaseMetaDat
a.xml -
Djava.util.logging.config.file=../config/das_rt_log
.prop -
Dcom.esecurity.configurationfile=../../configuratio
n.xml -
Djava.security.auth.login.config=../config/auth.log
in -Djava.security.krb5.conf=../../lib/krb5.conf -
jar ../../lib/ccsbase.jar ..//config//das_rt.xml"
min_instances="1" post_startup_delay="5"
shutdown_command="cmd //C
&amp;quot;$(ESEC_HOME)/sentinel/scripts/stop_container.
bat&amp;quot; localhost DAS_RT"
working_directory="$(ESEC_HOME)/sentinel/bin"/>
```

f. Pour effectuer cette modification au processus DAS_RT, cherchez la ligne contenant le texte

`-Dsrv_name=DAS_Query`

et ajoutez l'argument

`-Djava.io.tmpdir=<répertoire_tmp>`

juste après. Vous trouverez ci-dessous un exemple de l'aspect que la ligne doit avoir (vos arguments –Xmx, -Xms et –XX peuvent être différents) :

```
<composant du processus ="DAS"
   image="&amp;quot;$(ESEC_JAVA_HOME)/java&amp;quot; -server -
   Dsrv_name=DAS_Query -Djava.io.tmpdir=D:\Temp2 -
   Xmx256m -Xms85m -XX:+UseParallelGC -Xss128k -Xrs -
   Desecurity.dataobjects.config.file=/xml/BaseMetaDat
   a.xml,/xml/WorkflowMetaData.xml -
   Djava.util.logging.config.file=../config/das_query_
   log.prop -
   Djava.security.auth.login.config=../config/auth.log
   in -Djava.security.krb5.conf=../../lib/krb5.conf -
   Desecurity.execution.config.file=../config/executio
   n.properties -
   Dcom.esecurity.configurationfile=../../configuratio
   n.xml -jar ../../lib/ccsbase.jar
   ..//config//das_query.xml" min_instances="1"
   post_startup_delay="5" shutdown_command="cmd //C
   &amp;quot;$(ESEC_HOME)/sentinel/scripts/stop_container.
   bat&amp;quot; localhost DAS_Query"
   working_directory="$(ESEC_HOME)/sentinel/bin"/>
```

Maximisation de la création de rapport d'évènements pour Crystal Reports

En fonction du nombre d'évènements consultés par Crystal, vous pouvez obtenir une erreur sur la durée maximale de traitement ou sur la limite maximale d'enregistrements. Pour configurer le serveur afin qu'il traite un nombre supérieur ou illimité de rapports, vous devez reconfigurer Crystal Page Server.

Reconfiguration de Crystal Page Server (seulement Windows Crystal Server)

1. Cliquez *Démarrer* > *Tous les programmes* > *BusinessObjects 11* > *Crystal Reports Server*> *Central Configuration Manager*.
2. Cliquez avec le bouton droit sur *Crystal Page Server* et sélectionnez *Arrêter*.
3. Cliquez avec le bouton droit sur *Crystal Page Server* et sélectionnez *Propriétés*.
4. Dans le champ Commande sous l'onglet Propriétés, à la fin de la ligne de commandes ajoutez :

   ```
   maxDBResultRecords <valeur supérieure à 20 000 ou 0
      pour désactiver la limite par défaut>
   ```

5. Redémarrez *Crystal Page Server*.

Reconfiguration de Crystal Page Server (serveurs Linux ou Windows Crystal Server)

1. Ouvrez un navigateur Web et entrez l'URL suivant :

   Pour serveurs Linux Crystal :

   ```
   http://<DNS ou IP de Crystal
      Server>:8080/businessobjects/enterprise11/
      adminlaunch
   ```

   Pour serveurs Windows Crystal :

   ```
   http://<nom DNS ou adresse IP de votre serveur Web>
      /businessobjects/enterprise11/WebTools/adminlaunch/
      default.aspx
   ```

2. Cliquez sur *Console de gestion centralisée*.
3. Le nom du système devrait être le nom de l'ordinateur hôte. Le type d'authentification devrait être Enterprise. Dans le cas contraire, choisissez Enterprise.
4. Entrez votre nom d'utilisateur, votre mot de passe et cliquez sur *Se loguer*.
5. Cliquez sur *Serveurs*.
6. Cliquez sur <*nom_serveur*>.*pageserver*.
7. Sous *Enregistrements de la base de données à lire à l'aperçu ou au rafraîchissement d'un rapport*, cliquez sur *Enregistrements illimités*.
8. Cliquez sur *Appliquer*.
9. Une invite pour redémarrer le serveur de pages s'affiche, cliquez sur *OK*.
10. L'invite peut vous demander un nom de login et le mot de passe pour accéder au gestionnaire de services du système d'exploitation.

Rapports fournis par Sentinel

1. Pour v5.1.1 SP1 et les versions utlérieures, les rechercher de Top 10 rapports regroupent les tables au lieu des tables d'évènements détaillées. Vérifiez que les services EventFileRedirectService et Regroupement (résumés) sont activés.

   EventFileRedirectService est localisé sur la machine DAS et peut être activer en éditant le fichier das_binary.xml.

   Les trois résumés qui doivent être activés sont :

   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   REMARQUE : Pour plus d'informations concernant EventFileRedirectService et les trois résumés de regroupement, voir le chapitre sur SDM dans le *guide d'utilisateur Sentinel* ou les chapitres sur l'installation Crystal dans le *guide d'installation Sentinel*.

2. Les rapports qui recherchent une grande plage de données peuvent être exécutés lentement. Ils devraient être planifiés au lieu d'être exécutés de façon interactive.

   REMARQUE : Pour plus d'informations concernant la planification de Crystal Reports, voir la Documentation *Crystal BusinessObjects Enterprise™ 11*.

Conseils pour le développement personnalisé de Crystal Reports

Pour des rapports développés sur le mode personnalisé, il est recommandé de/d' :

1. utiliser autant que possible des tables de regroupement.
2. Si les rapports peuvent utiliser des tables de regroupement prédéfinies, sélectionnez la table de regroupement qui aboutit au traitement de la plus infime quantité de données.
3. Essayez de pousser la plupart du traitement de données vers le moteur de la base de données.
4. Afin de réduire la surcharge du traitement sur Crystal server, minimiser la quantité de données à récupérer vers lui.

Maintenance de bonnes pratiques

Analyse de base de données pour Oracle

Comme les évènements sont insérés de façon continue dans la base de données Sentinel, les statistiques de la base de données devraient être mises à jour régulièrement pour assurer la bonne performance de la recherche. L'utilitaire d'analyse de la base de données met à jour les statistiques de la base de données pour les données d'évènements sous Oracle. Pour une performance optimale, cet utilitaire devrait être planifié pour une exécution régulière.

REMARQUE : Cet utilitaire inclut le script SQL requis qui peut être mis à jour périodiquement. Il est recommandé de vérifier périodiquement le Sentinel Customer Portal pour des mises à jour.

Le script de shell suivant devrait être exécuté régulièrement via cron ou tout autre planificateur :

- AnalyzePartitions.sh

Analyse de partitions

Le script AnalyzePartitions analyse les partitions récemment remplies. Ce script devrait être planifié tous les jours, afin d'actualiser les statistiques sur les partitions remplies la veille. Il est recommandé d'exécuter ce script deux heures après minuit, lorsque les évènement de la veille ont été insérés dans la base de données.

Ce script est localisé dans $ESEC_HOME/utilities/db. Il doit être exécuté localement sur le serveur où la base de données Sentinel est installée. Le compte utilisateur UNIX qui exécute le script doit pouvoir se connecter à la base de données comme sysdba (par ex, oracle).

REMARQUE : Si vous avez téléchargé une nouvelle version de cet utilitaire installé actuellement sur la machine, vous devez installer sp_esec_dba_utl.sql.

Installation sp_esec_dba_utl.sql

1. Loguez-vous comme propriétaire du logiciel Oracle.
2. À l'aide de SQL*Plus, effectuez une connexion à la base de données comme ESECDBA.
3. Installez le package ESEC_DBA_UTL. À l'invite SQL (SQL>), entrez :

   ```
   @sp_esec_dba_utl.sql
   ```

4. Quittez SQL*Plus.

Exécution d'AnalyzePartitions.sh

1. Sur la machine du serveur de base de données Oracle, cd vers :

   ```
   $ESEC_HOME/utilities/db/
   ```

   ou cd vers l'emplacement où vous avez téléchargé le dernier fichier.
2. À l'invite de commande, entrez :

   Pour Solaris :

   ```
   ./AnalyzePartitions.sh <ORACLE_SID> >> <LogFileName>
   ```

   Pour Linux :

   ```
   ksh ./AnalyzePartitions.sh <ORACLE_SID> >>
   <LogFileName>
   ```

   - ORACLE_SID - le nom de l'instance Oracle pour la base de données.
   - LogFileName - le nom de chemin complet vers le fichier où vous voulez que les messages journaux soient écrits.

   Si le script réussit, il ferme avec un code de renvoi de 0. S'il échoue, il ferme avec un code de renvoi de 1. Planifiez dûment les travaux pour chercher le code de renvoi. Si le travail d'analyse échoue, cherchez des messages d'erreur détaillés dans le fichier journal.

Vérification de l'état de santé de la base de données pour Oracle

dbHealthCheck.sh est un script qui réunit des informations sur la base de données Sentinel Oracle. Le script effectue les tâches suivantes :

- il vérifie que l'instance de la base de données est bien active
- il vérifie que le processus d'écoute Oracle est bien actif
- il affiche l'utilisation de l'espace
- il cherche des index inutilisables
- il cherche des objets de base de données invalides
- il cherche des analyses de base de données

Le script devra être exécuté régulièrement via cron ou tout autre planificateur :

REMARQUE : Cet utilitaire inclut le script SQL requis qui peut être mis à jour périodiquement. Il est recommandé de vérifier périodiquement le Sentinel Customer Portal pour des mises à jour.

Installation et exécution de dbHealthCheck.sh

REMARQUE : Si vous avez téléchargé une nouvelle version de cet utilitaire installé actuellement sur la machine, vous devez installer sp_esec_dba_utl.sql.

Installation sp_esec_dba_utl.sql

1. Loguez-vous comme propriétaire du logiciel Oracle.
2. Sur le serveur de la base de données, vérifiez que $ORACLE_HOME et $ORACLE_SID sont définis dans votre environnement.
3. À l'aide de SQL*Plus, effectuez une connexion à la base de données comme ESECDBA.
4. Installez le package ESEC_DBA_UTL. À l'invite SQL (SQL>), entrez :

   ```
   @sp_esec_dba_utl.sql
   ```

5. Quittez SQL*Plus.

Exécution dbHealthCheck.sh

REMARQUE : le script doit être exécuté en utilisant le compte de propriétaire du logiciel Oracle ou tout autre compte connecté « COMME SYSDBA ».

REMARQUE : dbHealthCheck.sh doit être exécuté localement sur le serveur de la base de données.

1. Sur le serveur de la base de données, vérifiez que $ORACLE_HOME et $ORACLE_SID sont définis dans votre environnement.
2. Sur la machine du serveur de base de données SQL, cd vers :

   ```
   $ESEC_HOME/utilities/db/
   ```

   ou cd vers l'emplacement où vous avez téléchargé le dernier fichier.
3. À l'invite de commande, entrez :

   Pour Solaris :

   ```
   ./dbHealthCheck.sh
   ```

Les informations sur la base de données Sentinel s'affichent sur l'écran ou vous pouvez écrire les résultats dans un fichier.

```
./dbHealthCheck.sh >> <nomfichier>
```

Pour Linux :

```
ksh ./dbHealthCheck.sh
```

Les informations sur la base de données Sentinel s'affichent sur l'écran ou vous pouvez écrire les résultats dans un fichier.

```
ksh ./dbHealthCheck.sh >> <nomfichier>
```

Stockage automatique des données et ajout de partitions (seulement Windows)

REMARQUE : Si la machine n'a pas d'accès aux DAS_Binary et DAS_Query, l'option ligne de commande SDM peut être utilisée au lieu de SDM GUI.

Cette procédure n'est applicable qu'à Windows. Vérifiez que pendant la pré-configuration et la configuration les opérations suivantes sont bien effectuées :

- assurez-vous que sdm.connect est initialisé en utilisant SDM GUI ou la ligne de commande ;
- assurez-vous que le répertoire d'archives existe ;
- assurez-vous que les dates archiveConfig et dropPartitions sont les mêmes ;
- Avant de le planifier pour l'exécution automatique, vérifiez au moins un fois que le fichier batch est exécuté correctement depuis une invite de commande.

REMARQUE : Si les tâches planifiées échouent, vous ne recevez pas de notification. Le fichier est alors enregistré dans SDM_*.log

Pré-configuration

Avant la configuration automatique de Archiver données et Ajouter partitions, vous devez :

- enregistrer les propriétés de connexion
- établir les paramètres d'archivage

Enregistrement des propriétés de connexion dans le gestionnaire de données Sentinel

Vous devez faire cela avant d'utiliser les options de ligne de commande du gestionnaire de données Sentinel. Pour enregistrer la connexion (saveConnection) dans le gestionnaire de données Sentinel, vous devez exécuter la ligne de commande SDM avec l'action saveConnection.

Si vous avez exécuté le SDM GUI, vous pouvez utiliser le fichier sdm.connect créé à partir du GUI. Il est localisé à %ESEC_HOME%\sdm.

L'action saveConnection enregistre les détails de la connexion au connectFile. Le keyStore référencié dans le fichier configuration.xml est utilisé pour codifier le mot de passe avant de l'enregistrer dans le connectFile.

Les options de ligne de commande suivantes pour l'action saveConnection sont disponibles pour définir les détails de connexion.

-action	saveConnection
-server	Mssql
-host	<adresse IP hôte de la base de données ou nom d'hôte pour se connecter à>
-port	<numéro de port de la base de données pour se connecter à[SQL Server par défaut : 1433]>
-database	<nom de la base de données/SID pour se connecter à>
-user	<nom d'utilisateur de la base de données>
-password	<mot de passe de la base de données>
-winAuth	Utilisé pour l'authentification Windows. Si vous utilisez cette option, vous ne pouvez pas utiliser -user et –password
-connectFile	<nom de fichier où les détails de connexion sont enregistrés [nom de fichier au choix]>

L'application enregistre dans le fichier indiqué tous les détails de connexion mentionnés ci-dessus avec le mot de passe codifié. L'application utilise les détails de connexion enregistrés pour exécuter les autres opérations de ligne de commande SDM. Cette étape devrait être accomplie la première fois que vous démarrez l'application et chaque fois que vous voulez changer les détails de connexion.

Exécution saveConnection

1. Exécutez la commande suivante :

```
sdm -action saveConnection -server <oracle/mssql> -host
   <IpHôte/NomHôte> -port <numPort> -database
   <nomBaseDonnées/SID> [-driverProps
   <fichierPropriétés>] {-user <dbUser> -password
   <motPasseBD> | -winAuth} -connectFile
   <nomFichierPourEnregistrerConnexion>
```

   L'exemple suivant enregistre les détails de connexion dans le fichier sdm.connect pour la base de données nommée esec sur un hôte à l'adresse IP 172.16.0.36 et au port 1433 authentifiant comme utilisateur esecdba.

```
sdm -action saveConnection -server mssql -host
   172.16.0.36 -port 1433 -database esec -user esecdba
   -password XXXXXX -connectFile  sdm.connect
```

   L'exemple suivant d'authentification Windows enregistre les détails de connexion dans le fichier sdm.connect pour la base de données nommée esec_51 sur un hôte à l'adresse IP 172.16.1.3 et au port 1433 authentifiant à l'aide de l'authentification Windows.

```
sdm -action saveConnection -server mssql -host
   172.16.1.3 -port 1433 -database esec_51 –winAuth -
   connectFile  sdm.connect
```

Cette opération enregistre les détails de connexion dans le fichier sdm.connect. Toutes les autres opérations de ligne de commande prennent ce nom de fichier comme entrée, afin d'établir une connexion à la base de données désignée pour effectuer leurs opérations.

REMARQUE : Si vous avez créé un fichier de connexion à un emplacement ou avec un nom différent de celui indiqué dans l'exemple, vous devez éditer le fichier manage_data.bat.

Établissement des paramètres d'archivage

Il peut être fait à l'aide de la ligne de commande suivante :

Cette opération (archiveConfig) est utilisée pour configurer l'archivage. Cette configuration contrôle la façon dont les données sont archivées depuis les tables de la base de données Sentinel.

Cette opération utilise les drapeaux suivants :

-action	archiveConfig
-dirPath	<chemin de répertoire valide pour écrire les fichiers archivés dans>
-keepDays	<nombre de jours de conservation>
-connectFile	<chemin vers le nom de fichier enregistré par « saveConnection »>

Établissement des paramètres d'archivage via la ligne de commande

1. Créez un répertoire de sortie d'archive à la racine dénommée SDM_archive (c:\SDM_archive).

   REMARQUE : si vous avez créé un répertoire ou un emplacement de sortie différent, vous devez éditer le fichier manage_data.bat.

2. Exécutez la commande suivante :

   ```
   sdm -action archiveConfig  -dirPath <chemin
      de répertoire pour enregistrer les fichiers
      archivés> -keepDays <nombre de jours de
      conservation> -connectFile <chemin vers le nom
      de fichier enregistré par « saveConnection »>
   ```

   L'exemple suivant archive toutes les données datant de plus de 30 jours vers le répertoire c:\SDM_archive.

   ```
   sdm -action archiveConfig –dirpath c:\SDM_archive -
      keepDays 30 -connectFile sdm.connect
   ```

Établissement des paramètres d'archivage via GUI

1. Créez un répertoire de sortie d'archives à la racine dénommée SDM_archive (c:\SDM_archive).

   REMARQUE : si vous avez créé un répertoire ou un emplacement de sortie différent, vous devez éditer le fichier manage_data.bat.

2. Le SDM GUI ne requiert pas de paramètre d'archives. GUI peut archiver directement les données sans qu'il soit nécessaire d'établir des paramètres d'archive.

Supprimer les données (abandonner partitions)

Cette opération (deleteData) supprime les données datant de plus de « keepDays » dans les tables suivantes :

- EVENTS
- CORRELATED_EVENTS

Par défaut, cette opération n'abandonne aucune partition non archivée. Si vous voulez supprimer les partitions non archivées, le drapeau facultatif « forceDelete » doit être défini avec une valeur de vrai (true). Si forceDelete est utilisé :

false or not specified	il n'abandonne que les partitions archivées datant de plus de keepDays. il ne supprime pas les partitions non archivées, même si elles datent de plus de keepDays.
true	il abandonne toutes les partitions datant de plus de keepDays, y compris les partitions non archivées.

Cette commande utilise les drapeaux suivants :

-action	deleteData
-keepDays	<nombre de jours de conservation>
[-forceDelete]	<vrai ou faux>
-connectFile	<chemin vers le nom de fichier enregistré par « saveConnection »>

Exécution deleteData

1. Exécutez la commande suivante :

```
sdm -action deleteData -keepDays <nombre de jours
   de conservation> -connectFile <chemin vers
   le nom de fichier enregistré par « saveConnection »>
```

L'exemple suivant abandonne les partitions des tables EVENTS et CORRELATED_EVENTS qui datent de plus de 30 jours, assurant que toutes les partitions abandonnées sont archivées. À la fin, il liste toutes les partitions qui n'ont pas été éliminées si elles n'avaient pas été archivées.

```
sdm -action deleteData -keepDays 30 -connectFile
   sdm.connect
```

Planification du stockage de données et de l'ajout de partitions

REMARQUE : Le fichier manage_data.bat est configuré avec une valeur keepDay de 30 jours, les archives de sortie vers c:\SDM_archive et le fichier de connexion vers %ESEC_HOME%\SDM\sdm.connect. Si vos valeurs sont différentes, vous devez éditer le fichier manage_data.bat.

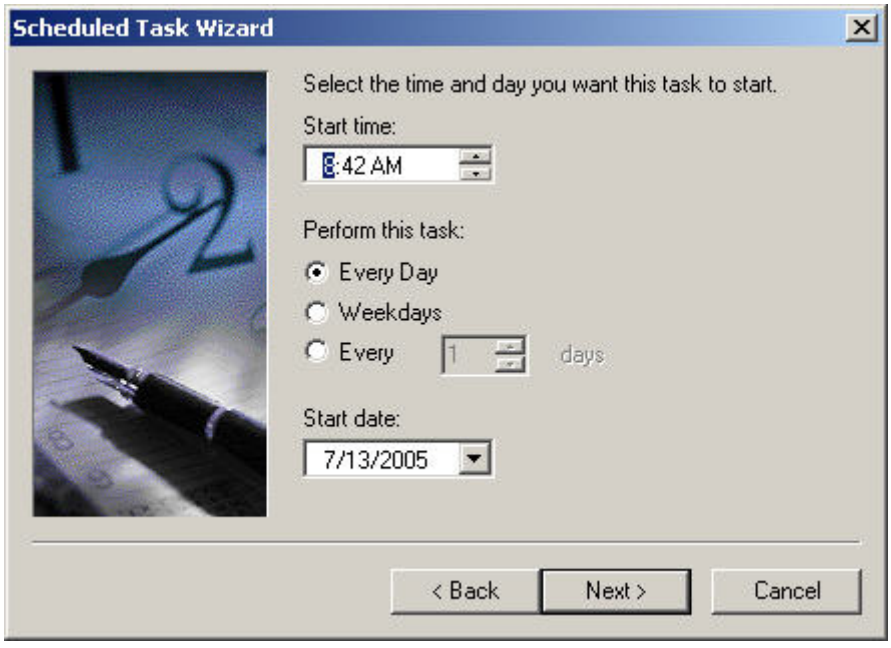
Vous devez configurer les propriétés de connexion et les paramètres d'archives, puis exécuter le manage_data.bat sur une invite de commande pour vérifier que tout fonctionne.

Pour archiver automatiquement des données et ajouter des partitions

REMARQUE : Les étapes suivantes sont destinées à Windows 2000 Professional. Les étapes pour Windows 2000 Server, XP et 2003 Server peuvent varier mais elles sont similaires.

1. Sous Windows, cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration*.
2. Double-cliquez sur *Tâches planifiées*.
3. Double-cliquez sur *Ajouter tâches planifiées*. Cliquez sur *Suivant.*
4. Cliquez sur *Parcourir* et naviguez vers le fichier manage_data.bat (%ESEC_HOME%\sdm).

5. Entrez un nom pour la tâche planifiée comme, par exemple, SDM_Archive. Sélectionnez *Une fois par jour* sous *Effectuer cette tâche :*. Cliquez sur *Suivant.*
6. Sélectionnez l'heure et le jour pour effectuer cette tâche. Cliquez sur *Suivant.*
7. Entrez une heure et une date au choix. Cliquez sur *Suivant.*



8. Entrez l'utilisateur sous lequel cette tâche est exécutée. Cet utilisateur ne peut pas correspondre au compte du système local. Il doit être exécuté comme un utilisate ur spécifique. Si vous utilisez l'authentification Windows pour vous connecter à la base de données, vous devez utilisez l'utilisateur Windows de la base de données Sentinel. Cliquez sur *Suivant.*
9. Cliquez sur *Terminer* pour conclure la tâche planifiée.

Moteur de corrélation

REMARQUE : Pour que le moteur de corrélation Sentinel fonctionne correctement, l'heure du système de la machine doit être synchronisée avec un délai de ± 30 secondes que toutes les machines du gestionnaire de collecteurs. Il est recommandé que toutes les machines du moteur de corrélation et du gestionnaire de collecteurs soient connectées à un serveur NTP (Network Time Protocol) ou autre type de serveur horaire.

Compréhension des règles de corrélation avancées

La règle de corrélation avancée est utilisée pour détecter les relations entre les évènements, comme la relation qui existe entre deux évènements, lorsqu'un évènement donné (évènement B) se déroule après un évènement A. Dans ce cas, l'évènement B est l'évènement actuel et il devrait être identifié par le filtre que avez entré dans le volet de l'assistant Critères de filtre d'évènements. L'évènement A est l'évènement passé et il devrait être identifié par le filtre que vous avez entré dans le volet de l'assistant Critères de filtre d'évènements passés. La relation entre les deux évènements (par ex, ils ont la même adresse IP source et cible) devrait être introduite dans le volet de l'assistant Critères de filtre d'évènements versus évènements passés. Dans ce volet, vous spécifiez aussi la durée maximale écoulée entre les deux évènements que vous voulez détecter, il s'agit de la fenêtre temporelle. Si un évènement

passe par tous ces critères, il peut alors être groupé et décompté dans la valeur de seuil indiqué dans le volet de l'assistant Critères de seuil et de groupement.

Contrôle de temps

Les opérations Fenêtre et Déclencheur ont toutes les deux une fenêtre temporelle qui leur est associée. Plus la fenêtre temporelle est grande, plus les évènements peuvent être stockés (pièces réelles d'informations d'évènement) dans la mémoire pour cette fenêtre temporelle. Pour l'opération Fenêtre, ce qui est stocké dépend du filtre indiqué pour les évènements passés. Plus ce filtre est spécifique, moins nombreux sont les évènements stockés dans la fenêtre temporelle, qui peuvent être ainsi utilisés pendant une plus grande période (le cas échéant). Pour l'opération Déclencher, l'espace total maximum de stockage à utiliser dépend de la cardinalité du discriminateur (c.-à-d., - plus la possibilité de groupement est grande, plus nombreux sont les évènements qui peuvent être stockés au fil du temps) jusqu'au seuil de chaque groupe. Souvent, la réduction proportionnelle du seuil et de la durée pour l'opération Déclencher produit des résultats équivalents.

Compréhension de la mise à jour de l'opération Déclencher

Supposons que vous avez reçu un évènement corrélé pour une règle, mais que vous vous attendiez à plus d'évènements corrélés. Cela peut être dû au comportement de mise à jour de l'opération Déclencher. Dans l'opération Déclencher, vous pouvez spécifier que si un ensemble de « n » évènements s'affichent pendant une certaine « d » durée, un évènement corrélé est déclenché. À chaque fois que le moteur de corrélation voit l'ensemble de « n » évènements pendant une certaine « d » durée, il se déclenche. Si lors du déclenchement il est déterminé qu'il s'est déjà déclenché (pour le même groupement) et s'il existe au moins un membre de l'ensemble en commun, ces membres sont ajoutés à l'évènement corrélé original, au lieu que soit crée un nouvel évènement corrélé.

Les expressions booléennes prennent en charge l'analyse court-circuit

Les comparaisons de chiffres sont plus rapides que les comparaisons de chaînes et les comparaisons de chaînes sont plus rapides que les comparaisons d'expressions normales. L'opération Filtrer effectue une analyse de court-circuit sur les expressions booléennes. Faites attention, si vous commandez l'expression, vous pouvez augmenter la vitesse d'évaluation.

N'ayez pas peur du format libre

Si vous n'arrivez pas à exprimer une règle de corrélation à l'aide des modèles prédéfinis de l'arborescence de l'assistant (Watchlist, Basic ou Advanced), n'hésitez pas à construire une règle de format libre. Tous les modèles finissent par former une règle de format libre pour l'utilisateur. Vous pouvez voir la représentation de format libre en éditant une règle et en changeant son type en format libre. Cela peut être une manière simple d'étendre une règle que vous n'arriviez pas à bien exprimer à l'aide d'une des trois options.

Journal de transactions

Pour SQL Server, par défaut, les bases de données Sentinel sont créées sous un modèle de récupération complète. Sous le modèle de récupération complète, l'espace utilisé du journal de transactions n'est pas libéré jusqu'à ce que la sauvegarde du journal de transactions soit exécutée. Afin d'éviter que le journal de transactions devienne complet, les sauvegardes des journaux devraient être planifiées dans SQL Server pendant toute la journée (3 ou 4 fois par jour, en fonction de votre taux d'évènements). Si votre organisation ne requiert pas la capacité d'effectuer une récupération jusqu'au point d'échec, vous pouvez

changer le modèle de récupération de la base de données en simple. Sous le modèle de récupération simple de la base de données, l'espace du journal de transactions est libéré automatiquement par SQL Server, sans l'aide des sauvegardes de journaux.

Emplacements des fichiers journaux Sentinel

Dans Sentinel, certains journaux sont utiles pour le dépannage du système. Ces journaux peuvent être extrêmement utiles, lorsque vous travaillez avec le support technique Novell pour résoudre des problèmes.

Gestionnaire de données Sentinel

Activités de journaux exécutées à l'aide du gestionnaire de données Sentinel pour le client spécifique, en cours d'exécution sur la même machine.

Pour Windows :

```
%ESEC_HOME%\sdm\SDM_*.0.log
```

Pour UNIX :

```
$ESEC_HOME/sdm/SDM_*.0.log
```

iTRAC

Activités des journaux liées à iTRAC.

Pour Windows :

```
%ESEC_HOME%\sentinel\log\das_itrac_0.*.log
```

Pour UNIX :

```
$ESEC_HOME/sentinel/log/das_itrac_0.*.log
```

Advisor

Activités des journaux liées au téléchargement et au traitement de données de l'Advisor.

Pour Windows :

```
%ESEC_HOME%\sentinel\log\advisor.log
%ESEC_HOME%\sentinel\log\Advisor_0.*.log
```

Pour UNIX :

```
$ESEC_HOME/sentinel/log/advisor.log
$ESEC_HOME/sentinel/log/Advisor_0.*.log
```

Insertion d’évènements

Activités des journaux liées à l’insertion d’évènements dans la base de données.

Pour Windows :

```
%ESEC_HOME%\sentinel\log\das_binary0.*.log
```

Pour UNIX :

```
$ESEC_HOME/sentinel/log/das_binary0.*.log
```

Recherches de base de données

Activités des journaux liées aux recherches de base de données, au collecteur, à l'état de santé du gestionnaire de collecteurs et à toutes les autres activités DAS, qui ne sont pas exécutées par d’autres composants DAS.

Pour Windows :

```
%ESEC_HOME%\sentinel\log\das_query0.*.log
```

Pour UNIX :

```
$ESEC_HOME/sentinel/log/das_query0.*.log
```

Active Views

Activités des journaux liées à Active Views.

Pour Windows :

```
%ESEC_HOME%\sentinel\log\das_rt0.*.log
```

Pour UNIX :

```
$ESEC_HOME/sentinel/log/das_rt0.*.log
```

Regroupement

Activités des journaux liées au regroupement.

Pour Windows :

```
%ESEC_HOME%\sentinel\log\das_aggregation0.*.log
```

Pour UNIX :

```
$ESEC_HOME/sentinel/log/das_aggregation0.*.log
```

Surveillance Sentinel

Activités des journaux liées à la surveillance Sentinel.

REMARQUE : sentinel_wrapper.log est destiné au wrapper de service.

Pour Windows :

```
%ESEC_HOME%\sentinel\log\sentinel0.*.log
%ESEC_HOME%\sentinel\log\sentinel_wrapper.log
```

Pour UNIX :

```
$ESEC_HOME/sentinel/log/sentinel0.*.log
$ESEC_HOME/sentinel/log/sentinel_wrapper.log
```

Gestionnaire de collecteurs

Activités des journaux liées au gestionnaire de collecteurs.

REMARQUE : agent-manager.log est destiné au wrapper de service.

Pour Windows :

```
%ESEC_HOME%\wizard\logs\agent-manager.log
%ESEC_HOME%\wizard\logs\am0.*.log
```

Pour UNIX :

```
$ESEC_HOME/wizard/logs/agent-manager.log
$ESEC_HOME/wizard/logs/am0.*.l
```

3 Installation de Sentinel 5 pour Oracle sur Solaris

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Ce chapitre décrit le mode d'installation de Novell Enterprise Security Management Sentinel 5 pour Oracle sur Solaris.

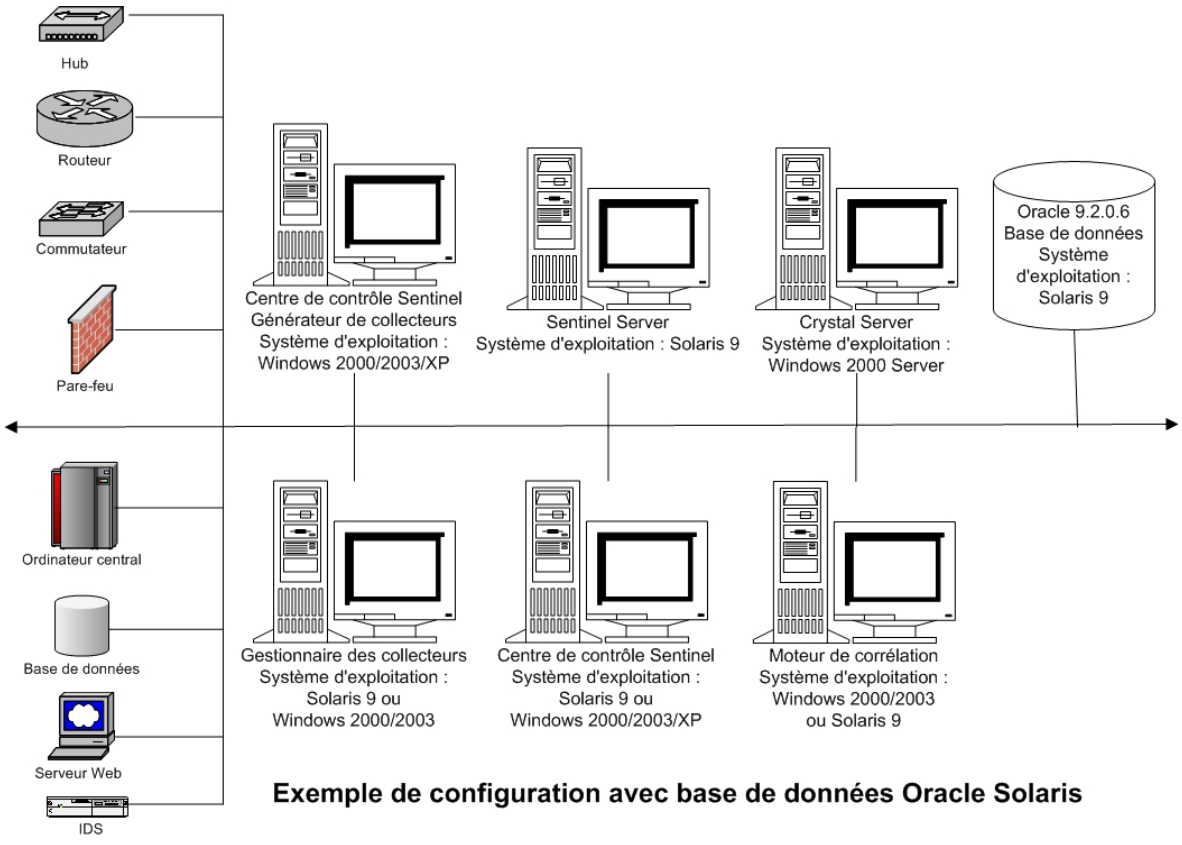
Préinstallation de Sentinel 5 pour Oracle sur Solaris

REMARQUE : avant l'installation, vérifiez que les machines sont bien conformes à la configuration système minimale requise et que le système d'exploitation a été renforcé selon les bonnes pratiques de sécurité actuelles.

REMARQUE : installez Oracle Enterprise avec partitionnement. Le gestionnaire de données Sentinel requiert cette fonction afin de gérer la base de données Sentinel.

REMARQUE : si vous effectuez une nouvelle installation de Sentinel sur un ordinateur sur lequel une version précédente de Sentinel avait été installée, vous devrez supprimer certains fichiers et paramètres système qui peuvent toujours subsister. Si ces fichiers et paramètres ne sont pas éliminés, la toute nouvelle installation peut échouer. Vous devriez le faire sur chaque machine où vous exécutez une nouvelle installation. Pour plus d'informations, voir *l'annexe E*.

Vous trouverez ci-dessous les configurations types de Solaris pour Sentinel. Votre configuration peut être différente, en fonction de l'environnement. Indépendamment de la configuration choisie, vous devez d'abord installer la base de données.



Exemple de configuration avec base de données Oracle Solaris

REMARQUE : pour plus d'informations concernant les systèmes d'exploitation pris en charge, voir le chapitre 1 - *Introduction, plates-formes prises en charge pour le serveur Sentinel sous Windows.*

Obtention d’une clé de licence

Le Database Access Service (DAS) du serveur Sentinel exige que vous ayez une clé de licence valide afin d'installer et d'exécuter le service. Cette clé de licence est verrouillée à la machine
où le DAS va être installé. Une clé de licence délivrée pour une machine ne marche pas sur une autre.

Pour obtenir la clé de licence, vous devez déterminer le numéro d'ID d'hôte et transmettre cette information à Novell qui vous attribuera une clé de licence.

Pour déterminer l'ID d’hôte (Solaris)

1. Entrez la commande suivante :

   ```
   hostid
   ```

2. Donnez ce numéro d'ID d’hôte au support client de Sentinel. Il vous fournira une clé de licence.

Base de données Sentinel

Avant d'installer la base de données Sentinel, vous avez besoin de :

- Pour connaître la configuration matérielle requise, voir *les chapitres 1 et 2*.
- serveur Sun SPARC Solaris qui exécute Solaris 9 avec la DATE de grappe de correctifs recommandée : 03/05/05
- Oracle 9i Enterprise Edition 9.2.0.6 ou 9.2.0.7 avec partitionnement
- Pour Solaris, une copie de la remarque Oracle : 148673.1 SOLARIS : Guide de démarrage rapide
- utilisateur du système d'exploitation Oracle (par défaut : oracle)
- Vérifiez que les variables d'environnement suivantes sont définies pour l'utilisateur du système d'exploitation Oracle :
  - ORACLE_HOME
  - ORACLE_BASE
  - PATH (il faut $ORACLE_HOME/bin)
  - Bien que cela ne soit pas recommandé, si vous créez manuellement l'instance de la base de données Oracle, reportez-vous au chapitre Création d'une instance Oracle pour la base de données Sentinel pour lire les instructions sur la création de l'instance Oracle. Si vous choisissez cette option, vous devez quand même utiliser le programme d'installation, pour ajouter les objets de base de données à l'instance de la base de données Oracle créée manuellement (voir Installation personnalisée pour les instructions).

REMARQUE : lors de l'utilisation d'une instance de la base de données Oracle, existante ou créée manuellement, elle doit être vide à l'exception de la présence de l'utilisateur esecdba.

- Si vous utilisez le programme d'installation pour créer l'instance de la base de données Oracle (recommandé), il vous faut les chemins de répertoire pour placer les fichiers de la base de données. Ces répertoires doivent exister avant l'exécution du programme d'installation, puisqu'il ne crée pas ces répertoires. Ces répertoires doivent être accessibles en écriture pour l'utilisateur du système d'exploitation Oracle (par ex. oracle).

REMARQUE : pour des raisons de performance, si vous installez en RAID et si l'environnement RAID le permet, le journal des répétitions doit cibler le disque d'écriture disponible le plus rapide.

REMARQUE : par défaut, le programme d'installation définit les espaces de table suivants pour NE PAS croître automatiquement : ESENTD, ESENTX, SENT_SMRYD et SENT_SMRYX. Tous les autres espaces de table sont définis pour croître automatiquement. Les espaces de tables ESENTD, ESENTX, SENT_SMRYD et SENT_SMRYX ne peuvent pas croître automatiquement parce qu'ils contiennent des évènements et des données d'évènements récapitulatives. L'utilisation de l'espace des événements et des résumés peut être très dynamique. Ces espaces de table d'évènements doivent être contrôlés et élargis de façon contrôlée selon la configuration du système de fichiers et en respectant l'équilibre E/S et la sauvegarde et récupération de la base de données.

La gestion de partitions SDM (archivage, déplacement et ajout des partitions) devrait être programmée pour maintenir les données d'évènements à une taille contrôlée.

Serveur Sentinel

REMARQUE : si vous n'installez pas la base de données Sentinel et le serveur Sentinel en même temps, la base de données Sentinel doit être installée en premier.

Avant d'installer le serveur Sentinel, vous avez besoin de :

- Pour connaître la configuration matérielle requise, voir *les chapitres 1 et 2.*
- serveur Sun SPARC Solaris qui exécute Solaris 9 avec la DATE de grappe de correctifs recommandée : 03/05/05
- le numéro de série de Novell Sentinel 5 et la clé de licence (pour DAS). Pour plus d'informations, voir Obtention d'une clé de licence.
- serveur SMTP – nécessaire pour envoyer un message électronique à partir de Sentinel.

Sentinel Control Center et Wizard

Avant d'installer le serveur Sentinel, vous avez besoin de :

- Pour connaître la configuration matérielle requise, voir *les chapitres 1 et 2.*
- Un des systèmes d'exploitation suivants :
  - serveur Sun SPARC Solaris qui exécute Solaris 9 avec la DATE de grappe de correctifs recommandée : correctifs 03/05/05
  - (seulement Collector Builder) – Windows 2000 ou 2003

Advisor

Pour installer l'Advisor, il vous faut obtenir un ID Advisor et un mot de passe de Novell. Le téléchargement direct d'Internet utilise le port 443.

REMARQUE : si vous pensez n'utiliser l'Advisor que pour la détection d'exploits, il n'est pas nécessaire d'installer le logiciel Crystal Enterprise. Cela n'est nécessaire que si vous avez l'intention d'utiliser les rapports Crystal pour Sentinel. Voir *le chapitre 8, « Configuration de l'Advisor »*, pour plus d'informations.

Vérification de la disposition Solaris (configuration système requise pour les correctifs)

Vérification de la disposition Solaris

1. Allez sur le site Internet Sun et téléchargez l'ensemble des correctifs recommandés pour Solaris 9 :
   - DATE de la grappe de correctifs : 03/05/05

   REMARQUE : consultez le fichier README et d'autres documentations incluses. La sauvegarde complète du système avant l'application des correctifs est FORTEMENT recommandée.
2. Loguez-vous comme utilisateur root et installez la grappe de correctifs et les correctifs kernel applicables.
3. Après la conclusion des correctifs, supprimez le fichier *_Recommended.zip et les fichiers agrandis dans les répertoires créés par le correctif, puis redémarrez le serveur.

Préinstallation Oracle sur Solaris

L'installation Oracle sur Solaris pour Sentinel requiert la réalisation des étapes suivantes :

- configuration des valeurs kernel.
- création d'un groupe et d'un compte utilisateur pour Oracle
- configuration des variables d'environnement
- installation d'Oracle 9.2.0.6 ou 9.2.0.7
- correctifs d'Oracle 9.2.0.6 ou 9.2.0.7

Configuration des valeurs Kernel pour Oracle sur Solaris

Pour Oracle sur Solaris, les valeurs kernel suivantes doivent être configurées dans /etc/system.

EXCLUSION DE GARANTIE : Vous trouverez ci-dessous des suggestions de valeurs minimums. Consultez l'administrateur système et la documentation Oracle pour plus d'informations.

- shmmax=4294967295
- shmmin=1
- shmseg=50
- shmmni=400
- semmns=14000
- semmni=1024
- semmsl=1024
- shmopm=100
- shmvmx=32767

REMARQUE : si les valeurs kernel sont égales ou supérieures à celles exigées ci-dessus, il n'est pas nécessaire de changer les paramètres.

1. Loguez-vous comme utilisateur root.
2. Faites une copie de sauvegarde de /etc/system.
3. Avec l'éditeur de texte, changez la configuration des paramètres kernel dans le fichier /etc/system comme indiqué dans le tableau ci-dessus.
4. Redémarrez.

Préinstallation Oracle sur Solaris

EXCLUSION DE GARANTIE : Les instructions suivantes ne remplacent pas la documentation Oracle. Il s'agit seulement d'un exemple de scénario de configuration. Cette documentation part du principe que le répertoire privé des utilisateurs Oracle est /export/home/oracle et qu'Oracle est installé dans /opt/oracle. La configuration exacte peut varier. Consultez la documentation concernant le système d'exploitation et Oracle, pour plus d'informations.

REMARQUE : lors de l'installation du logiciel Oracle, il est recommandé de choisir l'installation type. Si vous optez pour l'installation personnalisée, veillez à installer l'interface Oracle JDBC/OCI. Pour plus d'informations, voir la documentation Oracle.

1. Loguez-vous comme utilisateur root.
2. Créez un groupe UNIX et des comptes utilisateurs UNIX pour le propriétaire de la base de données Oracle.

   Ajoutez un groupe dba (comme root) :

   ```
   groupadd –g 400 dba
   ```

Ajoutez l' utilisateur oracle (comme root) :

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

3. Pour configurer les variables d'environnement nécessaires à Oracle, nous vous conseillons d'ajouter les informations suivantes au fichier local.cshrc :

```
umask 022

setenv ORACLE_HOME /opt/oracle

setenv ORACLE_SID ESEC

setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib

setenv DISPLAY :0.0

set path=(/bin /bin/java /usr/bin /usr/sbin
   ${ORACLE_HOME}/bin /usr/ucb/etc.)

if ( $?prompt ) then

set history=32

endif
```

4. Suivez les étapes décrites dans la remarque Oracle : 148673.1 SOLARIS : Guide de démarrage rapide.
5. Installez Oracle 9i édition 2 comme utilisateur oracle. Une invite vous demande deux CD-ROM supplémentaires. Vous devez naviguer vers des répertoires différents pour chaque CD-ROM supplémentaire.
6. Corrigez le système concernant l'édition 9.2.0.6.0 ou 9.2.0.7.0. Reportez-vous à la documentation Oracle pour les procédures des correctifs.
7. Pour vérifier le niveau de correctif, comme utilisateur oracle UNIX, entrez :

   ```
   sqlplus '/as sysdba'
   ```

   Les résultats doivent indiquer l'édition 9.2.0.6.0 ou 9.2.0.7.0. Sortez en introduisant Quitter.
8. Éliminez le répertoire créé pour le correctif.
9. Après l'installation des correctifs, éliminez les répertoires et fichiers de correctif.
10. Redémarrez.

Installation de Sentinel 5 pour Oracle sur Solaris

Sentinel 5 prend en charge deux types d'installation. À savoir :

- simple – option d'installation tout en un : services Sentinel, service collecteur et applications avec Oracle, tout sur la même machine. Ce type d'installation ne sert qu'à des fins de démonstration.
- personnalisée – elle permet une installation totalement distribuée.

Installation simple sur Solaris

Cette installation installe les composants les plus communs (elle n'inclut pas les fonctions de Collector Builder ou de logiciel d'intégration tiers) sur la même machine. Elle sert surtout à des fins de démonstration. Elle n'est pas recommandée pour l'utilisation dans un environnement de test ou de production.

REMARQUE : l'installation simple ne prend pas en charge l'authentification du mot de passe du gestionnaire de collecteurs.

Comment effectuer une installation simple

1. Vérifiez que vous avez collecté les informations, réalisé les tâches et rempli toutes les conditions définies à la section Préinstallation de Sentinel 5 pour Oracle pour les composants à installer.
2. Vérifiez la configuration de Solaris Oracle.
3. Loguez-vous comme utilisateur root.
4. Insérez et montez le CD d'installation de Sentinel.
5. Démarrez le programme d'installation en accédant au répertoire d'installation sur le CD-ROM et entrez :

   En mode GUI :

   ```
   ./setup.sh
   ```

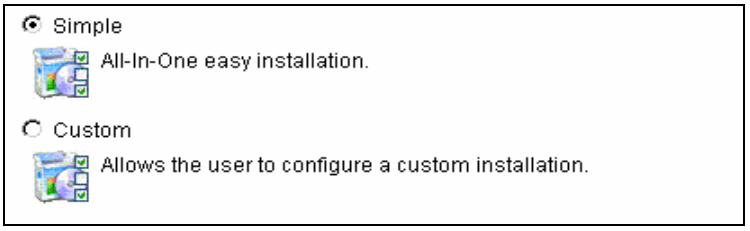
   ou

   En mode texte (« headless ») :

   ```
   ./setup.sh –console
   ```

6. Cliquez sur la flèche bas et sélectionnez une des langues suivantes au choix.
   - anglais
   - français
   - allemand
   - italien
   - portugais
   - espagnol
7. Suivez les invites du programme d'installation.
8. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
9. Acceptez l'accord de licence utilisateur final, puis cliquez sur *Suivant*.
10. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* afin d'indiquer l'emplacement de l'installation. Cliquez sur *Suivant*.

11. Sélectionnez *Simple*. Cliquez sur *Suivant*.



12. Entrez les informations de configuration :
    - numéro de série et clé de licence
    - serveur SMTP (nom DNS ou adresse IP), si vous voulez que Sentinel soit capable d'envoyer des messages électroniques.
    - courrier électronique - entrez une adresse électronique valide où les messages de notification de l'Advisor doivent être envoyés (par ex. Sent_Server@myserver.com).
    - mot de passe global du système – entrez le mot de passe et le mot de passe de confirmation correspondant. Celui-ci devient le mot de passe pour tous les utilisateurs par défaut, y compris l'utilisateur du système d'exploitation esecadm et les utilisateurs de la base de données. Voir Base de données Sentinel, à la section Post-installation de Sentinel 5 pour Oracle, pour consulter la liste des utilisateurs de la base de données par défaut, créée lors de l'installation.
    - répertoire de données – l'emplacement de tous les fichiers de données concernant la base de données et le téléchargement de l'Advisor (en cas d'installation de l'Advisor). Pour changer l'emplacement par défaut, cliquez sur le bouton …
      et sélectionnez un emplacement. Par défaut correspond à $ESEC_HOME/data.

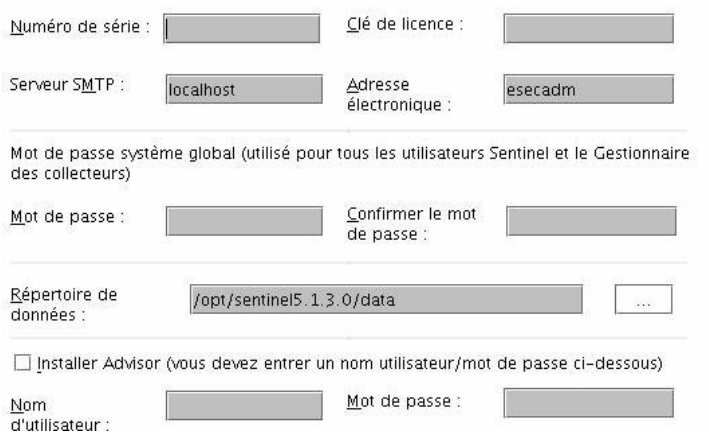
REMARQUE : l'utilisateur oracle et l'utilisateur esecadm doivent pouvoir accéder au répertoire de données (pour la lecture, l'écriture et l'exécution). Comme cette installation ne sert qu'à des fins de démonstration, il est recommandé de réaliser cette accessibilité en donnant à tout le monde l'accès au répertoire de données en lecture, écriture et exécution. Ce qui peut être fait en exécutant la commande suivante :

chmod 777 <chemin_répertoire>

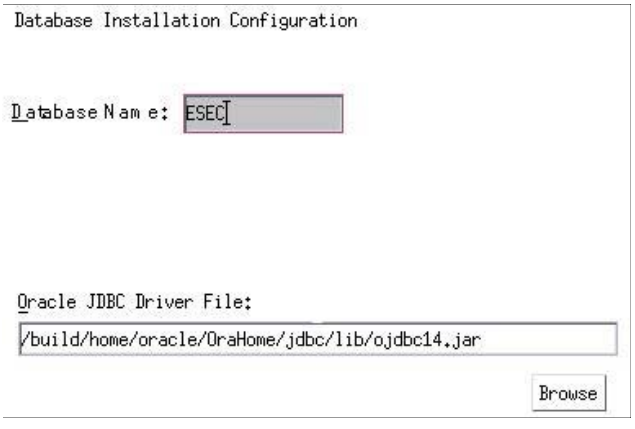
REMARQUE : si vous installez l'Advisor, l'installation simple configure l'Advisor pour utiliser le téléchargement direct d'Internet avec un intervalle de mise à jour de 12 heures et toutes les notifications par messages électroniques activées.

- Pour installer l'Advisor, cochez la case *d'installation Advisor*. Entrez un nom d'utilisateur et un mot de passe. S'il n'est pas possible de vérifier votre nom d'utilisateur ou votre mot de passe, lorsque vous cliquez sur Suivant, une invite vous demande si vous voulez continuer (déconseillé). Si vous choisissez de continuer, entrez de nouveau le mot de passe de l'Advisor dans la fenêtre Confirmation de mot de passe. Sinon, corrigez le mot de passe de l'Advisor.

Cliquez sur *Suivant.*



13. Entrez les informations de configuration de la base de données :
    - nom de la base de données – C'est le nom de l'instance de la base de données Oracle pour créer et installer des objets de base de données Sentinel. Aucune base de données portant ce nom ne doit déjà exister.
    - fichier pilote Oracle JDBC. C'est le chemin complet vers le fichier jar, normalement $ORACLE_HOME/jdbc/lib/ojdbc14.jar (impossible d'utiliser des variables d'environnement dans ce champ).



14. Cliquez *OK* sur le nom d'utilisateur oracle par défaut.

15. Lisez les informations sur les écrans qui apparaissent, avant de cliquer sur Suivant. Après avoir terminé l'installation, vous devez redémarrer le système.

REMARQUE : si vous voulez installer un logiciel d'intégration tiers (HP Service Desk ou Remedy Integration), après le redémarrage de la machine, exécutez de nouveau le programme d'installation et sélectionnez le logiciel d'intégration tiers que vous voulez installer. Pour plus d'informations, voir *le guide du logiciel d'intégration tiers.*

---

16. Par défaut, le programme d'installation Sentinel désactive l'Archivage de consignations. À des fins de récupération de bases de données, il est fortement recommandé d'activer l'Archivage de consignations après l'installation et avant de commencer à recevoir les données d'évènements de production. Vous devez aussi programmer la sauvegarde des archives de consignations pour libérer de l'espace dans le journal d'archive cible, sinon la base de données ne va plus accepter d'évènements.

Installation personnalisée sur Solaris

Comment effectuer une installation personnalisée

1. Vérifiez que vous avez collecté les informations, réalisé les tâches et rempli toutes les conditions définies à la section Préinstallation de Sentinel 5 pour Oracle pour les composants à installer.
2. Vérifiez la configuration de Solaris Oracle.
3. Loguez-vous comme utilisateur root.
4. Insérez et montez le CD d'installation de Sentinel.
5. Démarrez le programme d'installation en accédant au répertoire d'installation sur le CD-ROM et entrez :

   En mode GUI :

   ```
   ./setup.sh
   ```

   ou

   En mode texte (« headless ») :

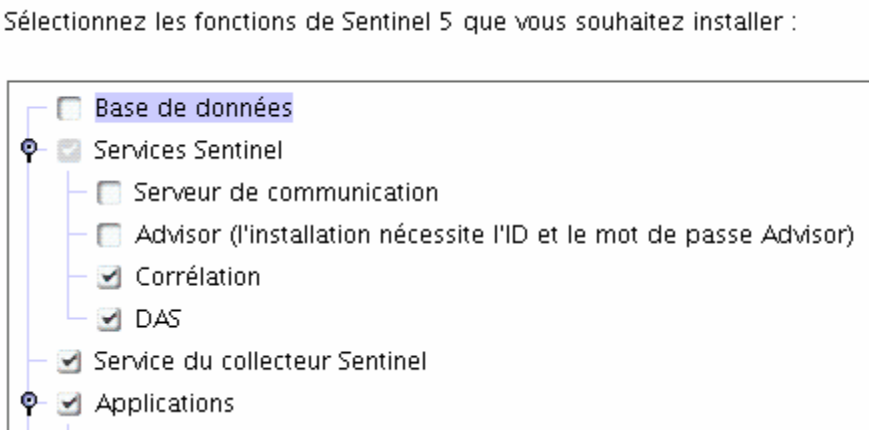
   ```
   ./setup.sh –console
   ```

6. Cliquez sur la flèche bas et sélectionnez une des langues suivantes au choix.
   - anglais
   - français
   - allemand
   - italien
   - portugais
   - espagnol
7. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
8. Acceptez l'accord de licence utilisateur final, puis cliquez sur *Suivant*.
9. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* afin d'indiquer l'emplacement de l'installation. Cliquez sur *Suivant*.

10. Sélectionnez *Personnalisée* (par défaut). Cliquez sur *Suivant*.
11. Sélectionnez les fonctions à installer.

REMARQUE : pour plus d'informations concernant le composant qui peut être installé pour les différentes configurations, voir *le chapitre 1 « Configuration système requise ».*

Les options suivantes sont disponibles :



- base de données – elle installe la base de données Sentinel
- serveur de communication – elle installe le bus de messages (iSCALE)
- Advisor
- moteur de corrélation
- DAS
- Service de collecteurs
- Sentinel Control Center
- Gestionnaire de données Sentinel
- HP OpenView Service Desk*
- Remedy Integration*

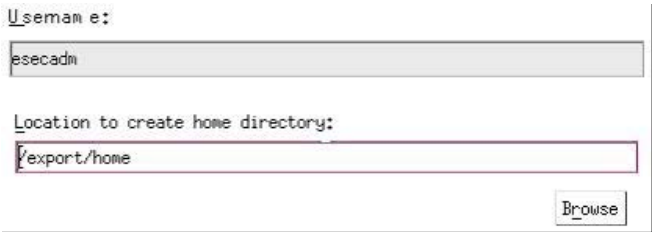
REMARQUE : *pour plus d'informations sur l'installation de HP OpenView Service Desk ou Remedy Integration, voir *le guide du logiciel d'intégration tiers.*

REMARQUE : si aucune des fonctions enfants de « Sentinel Services » n'est sélectionnée, la fonction « *Sentinel Services* » doit elle aussi être désélectionnée. Elle apparaît en gris et cochée en blanc si elle est encore sélectionnée alors qu'aucune de ses fonctions enfants n'est sélectionnée.

REMARQUE : pendant l'installation du composant de la base de données Sentinel, le programme d'installation place les fichiers dans le dossier $ESEC_HOME/utilities/db.

---

12. Si vous avez sélectionné l'installation du DAS, une invite vous demande :
    - le numéro de série
    - la clé de licence
13. Si vous avez sélectionné l'installation d'un logiciel d'intégration tiers (HP Service Desk ou Remedy Integration), vous devrez fournir un mot de passe pour déverrouiller le(s) composant(s) d'intégration tiers sélectionné(s). Pour plus d'informations, voir *le guide du logiciel d'intégration tiers.*
14. Indiquez le nom d'utilisateur de l'administrateur Sentinel du système d'exploitation et l'emplacement de son répertoire privé. Il s'agit du nom d'utilisateur du propriétaire du produit Sentinel installé. Un utilisateur est créé, s'il n'en existe pas encore, ainsi qu'un répertoire privé dans le répertoire indiqué.
    - nom d'utilisateur de l'administrateur du SE – par défaut esecadm
    - répertoire privé de l'utilisateur de l'administrateur du SE – par défaut « /export/home » Si le nom d'utilisateur est esecadm, le répertoire privé de l'utilisateur est /export/home/esecadm.



REMARQUE : si un nouvel utilisateur est créé, son mot de passe doit être défini manuellement, hors du programme d'installation. Il est fortement recommandé de le faire directement en se loguant au système après l'installation du produit.

afin d'accomplir les configurations de sécurité rigoureuses exigées par la certification de critères communs, Sentinel requiert un mot de passe fort avec les caractéristiques suivantes :

1. Choisissez des mots de passe comportant au moins 8 caractères qui incluent au moins un caractère en MAJUSCULE, un caractère en minuscule, un symbole spécial (#$_) et un caractère numérique (0 à 9). N'utilisez pas de vides.

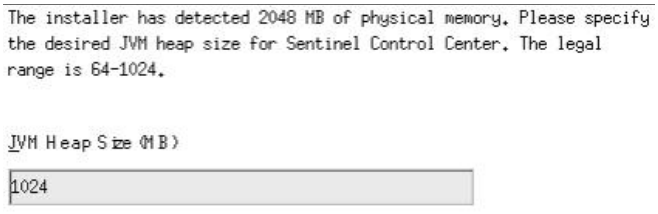
2. Le mot de passe ne peut contenir ni votre adresse électronique, ni aucune partie de votre nom complet.

3. Le mot de passe ne doit pas être un nom commun (par exemple, ce ne doit pas être un mot du dictionnaire ou d'argot d'usage commun).

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

5. Vous devriez choisir un mot de passe facile à mémoriser mais complexe. Par exemple, Mea5 !A (Mon enfant a 5 ans) OU JhaPdp5#a (J'habite à Paris depuis 5 ans).

15. Si vous sélectionnez l'installation de Sentinel Control Center, une invite taille heap JVM (Java Virtual Machine) apparaît :
    - taille heap JVM (Mo) - par défaut, elle est définie comme la moitié de la taille de la mémoire physique détectée sur la machine, au maximum 1 024 Mo. Elle correspond
      au maximum de taille heap JVM seulement utilisée par Sentinel Control Center.



16. Si vous décidez d'installer le *service de collecteurs*, choisissez de protéger ou non le gestionnaire de collecteurs de l'assistant à l'aide d'un mot de passe. Si vous choisissez de protéger le gestionnaire de collecteurs de l'assistant, vous êtes invité à créer un mot de passe du gestionnaire de collecteurs de l'assistant.

REMARQUE : si vous protégez le gestionnaire de collecteurs de l'assistant avec un mot de passe, vous devez entrer ce mot de passe lors du téléchargement ou du débogage des collecteurs dans ce gestionnaire de collecteurs de l'assistant. Ce mot de passe est aussi nécessaire, en plus du nom d'utilisateur Sentinel et du mot de passe correspondant, pour se loguer dans le gestionnaire de collecteurs de l'assistant.

REMARQUE : afin d'accomplir les configurations de sécurité rigoureuses exigées par la certification de critères communs, Sentinel requiert un mot de passe fort avec les caractéristiques suivantes :

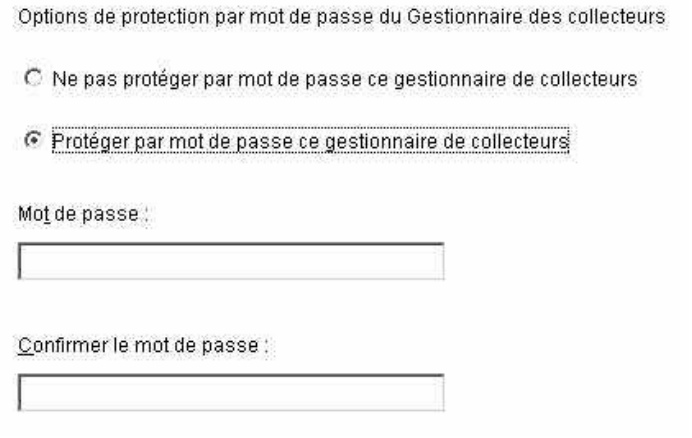
1. Choisissez des mots de passe comportant au moins 8 caractères qui incluent au moins un caractère en MAJUSCULE, un caractère en minuscule, un symbole spécial (!@#$%^&*()_+) et un caractère numérique (0 à 9).

2. Le mot de passe ne peut contenir ni votre adresse électronique, ni aucune partie de votre nom complet.

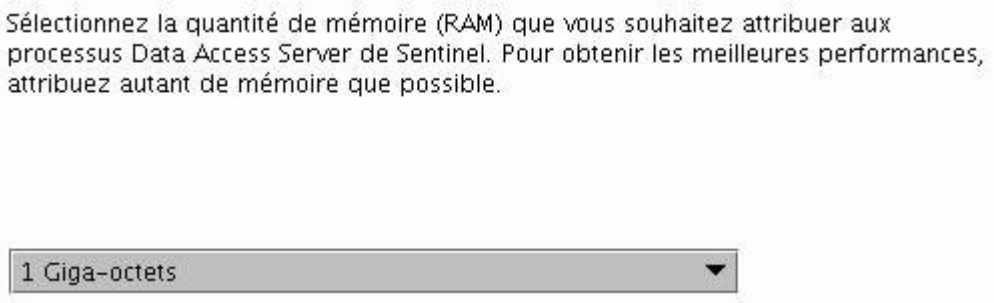
3. Le mot de passe ne doit pas être un nom commun (par exemple, ce ne doit pas être un mot du dictionnaire ou d'argot d'usage commun).

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

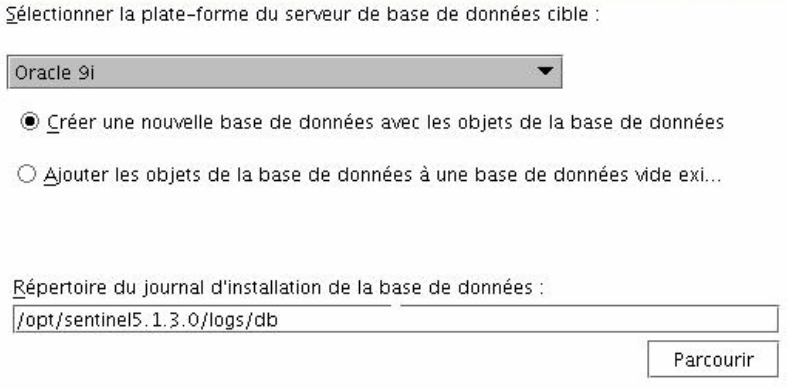
5. Vous devriez choisir un mot de passe facile à mémoriser mais complexe. Par exemple, Mea5!A (Mon enfant a 5 ans) OU JhaPdp5#a (J'habite à Paris depuis 5 ans).



17. Si vous choisissez d'installer le DAS, sélectionnez la quantité de RAM dans le système que vous voulez allouer au DAS (Data Access Service). Pour des environnements distribués, il est recommandé de sélectionner le maximum de mémoire (4 Go). Pour des environnements indépendants, il est recommandé de sélectionner la moitié de la mémoire RAM.



18. Pour l'installation de la base de données, vous avez les invites suivantes.
    a. Sélectionnez Oracle 9i comme plate-forme du serveur de la base de données cible et choisissez une des options suivantes :
        - créer une nouvelle base de données avec des objets de base de données – elle crée une nouvelle base de données Oracle et remplit la nouvelle instance avec des objets de base de données.
        - ajouter des objets de base de données à une base de données existante vide – elle ne fait qu'ajouter la base de données à une instance de la base de données Oracle existante. la base de données existante doit être vide, à l'exception de
          la présence de l'utilisateur esecdba.
    b. Entrez le répertoire journal d'installation de bases de données (par défaut : $ESEC_HOME/logs/db). Acceptez le « Répertoire journal d'installation de la base de données » par défaut ou cliquez sur Parcourir afin de spécifier un emplacement différent.



    c. Cliquez *OK* sur le nom d'utilisateur oracle par défaut.

    d. Si vous choisissez de créer une nouvelle base de données, entrez les éléments suivants :
        - le chemin du fichier pilote Oracle JDBC (le nom type du fichier jar correspond à ojdbc14.jar). C'est le chemin complet vers le fichier jar, normalement $ORACLE_HOME/jdbc/lib/ojdbc14.jar (impossible d'utiliser des variables d'environnement dans ce champ).

- nom d'hôte – le nom d'hôte de la machine pour installer la base de données Ce champ n'est pas configurable, si une nouvelle instance de base de données est créée.
- nom de la base de données – nom de l'instance de la base de données à installer

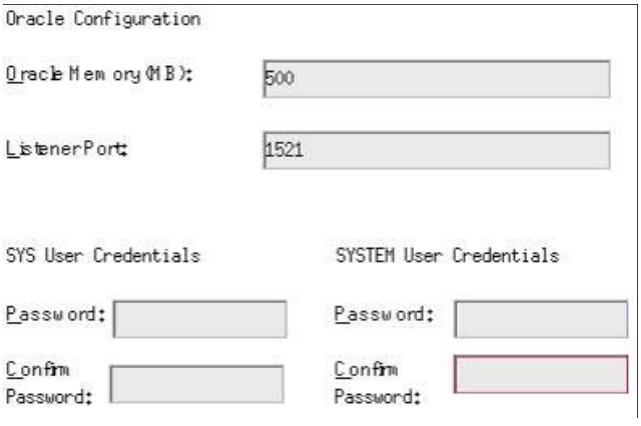
e. Si vous avez choisi d'ajouter des objets de la base de données à une base de données Oracle vide existante, une invite vous demande les informations suivantes :
   - le chemin du fichier pilote Oracle JDBC (le nom type du fichier jar correspond à ojdbc14.jar). C'est le chemin complet vers le fichier jar, normalement $ORACLE_HOME/jdbc/lib/ojdbc14.jar (impossible d'utiliser des variables d'environnement dans ce champ).
   - nom de la base de données ou adresse IP – le nom ou adresse IP de l'hôte où se trouve la base de données Oracle, à laquelle vous voulez ajouter des objets de base de données. Cela peut être le nom d'hôte local ou distant.
   - nom de la base de données – nom de l'instance de la base de données Oracle existante, vide, à laquelle vous voulez ajouter des objets de base de données (par défaut, ESEC). Ce nom de base de données doit s'afficher comme un nom de service dans le fichier tnsnames.ora (dans le répertoire $ORACLE_HOME/network/admin/) de la machine où le programme d'installation est exécuté.

REMARQUE : si le nom de la base de données n'est pas dans le fichier tnsnames.ora, le programme d'installation n'indique pas encore d'erreur à cette phase de l'installation (parce qu'il vérifie la connexion en utilisant une connexion directe JDBC), mais l'installation de la base de données échoue lorsque le programme d'installation de la base de données tente d'établir la connexion avec la base de données via sqlplus.
Si l'installation de la base de données échoue à cette phase, il est possible de retourner à cette invite et de corriger le nom de la base de données.

   - port de la base de données (par défaut, 1521)
   - Pour l'utilisateur de l'administrateur de la base de données Sentinel (DBA), indiquez le mot de passe de l'utilisateur « esecdba ». Le champ nom d'utilisateur de cette invite ne peut pas être édité.

f. Si vous choisissez de créer une nouvelle base de données, l'invite suivante s'affiche :

- mémoire Oracle (Mo) – la quantité de RAM à allouer à cette instance de la base
  de données Oracle.
- port du processus d'écoute – le port sur lequel est créé le processus d'écoute Oracle (par défaut, 1521)
- mot de passe de l'utilisateur SYS et confirmation de mot de passe – SYS est l'utilisateur oracle par défaut. Ce mot de passe d'utilisateur est défini avec la valeur indiquée ici.
- mot de passe de l'utilisateur SYSTEM et confirmation de mot de passe – SYSTEM est l'utilisateur oracle par défaut. Ce mot de passe d'utilisateur est défini avec la valeur indiquée ici.

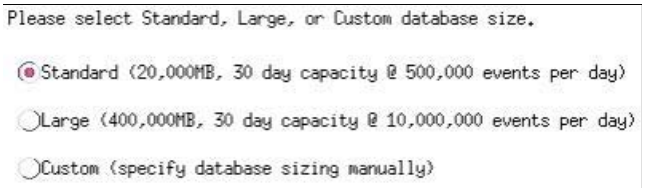


g. Si vous choisissez de créer une nouvelle base de données, une invite vous demande d'entrer la taille de la base de données. Vous avez les options suivantes :

- standard (20 Go)
- grande (400 Go)
- personnalisée (indiquez la taille manuellement). Si vous sélectionnez cette option, une invite vous demande :

  taille initiale de chaque fichier de la base de données en Mo (de 100 à 10 000)

taille maximum de chaque fichier de la base de données en Mo (de 2 000 à 100 000)
taille de tous les fichiers de la base de données en Mo (de 7 000 à 2 000 000)
taille de chaque fichier journal en Mo (de 100 à 100 000)



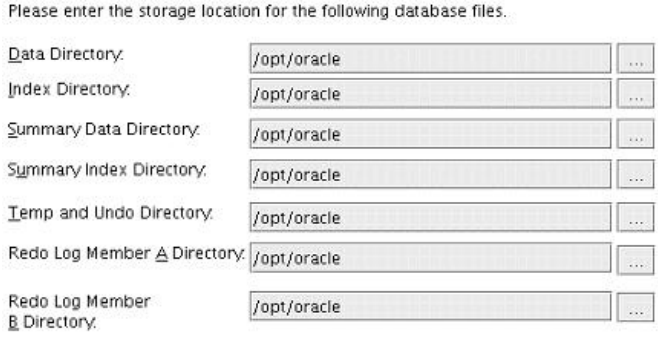
h. Si vous choisissez de créer une nouvelle base de données, une invite vous demande d'entrer l'emplacement d'archivage des fichiers de base de données suivants :

REMARQUE : à des fins de récupération et de performance, nous recommandons que ces emplacements soient dans des périphériques E/S différents.

Le programme d'installation ne crée pas ces répertoires, ils doivent donc être créés à l'extérieur avant de franchir cette étape.

Ces répertoires doivent être accessibles en écriture pour l'utilisateur oracle.

- répertoire de données
- répertoire d'index
- répertoire de données récapitulatif
- répertoire d'index récapitulatif
- répertoire temporaire et d'annulation d'espaces de table
- journal des répétitions du répertoire du membre A
- journal des répétitions du répertoire du membre B



i. Si vous choisissez de créer une nouvelle base de données, entrez les informations d'authentification de l'administrateur de la base de données Sentinel. C'est esecdba, le propriétaire des objets de la base de données.

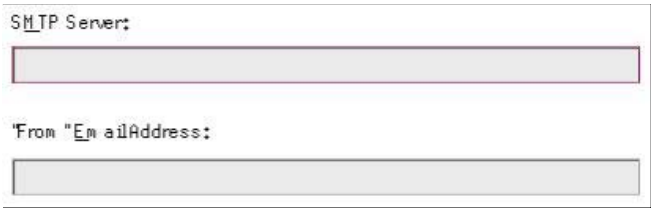
j. Entrez les informations d'authentification de l'utilisateur de la base de données de l'application Sentinel. C'est esecapp, le nom de l'utilisateur de l'application Sentinel que les procédures Sentinel utilisent pour se connecter à la base de données.

k. Entrez les informations d'authentification de l'utilisateur de la base de données de l'administrateur Sentinel. C'est esecadm, l'utilisateur de l'administrateur Sentinel.

l. Cliquez sur Suivant dans la fenêtre récapitulative de l'installation de la base de données.

19. Si vous avez choisi d'installer le DAS mais pas la base de données Sentinel, une invite vous demande les informations suivantes sur la base de données Oracle Sentinel. Ces informations sont utilisées pour configurer le DAS afin qu'il soit ciblé sur la base de données Sentinel.
    - nom d'hôte de la base de données ou adresse IP – C'est le nom ou l'IP de la base de données Oracle Sentinel existante à laquelle vous voulez connecter le composant DAS.
    - nom de la base de données – nom de l'instance de la base de données Oracle existante, vide, à laquelle vous voulez connecter le composant DAS (par défaut, ESEC).
    - port de la base de données (par défaut, 1521).
    - Pour l'utilisateur de la base de données de l'application Sentinel, indiquez le login « esecapp » et entrez le mot de passe donné à cet utilisateur lors de l'installation de la base de données Sentinel.

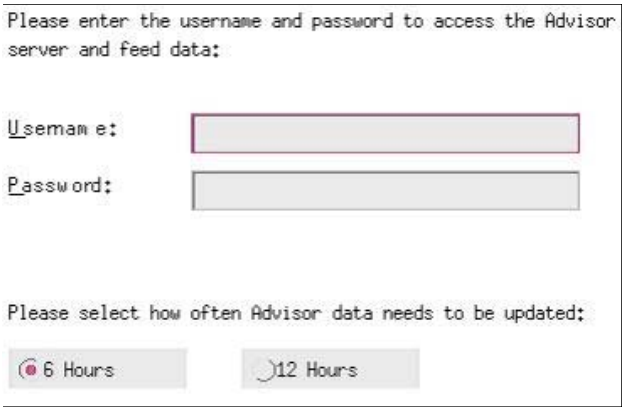
20. Si vous choisissez d'installer le DAS, configurez le support du courrier électronique Sentinel. Indiquez le serveur SMTP et l'adresse expéditeur que le Service d'exécution doit utiliser pour envoyer des messages (facultatif : vous pouvez éditer cela manuellement après avoir installé [$ESEC_HOME\sentinel\config\execution.properties]) :



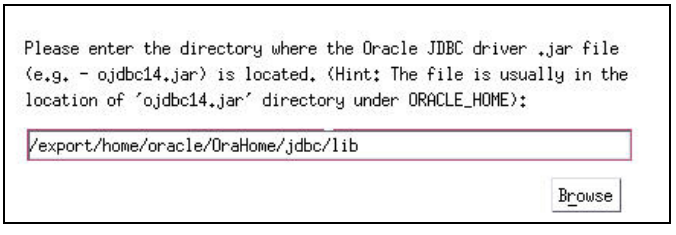
21. Si vous choisissez d'installer l'Advisor, sélectionnez le type d'installation Advisor (si l'option Advisor est choisie, un nom d'utilisateur et un mot de passe).
    - Téléchargement direct d'Internet – la machine Advisor est directement connectée à Internet. Dans cette configuration, les mises à jour de Novell sont automatiquement téléchargées de Novell sur Internet, à un rythme régulier.

- Indépendant – l'Advisor est configuré comme un système isolé qui requiert une intervention manuelle pour recevoir des mises à jour de Novell.

22. Si vous choisissez d'installer l'Advisor et sélectionnez l'option de téléchargement direct d'Internet, entrez le nom d'utilisateur de l'Advisor, le mot de passe, ainsi que le rythme souhaité des mises à jour de l'Advisor. S'il n'est pas possible de vérifier votre nom d'utilisateur ou votre mot de passe, lorsque vous cliquez sur Suivant, une invite vous demande si vous voulez continuer (déconseillé). Si vous choisissez de continuer, entrez de nouveau le mot de passe de l'Advisor dans la fenêtre Confirmation de mot de passe. Sinon, corrigez le mot de passe de l'Advisor.



23. Si vous choisissez d'installer l'Advisor, entrez le chemin vers le répertoire qui contient le pilote Oracle JDBC (le nom type du fichier pilote correspond à ojdbc14.jar). C'est le chemin complet vers le répertoire qui contient le fichier jar pilote, normalement $ORACLE_HOME/jdbc/lib (impossible d'utiliser les variables d'environnement dans
ce champ).



24. Si vous choisissez d'installer l'Advisor, entrez :
    - Le répertoire où les fichiers d'alimentation de données de l'Advisor sont archivés. C'est l'emplacement où les fichiers d'alimentation d'attaque et d'alerte sont enregistrés lors du téléchargement.

REMARQUE : le répertoire des fichiers d'alimentation de données Advisor doit avoir les paramètres de propriétaire suivants :

utilisateur – esecadm

groupe – esec

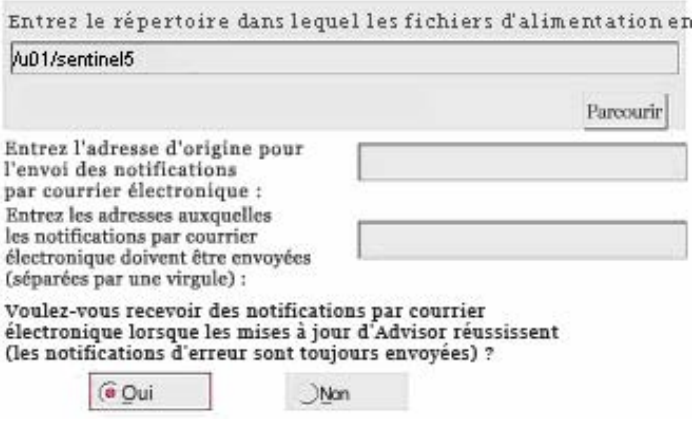
Si le répertoire ne comprend pas ces paramètres de propriétaire, exécutez la commande suivante comme utilisateur root pour configurer la propriété du répertoire :

```
chown esecadm:esec <chemin_répertoire>
```

- adresse expéditeur, qui apparaît dans les notifications par message électronique
- adresse destinataire, pour l'envoi de notifications par message électronique

REMARQUE : après l'installation, vous pouvez changer les adresses électroniques de l'Advisor, en éditant les fichiers attackcontainer.xml et alertcontainer.xml. dans le répertoire $ESEC_HOME/sentinel/config directory. Pour plus d'informations, voir le *chapitre 7, « L'onglet Advisor » dans le guide d'utilisateur Sentinel.*

- Sélectionnez Oui si vous voulez recevoir des messages électroniques concernant les mises à jour réussies de l'Advisor, ou Non dans le cas contraire. Les notifications d'erreurs sont toujours envoyées.



25. Si vous choisissez d'installer HP OpenView Service Desk ou Remedy Integration, une invite vous demande des informations supplémentaires. Pour plus d'informations, voir *le guide du logiciel d'intégration tiers Sentinel.*
26. Lisez les informations sur les écrans qui apparaissent, avant de cliquer sur Suivant. Une fois l'installation terminée, une invite vous demande de redémarrer. Cliquez sur *Terminer* pour redémarrer le système.
27. Par défaut, le programme d'installation Sentinel désactive l'Archivage de consignations. À des fins de récupération de bases de données, il est fortement recommandé d'activer l'Archivage de consignations après l'installation et avant de commencer à recevoir les données d'évènements de production. Vous devez aussi programmer la sauvegarde des archives de consignations pour libérer de l'espace dans le journal d'archive cible, sinon la base de données ne va plus accepter d'évènements.

28. Si vous prévoyez un taux d'évènements élevé (supérieur à 500 évènements par seconde), vous devez suivre les instructions de configuration supplémentaires de la section Configurer la stratégie d'insertion d'évènements d'objets de l'interface d'appel Oracle (OCI – Oracle Call Interface).

Post-Installation de Sentinel 5 pour Oracle

Mise à jour du courrier électronique Sentinel pour authentification SMTP

Si le système requiert une authentification SMTP, vous devez mettre à jour le fichier execution.properties. Ce fichier est sur la machine où le DAS est installé. Il est localisé à $ESEC_HOME/sentinel/config. Pour configurer ce fichier, exécutez mailconfig.sh, afin de changer le fichier et mailconfigtest.sh pour tester ces changements.

Pour configurer le fichier execution.properties

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfig de la façon suivante :

   ```
   ./mailconfig.sh -host <serveur SMTP> -from <adresse
      électronique source> -user <utilisateur
      authentification courrier électronique> –password
   ```

   Exemple :

   ```
   mailconfig.bat -host 10.0.1.14 -from nom@domaine.com -
      user nom_utilisateur –password
   ```

   Après cette commande, une invite vous demande d'entrer un nouveau mot de passe.

   ```
   Entrez le mot de passe :*********
   Confirmez le mot de passe :*********
   ```

REMARQUE : lors de l'utilisation de l'option de mot de passe, ce doit être le dernier argument.

Pour tester la configuration d'execution.properties

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfigtest de la façon suivante :

   ```
   ./mailconfigtest.sh -to <adresse électronique cible>
   ```

   Si l'envoi du message électronique a abouti, vous obtenez le résultat suivant sur l'écran et le message est reçu à l'adresse cible.

   ```
   Message électronique envoyé avec succès !
   ```

Vérifiez la boîte aux lettres de l'adresse cible pour confirmer la réception du message.
La ligne d'objet et le contenu devraient être les suivants :

```
Objet : Test des propriétés du courrier électronique
   Sentinel

Test de configuration des propriétés du courrier
   électronique Sentinel. Si ce message apparaît, les
   propriétés du courrier électronique Sentinel ont été
   correctement configurées pour envoyer des messages.
```

Base de données Sentinel

Après l'installation de la base de données Sentinel, la base de données contient les utilisateurs suivants par défaut :

- esecdba – propriétaire de schéma de la base de données Le privilège DBA n'est pas attribué à esecdba pour des raisons de sécurité. Pour utiliser l'Enterprise Manager, créez un utilisateur avec des privilèges DBA.
- esecapp – utilisateur de l'application de la base de données. C'est l'utilisateur de l'application utilisé pour la connexion avec la base de données.
- esecadm – utilisateur de la base de donnés qui est l'administrateur Sentinel Sentinel. Ce n'est pas le même compte utilisateur que celui de l'utilisateur du système d'exploitation esecadm.
- esecrpt – utilisateur de rapports de la base de données
- SYS – utilisateur de la base de données SYS
- SYSTEM – utilisateur de la base de données SYSTEM

Service de collecteurs

Lors de l'installation du service de collecteurs, les collecteurs suivants sont installés et chacun possède un programme d'installation de port de collecteur pour son exécution.

Produit	**Nom de collecteur**
Collecteurs démo	
Test de téléchargement d'actifs, travaille avec le collecteur DemoEvents	DemoAssetUpload
Test d'évènements démo, travaille avec les collecteurs DemoAssetUpload et DemoVulnerabilityUpload	DemoEvents
Test de téléchargement de vulnérabilité, travaille avec le collecteur DemoEvents	DemoVulnerabilityUpload
Test d'envoi d'un évènement	SendOneEvent
Test d'envoi de plusieurs évènements	SendMultipleEvents

REMARQUE : pour plus d'informations sur la configuration des collecteurs démo, voir le *chapitre 12 « Tester l'installation »*.

REMARQUE : pour plus de collecteurs, veuillez consulter le Sentinel Customer Portal. Pour plus d'informations (y compris la configuration), voir la documentation fournie avec chaque collecteur à : $WORKBENCH_HOME/Elements/<nom_collecteur>/Docs/

Pour installer d'autres collecteurs, exécutez le script Service Pack sur le CD Service Pack. Ce script installe les collecteurs localement.

Sous Windows :

```
.\service_pack.bat
```

Sur UNIX :

```
./service_pack.sh
```

Pour lire les instructions d'installation du Service Pack et la liste des collecteurs, voir *les notes de publication du Service Pack.*

Mise à jour de la clé de licence

Comment mettre à jour la clé de licence (Solaris)

1. Loguez-vous comme utilisateur esecadm.
2. Allez vers $ESEC_HOME/utilities.
3. Entrez la commande suivante :

```
/softwarekey
```

4. Entrez le numéro 1 pour entrer la clé principale. Appuyez sur Enter.

Création d'une instance Oracle pour la base de données Sentinel

REMARQUE : cette procédure est fournie comme exemple si vous voulez créer des espaces de table à l'aide de la fonction de création d'espaces de table incluse sur le CD d'installation. Les valeurs de la taille peuvent varier en fonction de la configuration et des conditions requises du système. Les espaces de table doivent être nommés exactement comme suit.

Sur l'instance Oracle, vous devez configurer :

- les paramètres
- les espaces de table

Création d'une instance Oracle

1. Loguez-vous comme utilisateur oracle.
2. À l'aide du GUI assistant de la base de données Oracle, créez ce qui suit :

REMARQUE : les valeurs peuvent varier en fonction de la configuration et des conditions requises du système.

Paramètres minimaux recommandés pour la configuration Solaris	
Paramètres	**Taille (octets ou tout autre indiqué)**

Paramètres minimaux recommandés pour la configuration Solaris	
Paramètres	**Taille (octets ou tout autre indiqué)**
db_cache_size	1 Go
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 Mo
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAIRE
hash_join_enabled	VRAI
optimizer_index_caching	50
optimizer_index_cost_adj	55

Taille minimale recommandée pour les espaces de table Solaris		
Espace de table	**Taille exemple :**	**Remarques**
REDO	3 x 100M	Valeur minimale. Vous devez créer des journaux de répétition plus grands si vous avez un EPS élevé.
SYSTEM	500M	Valeur minimum
TEMP	1G	Valeur minimum
UNDO	1G	Valeur minimum
ESENTD	5G	Valeur minimum Pour des données d'évènements
ESENTD2	500M	Valeur minimum Données pour configuration, actifs, vulnérabilité et associations (extension automatique activée)
ESENTWFD	250M	Pour données iTrac (extension automatique activée)
ESENTWFX	250M	Pour index iTrac (extension automatique activée)
ESENTX	3G	Valeur minimum Pour index d'évènements
ESENTX2	500M	Valeur minimum Index pour configuration, actifs, vulnérabilité et associations (extension automatique activée)
SENT_ADVISORD	200M	Valeur minimum Pour données Advisor (extension automatique activée)
SENT_ADVISORX	100M	Valeur minimum Pour index Advisor (extension automatique activée)
SENT_LOBS	100M	Valeur minimum Pour grands objets de base de données (extension automatique activée)
SENT_SMRYD	3G	Valeur minimum Pour regroupement, données récapitulatives

Taille minimale recommandée pour les espaces de table Solaris		
Espace de table	**Taille exemple :**	**Remarques**
SENT_SMRYX	2G	Valeur minimum Pour regroupement, index récapitulatif

3. Exécutez le script createEsecdba.sh qui se trouve dans le répertoire sentinel\dbsetup\bin sur le CD d'installation Sentinel. Ce script créé l'utilisateur esecdba qui est nécessaire pour ajouter des objets de la base de données à l'aide du programme d'installation Sentinel.
4. Sauvegardez la base de données.

Configuration de la stratégie d'insertion d'évènements de l'interface d'appel Oracle (OCI – Oracle Call Interface)

Sentinel 5.1 fournit une structure pour l'intégration de différentes stratégies afin d'insérer des évènements dans une base de données. Sentinel 5.1 fournit deux stratégies pour insérer des évènements dans la base de données Oracle.

- JDBCLoadStrategy
- OCILoadStrategy

La stratégie à utiliser pour l'insertion d'évènements est régie par la propriété insert.strategy du composant EventStoreService dans das_binary.xml.

La stratégie JDBC est la stratégie par défaut configurée au départ.

La stratégie OCI est une stratégie d'insertion native pour insérer les évènements plus rapidement. Cette stratégie requiert l'installation des bibliothèques Oracle OCI sur la machine où le composant DAS est exécuté. La stratégie OCI doit être utilisée dans les configurations qui requièrent un taux d'évènements élevé.

Le nombre d'évènements à regrouper pour être insérés dans la base de données est régi par la propriété insert.batchsize. Cette propriété insert.batchsize est utilisée par toutes les stratégies d'insertion d'évènements.

Pour changer de stratégie d'insertion d'évènements de Sentinel en passant de la stratégie d'insertion JDBC par défaut à la stratégie d'insertion OCI, il faut exécuter certaines étapes.

Passer de la stratégie d'insertion d'évènements JDBC à la stratégie d'insertion OCI

1. Vérifiez que les bibliothèques Oracle OCI sont installées sur la machine où le composant Sentinel DAS est exécuté. Vous devrez connaître le chemin d'ORACLE_HOME dans les étapes suivantes.
2. Loguez-vous sur la machine dès l'étape 1 comme utilisateur esecadm.
3. Créez un fichier « profil » dans le répertoire privé de l'utilisateur esecadm. Entrez le texte suivant dans le fichier (modifiez le chemin d'ORACLE_HOME pour être conforme à l'installation) :

```
ORACLE_HOME=/build/home/oracle/OraHome
export ORACLE_HOME
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

4. Ouvrez le fichier $ESEC_HOME/sentinel/config/das_binary.xml pour l'édition dans un éditeur de texte, quel qu'il soit.
5. Effectuez une recherche du texte suivant :

   ```
   JDBCLoadStrategy
   ```

6. Transformez le texte en :

   ```
   OCILoadStrategy
   ```

7. Enregistrez ce changement dans le fichier das_binary.xml.
8. Redémarrez l'application DAS Binary. (La manière la plus facile d'effectuer cette opération consiste à exécuter « ps –ef | grep DAS_Binary » pour obtenir l'ID de processus, détruire le processus puis permettre à l'application de surveillance Sentinel de le redémarrer.)

   Après le redémarrage de l'application DAS Binary, la bibliothèque $ESEC_HOME/sentinel/lib/libocievent.so est chargée et utilisée pour effectuer les insertions d'évènements dans la base de données via OCI.

Options supplémentaires d'insertion d'évènements OCI

Outre la spécification du « OCILoadStrategy » dans le fichier das_binary.xml, plusieurs autres options liées à l'OCI peuvent être configurées.

- insert.batchsize – ce paramètre vous permet de configurer le maximum d'évènements à insérer dans une base de données en une seule fois.
- insert.oci.workerCount – ce paramètre vous permet de configurer le nombre de threads utilisés pour insérer des données d'évènements dans la base de données.
- insert.oci.queueWaitTime – ce paramètre indique l'attente maximum en secondes avant d'insérer les données depuis la file d'attente entrante dans la base de données. Lorsqu'un lot complet d'évènements est reçu, tout le lot est inséré. Mais si le flux entrant d'évènements est lent, la période d'attente est utilisée pour déterminer le moment de l'insertion de la base de données (même si un lot complet d'évènements n'a pas encore été reçu).
- insert.oci.highWatermark – le haut filigrane de la file d'attente d'évènements entrants.
- insert.oci.lowWatermark – le bas filigrane de la file d'attente d'évènements entrants.
- insert.oci.optimizationFlag – drapeau d'optimisation « actif » ou « inactif »
-

Conseils de débogage OCI

L'interface OCI enregistre des messages dans le fichier $ESEC_HOME/sentinel/log/ocievent.log. Les messages initiaux enregistrés dans le fichier journal incluent des messages de connexion à la base de données réussis (ou échoués)…. C'est le lieu adéquat pour vérifiez si la bibliothèque OCI a été correctement chargée et configurée.

L'interface OCI enregistre aussi les erreurs dans le fichier journal das_binary localisé dans le répertoire $ESEC_HOME/sentinel/log. Les erreurs enregistrées dans le fichier journal das_binary comprennent les échecs de localisation/chargement de la bibliothèque libocievent.so, les échecs de connexion à la base de données et les échecs d'insertions d'évènements et d'associations d'évènements.

Si les messages d'erreur indiquent que le fichier « libocievent.so » n'est pas localisé ni chargé, il faut vérifier trois éléments :

1. Assurez-vous que les bibliothèques Oracle OCI sont installées.
2. Assurez-vous que le fichier « libocievent.so » est localisé dans le répertoire $ESEC_HOME/sentinel/lib.
3. Assurez-vous que le répertoire $ESEC_HOME/sentinel/lib est dans le chemin « LD_LIBRARY_PATH » de l'utilisateur « esecadm ». Sinon, vous pouvez mettre à jour le LD_LIBRARY_PATH dans le profil de l'utilisateur « esecadm ».
4. Assurez-vous que les variables d'environnement ORACLE_HOME et LD_LIBRARY_PATH sont correctement mises à jour dans les variables d'environnement de l'utilisateur esecadm, comme mentionné dans la section « Passer de la stratégie d'insertion d'évènements JDBC à la stratégie d'insertion OCI ».

4 Installation de Sentinel 5 pour Oracle sur Linux

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Ce chapitre décrit le mode d'installation de Sentinel Enterprise Security Management Sentinel 5 pour Oracle sur SuSe Linux Enterprise Server et Red Hat Enterprise Linux.

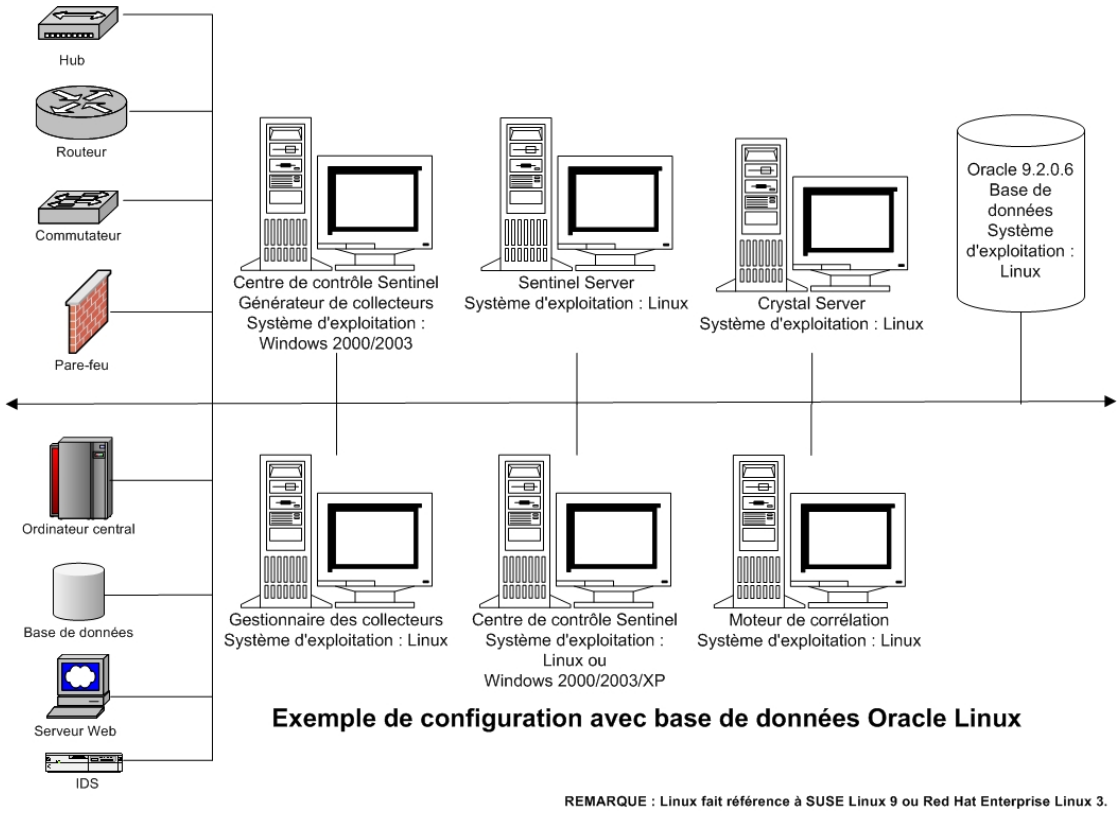
Préinstallation de Sentinel 5 pour Oracle sur Linux

REMARQUE : avant l'installation, vérifiez que les machines sont bien conformes à la configuration système minimale requise et que le système d'exploitation a été renforcé selon les bonnes pratiques de sécurité actuelles.

REMARQUE : installez Oracle Enterprise avec partitionnement. Sentinel Data Manager requiert cette fonction afin de gérer la base de données Sentinel.

REMARQUE : si vous effectuez une nouvelle installation de Sentinel sur un ordinateur sur lequel une version précédente de Sentinel avait été installée, vous devrez supprimer certains fichiers et paramètres système qui peuvent toujours subsister. Si ces fichiers et paramètres ne sont pas éliminés, la toute nouvelle installation peut échouer. Vous devriez le faire sur chaque machine où vous exécutez une nouvelle installation. Pour plus d'informations, voir *l'annexe E*.

Voici ci-dessous les configurations types de Linux pour Sentinel. Votre configuration peut être différente, en fonction de l'environnement. Indépendamment de la configuration choisie, vous devez d'abord installer la base de données.



REMARQUE : pour plus d'informations concernant les systèmes d'exploitation pris en charge, voir le chapitre 1 *Introduction, plates-formes prises en charge pour le serveur Sentinel sous Windows.*

Obtention d'une clé de licence

Le Database Access Service (DAS) du serveur Sentinel exige que vous ayez une clé de licence valide afin d'installer et exécuter le service. Cette clé de licence est verrouillée à la machine où le DAS est installé. Une clé de licence délivrée pour une machine ne marche pas sur une autre.

Pour obtenir la clé de licence, vous devez déterminer le numéro d'ID d'hôte et transmettre cette information à Novell qui vous attribuera une clé de licence.

Pour déterminer l'ID d'hôte (Linux)

1. Loguez-vous comme utilisateur root.
2. Insérez et montez le CD d'installation de Sentinel.
3. Dans le cd, allez à utilities/linux et entrez :

   ```
   ./esechostid
   ```

4. Donnez ce numéro d'ID d'hôte au support technique de Novell. Il vous fournira une clé de licence.

Base de données Sentinel

Avant d'installer la base de données Sentinel, vous avez besoin de :

- Pour connaître la configuration matérielle requise, voir les *chapitres 1 et 2*
- SuSE Linux Enterprise Server 9 ou Red Hat Enterprise Linux 3 Mise à jour 5 ES (x86)
- Oracle 9i Enterprise Edition 9.2.0.6 ou 9.2.0.7 avec partitionnement
- utilisateur du système d'exploitation Oracle (par défaut : oracle)
- Vérifiez que les variables d'environnement suivantes sont définies pour l'utilisateur du système d'exploitation Oracle :
  `ORACLE_HOME`

  `ORACLE_BASE`

  `PATH (il faut $ORACLE_HOME/bin)`

  - Bien que cela ne soit pas recommandé, si vous créez manuellement l'instance de la base de données Oracle, reportez-vous au chapitre Création d'une instance Oracle pour la base de données Sentinel pour lire les instructions sur la création de l'instance Oracle. Si vous choisissez cette option, vous devez quand même utiliser le programme d'installation, pour ajouter les objets de base de données à l'instance de la base de données Oracle créée manuellement (voir Installation personnalisée pour les instructions).

REMARQUE : lors de l'utilisation d'une instance de la base de données Oracle, existante ou créée manuellement, elle doit être vide à l'exception de la présence de l'utilisateur esecdba. La section Création d'une instance Oracle pour la base de données Sentinel contient des instructions pour créer cet utilisateur, s'il n'existe pas encore.

- Si vous utilisez le programme d'installation pour créer l'instance de la base de données Oracle (recommandé), il vous faut les chemins de répertoire pour placer les fichiers de la base de données. Ces répertoires doivent exister avant l'exécution du programme d'installation, puisqu'il ne crée pas ces répertoires. Ces répertoires doivent être accessibles en écriture pour l'utilisateur du système d'exploitation Oracle (par ex. oracle).

REMARQUE : pour des raisons de performance, si vous installez en RAID et si l'environnement RAID le permet, le journal des répétitions doit cibler le disque d'écriture disponible le plus rapide.

REMARQUE : par défaut, le programme d'installation définit les espaces de table suivants pour NE PAS croître automatiquement : ESENTD, ESENTX, SENT_SMRYD et SENT_SMRYX. Tous les autres espaces de table sont définis pour croître automatiquement. Les espaces de tables ESENTD, ESENTX, SENT_SMRYD et SENT_SMRYX ne peuvent pas croître automatiquement parce qu'ils contiennent des évènements et des données d'évènements récapitulatives. L'utilisation de l'espace des évènements et des résumés peut être très dynamique. Ces espaces de table d'évènements doivent être contrôlés et élargis de façon contrôlée selon la configuration du système de fichiers et en respectant l'équilibre E/S et la sauvegarde et récupération de la base de données.

La gestion de partitions SDM (archivage, déplacement et ajout des partitions) doit être programmée pour maintenir les donnés d'évènements dans une taille contrôlée.

Serveur Sentinel

REMARQUE : si vous n'installez pas la base de données Sentinel et le serveur Sentinel en même temps, la base de données Sentinel doit être installée en premier.

Avant d'installer le serveur Sentinel, vous avez besoin de :

- Pour connaître la configuration matérielle requise, voir les *chapitres 1 et 2*.
- SuSE Linux Enterprise Server 9 ou Red Hat Enterprise Linux 3 Mise à jour 5 ES (x86).
- Le numéro de série de Sentinel 5 et la clé de licence (pour DAS). Pour plus d'informations, voir Obtention d'une clé de licence.
- serveur SMTP – nécessaire pour envoyer un message électronique à partir de Sentinel.

Sentinel Control Center et Wizard

Avant d'installer le serveur Sentinel, vous avez besoin de :

- Pour connaître la configuration matérielle requise, voir les *chapitres 1 et 2*
- SuSE Linux Enterprise Server 9 ou Red Hat Enterprise Linux 3 Mise à jour 5 ES (x86)
- (Collector Builder et Sentinel Control Center) – Windows 2000 ou 2003

Advisor

Pour installer l'Advisor, il vous faut obtenir un ID Advisor et un mot de passe de Sentinel. Le téléchargement direct d'Internet utilise le port 443.

REMARQUE : si vous pensez n'utilisez l'Advisor que pour la détection d'exploits, il n'est pas nécessaire d'installer le logiciel Crystal Enterprise. Cela n'est nécessaire que si vous avez l'intention d'utiliser les rapports Crystal pour Sentinel. Voir le *chapitre 10*, *Configuration de l'Advisor*, pour plus d'informations.

Préinstallation Oracle sur Linux

L'installation Oracle sur Linux pour Sentinel requiert la réalisation des étapes suivantes :

- configuration des valeurs kernel
- création d'un groupe et d'un compte utilisateur pour Oracle
- configuration des variables d'environnement pour l'utilisateur Oracle
- liaison de gcc
- correctifs du système d'exploitation Linux à installer sur Oracle 9.2.0.4 (procurez-vous le correctif p3006854_9204_LINUX directement depuis Oracle)
- installation d'Oracle 9.2.0.4 (procurez-vous ce logiciel directement depuis Oracle)
- correctifs d'Oracle de 9.2.0.4 à Oracle 9.2.0.6 ou 9.2.0.7 (procurez-vous le chemin vers Oracle 9.2.0.6 ou 9.2.0.7 directement depuis Oracle)

Configuration des valeurs Kernel pour Oracle sur Linux

Pour Oracle sur Linux, les valeurs kernel suivantes doivent être définies.

EXCLUSION DE GARANTIE : Vous trouverez ci-dessous des suggestions de valeurs minimums. Si les paramètres actuels sont supérieurs à ces chiffres, ne les modifiez pas. Consultez l'administrateur système et la documentation Oracle pour plus d'informations.

- shmmax=2147483648 (valeur minimum)
- shmmni=4096
- semmns=32000
- semmni=1024
- semmsl=1024
- semopm=100

1. Loguez-vous comme utilisateur root.
2. Configurez les paramètres kernel en ajoutant le texte suivant à la fin du fichier « /etc/sysctl.conf » :

REMARQUE : Les paramètres suivants sont les valeurs minimums suggérées. Si les paramètres sont supérieurs à ces chiffres, ne les modifiez pas. Pour déterminer les valeurs actuelles pour un paramètre kernel particulier, exécutez la commande suivante :

```
sysctl <paramètre_kernel>
```

Par exemple, pour vérifiez la valeur actuelle du paramètre kernel « kernel.sem », exécutez la commande :

```
sysctl kernel.sem
```

```
# Paramètres Kernel pour Oracle
# kernel.sem = <SEMMSL> <SEMMNS> <SEMOPM> <SEMMNI>
kernel.sem = 1024        32000   100      1024
kernel.shmmax = 2147483648
kernel.shmmni = 4096
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
```

3. Exécutez la commande suivante pour charger les modifications dans le fichier « /etc/sysctl.conf » :

```
sysctl -p
```

4. Configurez les identificateurs de fichier et les limites de processus en ajoutant le texte suivant à la fin du fichier « /etc/security/limits.conf » : « nproc » est la limite maximum du nombre de processus et « nofile » est la limite maximum du nombre de fichiers ouverts. Ce sont les valeurs recommandées, mais elles peuvent être modifiées le cas échéant. Le texte suivant part du principe que l'ID d'utilisateur Oracle est « oracle ». Si l'ID utilisateur Oracle est différent, remplacez « oracle » dans le texte suivant par l'ID utilisateur Oracle.

```
# Paramètres ajoutés pour Oracle
oracle          soft    nproc   16384
oracle          hard    nproc   16384
oracle          soft    nofile  65536
oracle          hard    nofile  65536
```

Préinstallation Oracle sur Linux

Préinstallation Oracle sur Linux

EXCLUSION DE GARANTIE : Les instructions suivantes ne remplacent pas la documentation Oracle. Il s'agit seulement d'un exemple de scénario de configuration. Cette documentation part du principe que le répertoire privé des utilisateurs Oracle est **/export/home/oracle** et qu'Oracle est installé dans **/opt/oracle**. La configuration exacte peut varier. Consultez la documentation concernant le système d'exploitation et Oracle, pour plus d'informations.

1. Loguez-vous comme utilisateur root.
2. Créez un groupe UNIX et un compte d'utilisateur UNIX pour le propriétaire de la base de données Oracle.

   Ajoutez un groupe dba (comme root) :

   ```
   groupadd dba
   ```

3. Ajoutez un utilisateur Oracle (comme root) :

   ```
   useradd –g dba –s /bin/bash –d /export/home/oracle –m
      oracle
   ```

4. Créez un répertoire pour ORACLE_HOME et ORACLE_BASE :

   ```
   mkdir –p /opt/oracle/
   ```

5. Transformez la propriété du répertoire ORACLE_BASE et suivants en oracle/dba :

   ```
   chown -R oracle:dba /opt/oracle
   ```

6. Passez à l'utilisateur Oracle :

   ```
   su - oracle
   ```

7. Ouvrez le fichier « bash_profile » (dans le répertoire privé de l'utilisateur oracle) afin d'éditer et ajouter le suivant à la fin du fichier :

REMARQUE : Cet ensemble de variables d'environnement ne peut être utilisé que pour l'utilisateur Oracle. En particulier, ces variables ne doivent pas être configurées dans l'environnement du système ou dans l'environnement de l'utilisateur esecadm.

```
# Configurez la variable d'environnement LD_ASSUME_KERNEL
   seulement pour Red Hat 9,
# RHEL AS 3, et RHEL AS 4 !!
# Utilisez l'implémentation « Linuxthreads with floating
   stacks » au lieu de NPTL :
# pour RH 9 et RHEL AS 3
export LD_ASSUME_KERNEL=2.4.1
# pour RHEL AS 4
# exportez LD_ASSUME_KERNEL=2.4.19
# Oracle Environment
export ORACLE_BASE=/opt/oracle
```

```
export ORACLE_HOME=$ORACLE_BASE/
export ORACLE_SID=test
export ORACLE_TERM=xterm
# exportez TNS_ADMIN= Set si sqlnet.ora, tnsnames.ora,
   etc. ne sont pas dans $ORACLE_HOME/network/admin
export NLS_LANG=AMERICAN;
export ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data
LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
export LD_LIBRARY_PATH
# Définissez les chemins de recherche shell
export PATH=$PATH:$ORACLE_HOME/bin
```

8. Reloguez-vous comme utilisateur oracle pour charger les modifications des variables d'environnement depuis la dernière étape :

```
exit
su - oracle
```

9. Reliez gcc à la version 2.9.6

REMARQUE : Si /usr/bin/gcc296 ou /usr/bin/g++296 n'existent pas, cela signifie que le gcc ou le g++ n'ont pas été installés Dans ce cas, installez ces composants et puis retournez à cette étape.

```
su - root
ln -s /usr/bin/gcc296 /usr/bin/gcc
ln -s /usr/bin/g++296 /usr/bin/g++
```

10. Quittez pour retourner à l'invite d'utilisateur oracle.

```
exit
```

11. Exécutez le correctif Oracle p3006854_9204_LINUX.zip qui corrige le système d'exploitation Linux pour installer Oracle. Vous pouvez vous procurer ce correctif sur Oracle.

```
su - root
unzip p3006854_9204_LINUX.zip
cd 3006854
sh rhel3_pre_install.sh
```

12. Quittez pour retourner à l'invite d'utilisateur oracle.

```
exit
```

13. Pour installer 9.2.0.4 à partir du disque 1, exécutez le script :

```
./runInstaller
```

14. Au fur et à mesure du programme d'installation, laissez les invites avec les valeurs par défaut, sauf indication contraire ci-dessous.
    - À l'invite du nom de groupe UNIX, entrez : dba
    - À l'invite du type d'installation, sélectionnez Personnalisée.

    Sélectionnez les composants suivants à installer :
    - Oracle 9i 9.2.0.4.0
    - Enterprise Edition Options 9.2.0.1.0
        - Oracle Partitioning 9i 9.2.0.4.0
    - Oracle Net Services 9.2.0.1.0
        - Oracle Net Listener 9.2.0.4.0
    - Oracle Enterprise Manager Products 9.2.0.1.0 (Tous)
    - Oracle 9i Development Kit 9.2.0.1.0 (Tous)
    - Oracle 9i for UNIX Documentation 9.2.0.1.0
    - Oracle HTTP Server 9.2.0.1.0 (tous)
    - iSQL*Plus 9.2.0.4.0 (tous)
    - Oracle JDBC/OCI Interfaces 9.2.0.1.0
15. À l'invite Créer base de donnée, sélectionnez NON.
16. Facultatif – annuler tous les assistants de configuration lancés par le programme d'installation.
17. Modifiez le fichier « /opt/oracle/network/admin/sqlnet.ora » (ou créez le fichier s'il n'existe pas encore) pour contenir ce qui suit (déplacez toutes les informations non commentées existantes dans le fichier) :

    ```
    NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
    ```

18. Pour appliquer le correctif d'Oracle 9.2.0.6 ou 9.2.0.7 au programme d'installation Oracle, à partir du disque 1 de la distribution du Correctif 9.2.0.6 ou 9.2.0.7 Oracle, exécutez le script.

    REMARQUE : Le correctif Oracle 9.2.0.6 n'est pas appliqué, sauf si le programme d'installation Oracle est d'abord corrigé.

    ```
    ./runInstaller
    ```

19. Au fur et à mesure du programme d'installation, laissez les invites avec les valeurs par défaut, sauf indication contraire ci-dessous.
    - Sur l'écran d'accueil, cliquez sur *Suivant*.
    - Sur l'écran Indiquer l'emplacement des fichiers, sélectionnez comme nom cible *OUIHome* dans la liste déroulante (ou tout autre nom que vous avez indiqué comme nome cible lors de l'installation d'Oracle 9.2.0.4). Puis cliquez sur *Suivant*.
    - Sur l'écran Sélectionner produit à installer, sélectionnez *Oracle Universal Installer 10.1.0.3.0*. Puis cliquez sur *Suivant*.
    - Sur l'écran Résumé, révisez le résumé de l'installation, puis cliquez sur *Installer*.
    - Sur l'écran Fin de l'installation, cliquez sur *Quitter*.

20. Pour appliquer le correctif d'Oracle 9.2.0.6 ou 9.2.0.7 à Oracle, à partir du disque 1 de la distribution du Correctif 9.2.0.6 ou 9.2.0.7 Oracle, exécutez le script.

```
./runInstaller
```

21. Au fur et à mesure du programme d'installation, laissez les invites avec les valeurs par défaut, sauf indication contraire ci-dessous.
    - Sur l'écran d'accueil, cliquez sur *Suivant*.
    - Sur l'écran Indiquer l'emplacement des fichiers, sélectionnez comme nom cible « OUIHome » dans la liste déroulante (ou tout autre nom que vous avez indiqué comme nome cible lors de l'installation d'Oracle 9.2.0.4). Puis cliquez sur *Suivant*.
    - En fonction de votre version, sur l'écran Sélectionner produit à installer, sélectionnez *Oracle 9iR2 Patchset 9.2.0.6.0* ou *Oracle 9iR2 Patchset 9.2.0.7.0*. Puis cliquez sur *Suivant*.
    - Sur l'écran Résumé, révisez le résumé de l'installation, puis cliquez sur *Installer*.
    - Sur l'écran Fin de l'installation, cliquez sur *Quitter*.
22. Déconnectez gcc :

```
su – root
rm /usr/bin/gcc
rm /usr/bin/g++
```

23. Quittez pour retourner à l'invite d'utilisateur oracle.

```
exit
```

Installation de Sentinel 5 pour Oracle sur Linux

Sentinel 5 prend en charge deux types d'installation. À savoir :

- simple – option d'installation tout en un : services Sentinel, service collecteur et applications avec Oracle, tout sur la même machine. Ce type d'installation ne sert qu'à des fins de démonstration.
- personnalisée – elle permet une installation totalement distribuée.

Installation simple en Linux

Cette installation installe les composants les plus communs (elle n'inclut pas les fonctions de Collector Builder ou de logiciel d'intégration tiers) sur la même machine. Elle sert surtout à des fins de démonstration. Elle n'est pas recommandée pour l'utilisation dans un environnement de test ou de production.

REMARQUE : l'installation simple ne prend pas en charge l'authentification du mot de passe du gestionnaire de collecteurs.

Comment effectuer une installation simple

1. Vérifiez que vous avez collecté les informations, réalisé les tâches et rempli toutes les conditions définies à la section Préinstallation de Sentinel 5 pour Oracle pour les composants à installer.
2. Vérifiez la configuration de Linux Oracle.
3. Loguez-vous comme utilisateur root.
4. Insérez et montez le CD d'installation de Sentinel.
5. Démarrez le programme d'installation en accédant au répertoire d'installation sur le CD-ROM et entrez :

   En mode GUI :

   ```
   ./setup.sh
   ```

   ou

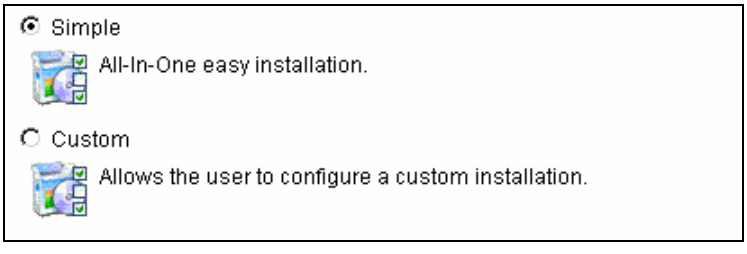
   En mode texte (« headless ») :

   ```
   ./setup.sh -console
   ```

6. Cliquez sur la flèche bas et sélectionnez une des langues suivantes au choix.
   - anglais
   - français
   - allemand
   - italien
   - portugais
   - espagnol

7. Suivez les invites du programme d'installation.
8. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
9. Acceptez l'accord de licence utilisateur final, puis cliquez sur *Suivant*.
10. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* afin d'indiquer l'emplacement de l'installation. Cliquez sur *Suivant.*

11. Sélectionnez *Simple*. Cliquez sur *Suivant.*



12. Entrez les informations de configuration :
    - numéro de série et clé de licence
    - serveur SMTP (nom DNS ou adresse IP), si vous voulez que Sentinel soit capable d'envoyer des messages électroniques.

- courrier électronique – entrez une adresse électronique valide où les messages de notification de l'Advisor doivent être envoyés (par ex. Sent_Server@myserver.com).
- mot de passe global du système – entrez le mot de passe et le mot de passe de confirmation correspondant. Celui-ci devient le mot de passe pour tous les utilisateurs par défaut, y compris l'utilisateur du système d'exploitation esecadm et les utilisateurs de la base de données. Voir Base de données Sentinel, à la section Post-installation de Sentinel 5 pour Oracle, pour consulter la liste des utilisateurs de la base de données par défaut, créée lors de l'installation.
- répertoire de données – l'emplacement pour tous les fichiers de données de la base de données e de la base de données de l'Advisor. Pour changer l'emplacement par défaut, cliquez sur le bouton … et sélectionnez un emplacement. Par défaut correspond à $ESEC_HOME/data.

REMARQUE : Le répertoire de données doit pouvoir être écrit par l'utilisateur Oracle. Ce qui peut être fait en exécutant la commande suivante comme utilisateur root :

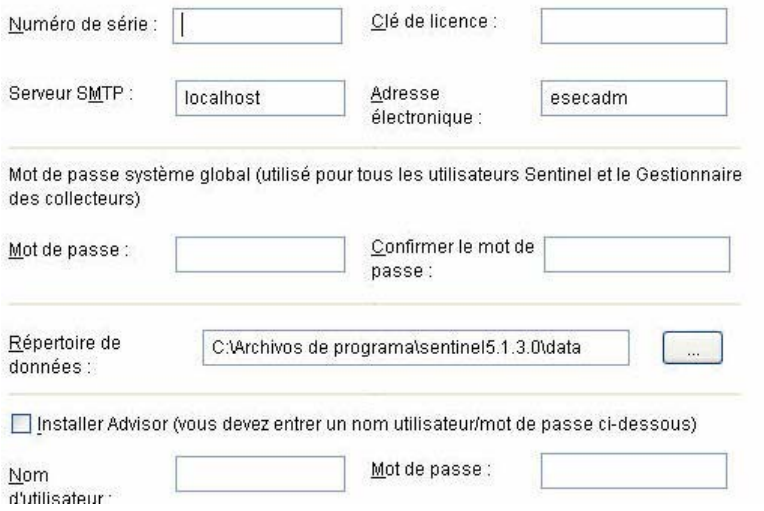
```
chown –R oracle:dba <chemin_répertoire>
chmod –R 770 <chemin_répertoire>
```

en partant du principe qu' « oracle » est le nom d'utilisateur Oracle et « dba » est le nom de groupe « oracle ».

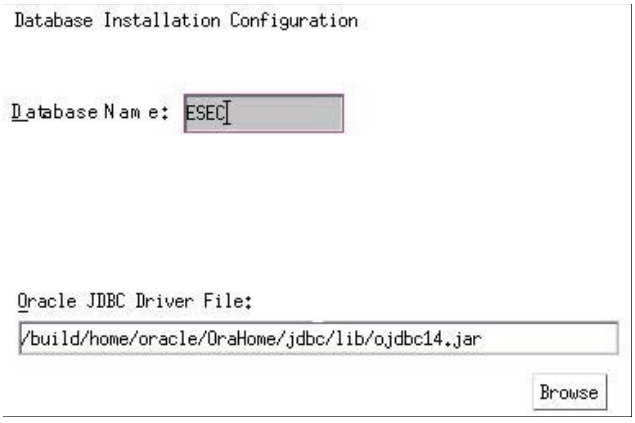
REMARQUE : si vous installez l'Advisor, l'installation simple configure l'Advisor pour utiliser le téléchargement direct d'Internet avec un intervalle de mise à jour de 12 heures et toutes les notifications par messages électroniques activées.

- Pour installer l'Advisor, sélectionnez *Installer Advisor*. Entrez un nom d'utilisateur et un mot de passe. S'il n'est pas possible de vérifier votre nom d'utilisateur ou votre mot de passe, lorsque vous cliquez sur *Suivant*, une invite vous demande si vous voulez continuer (déconseillé). Si vous choisissez de continuer, entrez de nouveau le mot de passe de l'Advisor dans la fenêtre Confirmation de mot de passe. Sinon, corrigez le mot de passe de l'Advisor.

Cliquez sur *Suivant.*



13. Entrez les informations de configuration de la base de données :
    - nom de la base de données – C'est le nom de l'instance de la base de données Oracle pour créer et installer des objets de base de données Sentinel. Aucune base de données portant ce nom ne doit déjà exister.
    - fichier pilote Oracle JDBC. C'est le chemin complet vers le fichier jar, normalement $ORACLE_HOME/jdbc/lib/ojdbc14.jar (impossible d'utiliser des variables d'environnement dans ce champ).



14. Cliquez *OK* sur le nom d'utilisateur oracle par défaut.

15. Lisez les informations sur les écrans qui apparaissent, avant de cliquer sur *Suivant*. Après avoir terminé l'installation, vous devez redémarrer le système.

    REMARQUE : si vous voulez installer un logiciel d'intégration tiers (HP Service Desk ou Remedy Integration), après le redémarrage de la machine, exécutez de nouveau le programme d'installation et sélectionnez le logiciel d'intégration tiers que vous voulez installer. Pour plus d'informations, voir le *guide du logiciel d'intégration tiers*.

16. Par défaut, le programme d'installation désactive l'Archivage de consignations. À des fins de récupération de bases de données, il est fortement recommandé d'activer l'Archivage de consignations après l'installation et avant de commencer à recevoir les données d'évènements de production. Vous devez aussi programmer la sauvegarde des archives de consignations pour libérer de l'espace dans le journal d'archive cible, sinon la base de données ne va plus accepter d'évènements.

Installation personnalisée en Linux

Comment effectuer une installation personnalisée

1. Vérifiez que vous avez collecté les informations, réalisé les tâches et rempli toutes les conditions définies à la section Préinstallation de Sentinel 5 pour Oracle pour les composants à installer.
2. Vérifiez la configuration de Linux Oracle.
3. Loguez-vous comme utilisateur root.
4. Insérez et montez le CD d'installation de Sentinel.

5. Démarrez le programme d'installation en accédant au répertoire d'installation sur le CD-ROM et entrez :

   En mode GUI :

   ```
   ./setup.sh
   ```

   ou

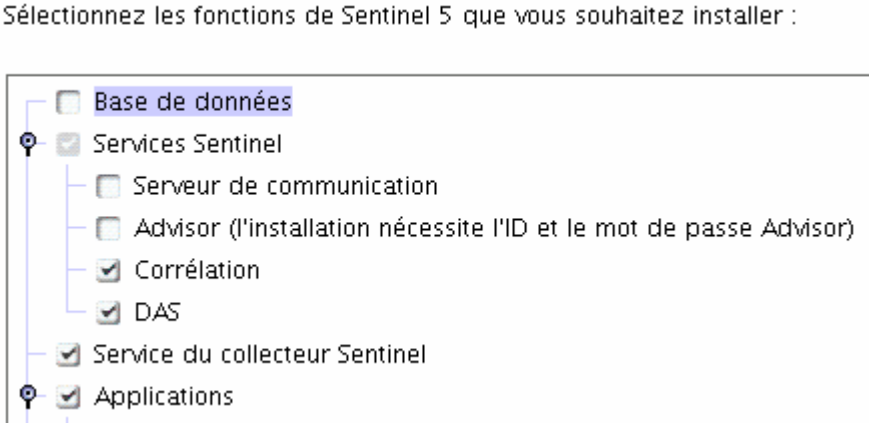
   En mode texte (« headless ») :

   ```
   ./setup.sh –console
   ```

6. Cliquez sur la flèche bas et sélectionnez une des langues suivantes au choix.
   - anglais
   - français
   - allemand
   - italien
   - portugais
   - espagnol
7. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
8. Acceptez l'accord de licence utilisateur final, puis cliquez sur *Suivant*.
9. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* afin d'indiquer l'emplacement de l'installation. Cliquez sur *Suivant.*

10. Sélectionnez *Personnalisée* (par défaut). Cliquez sur *Suivant.*
11. Sélectionnez les fonctions à installer.

REMARQUE : pour plus d'informations concernant le composant qui peut être installé pour les différentes configurations, voir le *chapitre 1 Configuration système requise*.



Les options suivantes sont disponibles :

- base de données – elle installe la base de données Sentinel
- serveur de communication – elle installe le bus de messages (iSCALE)
- Advisor
- Service de collecteurs
- Sentinel Control Center
- collecteur de données Sentinel
- HP OpenView Service Desk**
- Remedy Integration**

- moteur de corrélation
- DAS

REMARQUE : pour 5.1.1 Linux, la fonction des services base Sentinel présente dans la version 5.1.1 pour Windows et Solaris a été incluse dans la fonction d'installation de DAS. L'installation séparée de cette fonction ne présentait apparemment aucun avantage au niveau de la performance.

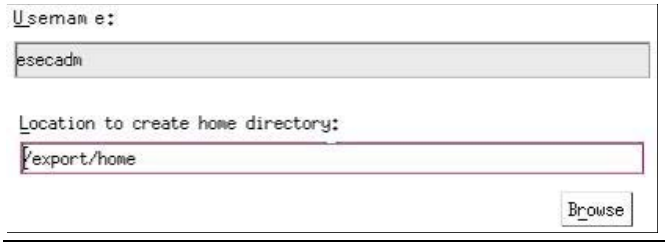
REMARQUE : **Pour plus d'informations sur l'installation de HP OpenView Service Desk ou Remedy Integration, voir le *guide du logiciel d'intégration tiers*.

REMARQUE : si aucune des fonctions enfants de « Sentinel Services » n'est sélectionnée, la fonction « Sentinel Services » doit elle aussi être désélectionnée. Elle apparaît en gris et cochée en blanc si elle est encore sélectionnée alors qu'aucune de ses fonctions enfants n'est sélectionnée.

REMARQUE : pendant l'installation du composant de la base de données Sentinel, le programme d'installation place les fichiers dans le dossier $ESEC_HOME/utilities/db.

REMARQUE : pour l'édition Linux (v5.1.1.1), les composants pris en charge sous Windows sont le générateur de collecteurs et Sentinel Control Center.

12. Si vous avez sélectionné l'installation du DAS, une invite vous demande :
    - le numéro de série
    - la clé de licence
13. Si vous avez sélectionné l'installation d'un logiciel d'intégration tiers (HP Service Desk ou Remedy Integration), vous devrez fournir un mot de passe pour déverrouiller le(s) composant(s) d'intégration tiers sélectionné(s). Pour plus d'informations, voir le *guide du logiciel d'intégration tiers*.
14. Indiquez le nom d'utilisateur de l'administrateur Sentinel du système d'exploitation et l'emplacement de son répertoire privé. Il s'agit du nom d'utilisateur du propriétaire du produit Sentinel installé. Un utilisateur est créé, s'il n'en existe pas encore, ainsi qu'un répertoire privé dans le répertoire indiqué.
    - nom d'utilisateur de l'administrateur du SE – par défaut esecadm
    - répertoire privé de l'utilisateur de l'administrateur du SE – par défaut « /export/home » Si le nom d'utilisateur est esecadm, le répertoire privé de l'utilisateur est /export/home/esecadm.



REMARQUE : si un nouvel utilisateur est créé, son mot de passe doit être défini manuellement, hors du programme d'installation. Sentinel recommande de le faire directement en se loguant dans le système après l'installation du produit.

afin d'accomplir les configurations de sécurité rigoureuses exigées par la certification de critères communs, Sentinel requiert un mot de passe fort avec les caractéristiques suivantes :

1. Choisissez des mots de passe comportant au moins 8 caractères qui incluent au moins un caractère en MAJUSCULE, un caractère en minuscule, un symbole spécial (#$_) et un caractère numérique (0 à 9). N'utilisez pas de vides.

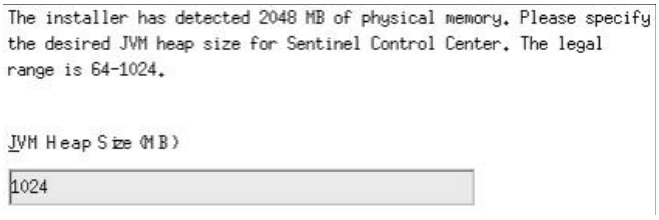
2. Le mot de passe ne peut contenir ni votre adresse électronique, ni aucune partie de votre nom complet.

3. Le mot de passe ne doit pas être un nom commun (par exemple, ce ne doit pas être un mot du dictionnaire ou d'argot d'usage commun).

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

5. Vous devriez choisir un mot de passe facile à mémoriser mais complexe.
Par exemple, Mea5 !A (Mon enfant a 5 ans) OU JhaPdp5#a (J'habite à Paris depuis 5 ans).

15. Si vous sélectionnez l'installation de Sentinel Control Center, une invite taille heap JVM (Java Virtual Machine) apparaît :
    - taille heap JVM (Mo) - par défaut, elle est définie comme la moitié de la taille de la mémoire physique détectée sur la machine, au maximum 1 024 Mo. Elle correspond au maximum de taille heap JVM seulement utilisée par Sentinel Control Center.



16. Si vous décidez d'installer le service de collecteurs, choisissez de protéger ou non le gestionnaire de collecteurs de l'assistant à l'aide d'un mot de passe. Si vous choisissez de protéger le gestionnaire de collecteurs de l'assistant, vous êtes invité à créer un mot de passe du gestionnaire de collecteurs de l'assistant.

REMARQUE : si vous protégez le gestionnaire de collecteurs de l'assistant avec un mot de passe, vous devez entrer ce mot de passe lors du téléchargement ou du débogage des collecteurs dans ce gestionnaire de collecteurs de l'assistant. Ce mot de passe est aussi nécessaire, en plus du nom d'utilisateur Sentinel et du mot de passe correspondant, pour se loguer dans le gestionnaire de collecteurs de l'assistant.
REMARQUE : afin d'accomplir les configurations de sécurité rigoureuses exigées par la certification de critères communs, Sentinel requiert un mot de passe fort avec les caractéristiques suivantes :

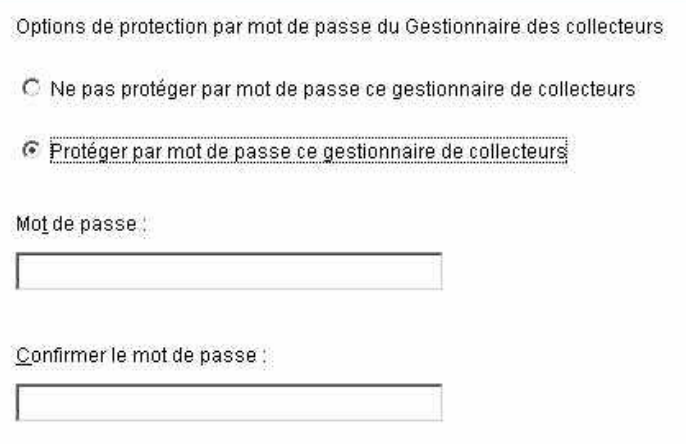
1. Choisissez des mots de passe comportant au moins 8 caractères qui incluent au moins un caractère en MAJUSCULE, un caractère en minuscule, un symbole spécial (!@#$%^&*()_+) et un caractère numérique (0 à 9).

2. Le mot de passe ne peut contenir ni votre adresse électronique, ni aucune partie de votre nom complet.

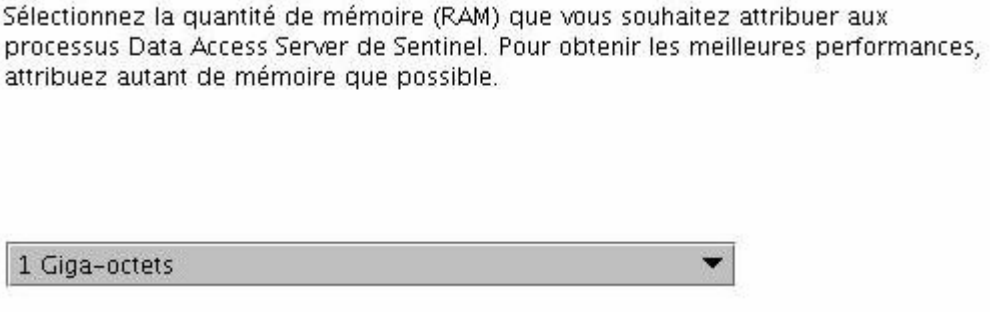
3. Le mot de passe ne doit pas être un nom commun (par exemple, ce ne doit pas être un mot du dictionnaire ou d'argot d'usage commun).

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

5. Vous devriez choisir un mot de passe facile à mémoriser mais complexe. Par exemple, Mea5!A (Mon enfant a 5 ans) OU JhaPdp5#a (J'habite à Paris depuis 5 ans).

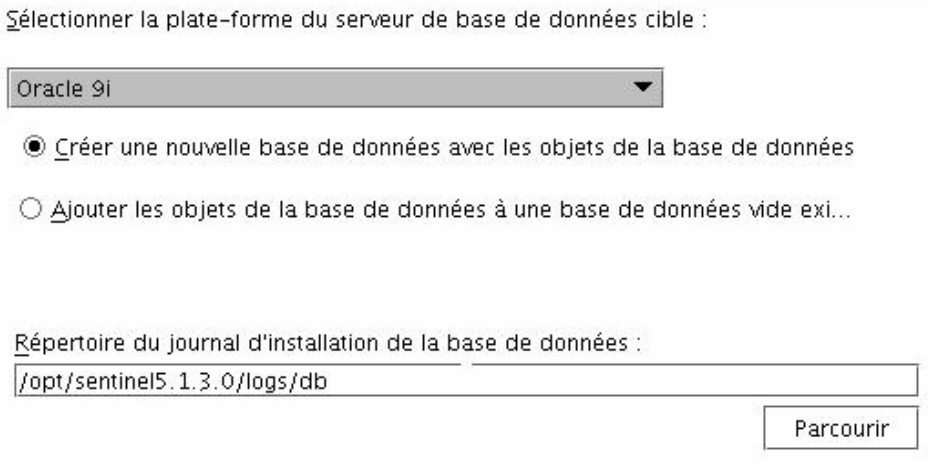


17. Si vous choisissez d'installer le DAS, sélectionnez la quantité de RAM dans le système que vous voulez allouer au DAS (Data Access Service). Pour des environnements distribués, il est recommandé de sélectionner le maximum de mémoire (4 Go). Pour des environnements indépendants, il est recommandé de sélectionner la moitié de la mémoire RAM.



18. Pour l'installation de la base de données, vous avez les invites suivantes.
    a. Sélectionnez Oracle 9i comme plate-forme du serveur de la base de données cible et choisissez une des options suivantes :
        - créer une nouvelle base de données avec des objets de base de données – elle crée une nouvelle base de données Oracle et remplit la nouvelle instance avec des objets de base de données.
        - ajouter des objets de base de données à une base de données existante vide – elle ne fait qu'ajouter la base de données à une instance de la base de données Oracle existante. la base de données existante doit être vide, à l'exception de la présence de l'utilisateur esecdba.

b. Entrez le répertoire journal d'installation de bases de données (par défaut : $ESEC_HOME/logs/db). Acceptez le « Répertoire journal d'installation de la base de données » par défaut ou cliquez sur *Parcourir* afin d'indiquer un emplacement différent.



c. Cliquez *OK* sur le nom d'utilisateur oracle par défaut.

d. Si vous choisissez de créer une nouvelle base de données, entrez ce qui suit :
   - le chemin du fichier pilote Oracle JDBC (le nom type du fichier jar correspond à ojdbc14.jar). C'est le chemin complet vers le fichier jar, normalement $ORACLE_HOME/jdbc/lib/ojdbc14.jar (impossible d'utiliser des variables d'environnement dans ce champ).
   - nom d'hôte – le nom d'hôte de la machine pour installer la base de données Ce champ n'est pas configurable, si une nouvelle instance de base de données est créée.
   - nom de la base de données – nom de l'instance de la base de données à installer

e. Si vous avez choisi d'ajouter des objets de la base de données à une base de données Oracle vide existante, une invite vous demande les informations suivantes :

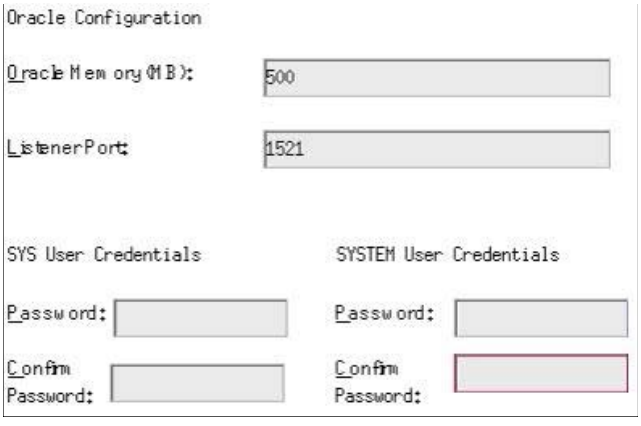
- le chemin du fichier pilote Oracle JDBC (le nom type du fichier jar correspond à ojdbc14.jar). C'est le chemin complet vers le fichier jar, normalement $ORACLE_HOME/jdbc/lib/ojdbc14.jar (impossible d'utiliser des variables d'environnement dans ce champ).
- nom de la base de données ou adresse IP – le nom ou adresse IP de l'hôte où se trouve la base de données Oracle, à laquelle vous voulez ajouter des objets de base de données. Cela peut être le nom d'hôte local ou distant.
- nom de la base de données – nom de l'instance de la base de données Oracle existante, vide, à laquelle vous voulez ajouter des objets de base de données (par défaut, ESEC). Ce nom de base de données doit s'afficher comme un nom de service dans le fichier tnsnames.ora (dans le répertoire ORACLE_HOME/network/admin/) de la machine où le programme d'installation est exécuté.

REMARQUE : si le nom de la base de données n'est pas dans le fichier tnsnames.ora, le programme d'installation n'indique pas encore d'erreur à cette phase de l'installation (parce qu'il vérifie la connexion en utilisant une connexion directe JDBC), mais l'installation de la base de données échoue lorsque le programme d'installation de la base de données tente d'établir la connexion avec la base de données via sqlplus. Si l'installation de la base de données échoue à cette phase, sans quitter le programme d'installation, vous devez modifier le nom de service de cette base de données dans le fichier tnsnames.ora sur cette machine, puis retourner sur l'écran précédent dans le programme d'installation et avancer de nouveau. Cette démarche va réessayer l'installation de la base de données avec les nouvelles valeurs dans le fichier tnsnames.ora.

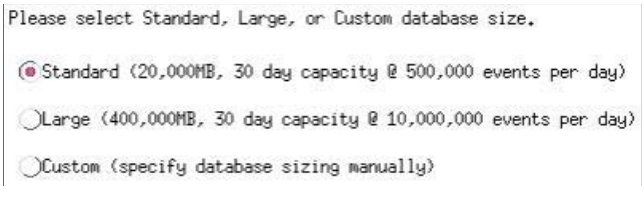
- port de la base de données (par défaut, 1521).
- Pour l'utilisateur de l'administrateur de la base de données Sentinel (DBA), indiquez le mot de passe de l'utilisateur « esecdba ». Le champ nom d'utilisateur de cette invite ne peut pas être édité.

f. Si vous choisissez de créer une nouvelle base de données, l'invite suivante s'affiche :

- mémoire Oracle (Mo) - la quantité de RAM à allouer à cette instance de la base de données Oracle.
- port d'écoute - le port sur lequel est créé l'écouteur Oracle (par défaut, 1521)
- mot de passe de l'utilisateur SYS et confirmation de mot de passe – SYS est l'utilisateur Oracle par défaut qui est créé dans la nouvelle instance de la base de données. Ce mot de passe d'utilisateur est défini avec la valeur indiquée ici.
- mot de passe de l'utilisateur SYSTEM et confirmation de mot de passe – SYSTEM est l'utilisateur Oracle par défaut qui est créé dans la nouvelle instance de la base de données. Ce mot de passe d'utilisateur est défini avec la valeur indiquée ici.



g. Si vous choisissez de créer une nouvelle base de données, une invite vous demande d'entrer la taille de la base de données. Vous avez les options suivantes :
   - standard (20 Go)
   - grande (400 Go)
   - personnalisée (indiquez la taille manuellement). Si vous sélectionnez cette option, une invite vous demande :
     - taille initiale de chaque fichier de la base de données en Mo (de 100 à 10 000)
     - taille maximum de chaque fichier de la base de données en Mo (de 2 000 à 100 000)
     - taille de tous les fichiers de la base de données en Mo (de 7 000 à 2 000 000)
     - taille de chaque fichier journal en Mo (de 100 à 100 000)



h. Si vous choisissez de créer une nouvelle base de données, une invite vous demande d'entrer l'emplacement d'archivage des fichiers de base de données suivants :

REMARQUE : à des fins de récupération et de performance, nous recommandons que ces emplacements soient dans des périphériques E/S différents.

Le programme d'installation ne crée pas ces répertoires, ils doivent donc être créés à l'extérieur avant de franchir cette étape.

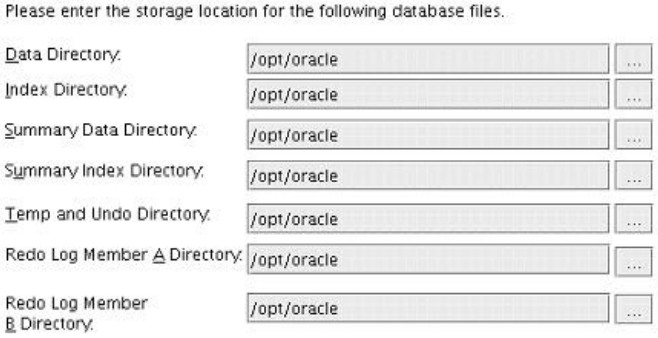
Ces répertoires doivent être accessibles en écriture pour l'utilisateur oracle. Pour que ces répertoires puissent être écrits par l'utilisateur oracle, exécutez les commandes suivantes pour chaque répertoire comme utilisateur root :

```
chown –R oracle:dba <chemin_répertoire>
chmod –R 770 <chemin_répertoire>
```

---

en partant du principe qu' « oracle » est le nom d'utilisateur Oracle et « dba » est le nom de groupe « oracle ».

- répertoire de données
- répertoire d'index
- répertoire de données récapitulatif
- répertoire d'index récapitulatif
- répertoire temporaire et d'annulation d'espaces de table
- journal des répétitions du répertoire du membre A
- journal des répétitions du répertoire du membre B



i. Si vous choisissez de créer une nouvelle base de données, entrez les informations d'authentification de l'administrateur de la base de données Sentinel. C'est esecdba, le propriétaire des objets de la base de données.

j. Entrez les informations d'authentification de l'utilisateur de la base de données de l'application Sentinel. C'est esecapp, le nom de l'utilisateur de l'application Sentinel que les procédures Sentinel utilisent pour se connecter à la base de données.

k. Entrez les informations d'authentification de l'utilisateur de la base de données de l'administrateur Sentinel. C'est esecadm, l'utilisateur de l'administrateur Sentinel.

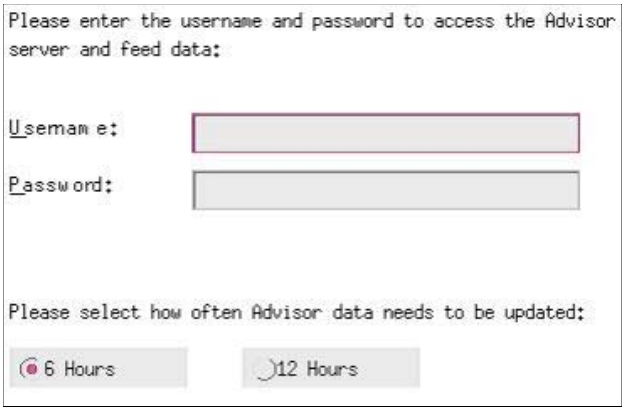
l. Cliquez sur *Suivant* dans la fenêtre récapitulative de l'installation de la base de données.

19. Si vous avez choisi d'installer le DAS mais pas la base de données Sentinel, une invite vous demande les informations suivantes sur la base de données Oracle Sentinel. Ces informations sont utilisées pour configurer le DAS afin qu'il soit ciblé sur la base de données Sentinel.
    - nom d'hôte de la base de données ou adresse IP – C'est le nom ou l'IP de la base de données Oracle Sentinel existante à laquelle vous voulez connecter le composant DAS.
    - nom de la base de données – nom de l'instance de la base de données Oracle existante, vide, à laquelle vous voulez connecter le composant DAS (par défaut, ESEC).
    - port de la base de données (par défaut, 1521).
    - Pour l'utilisateur de la base de données de l'application Sentinel, indiquez le login « esecapp » et entrez le mot de passe donné à cet utilisateur lors de l'installation de la base de données Sentinel.

20. Si vous choisissez d'installer le DAS, configurez le support du courrier électronique Sentinel. Indiquez le serveur SMTP et l'adresse expéditeur que le Service d'exécution doit utiliser pour envoyer des messages (facultatif : vous pouvez éditer cela manuellement après avoir installé [$ESEC_HOME\sentinel\config\execution.properties]) :

21. Si vous choisissez d'installer l'Advisor, sélectionnez le type d'installation Advisor (si l'option Advisor est choisie, un nom d'utilisateur et un mot de passe).
    - Téléchargement direct d'Internet – la machine Advisor est directement connectée à Internet. Dans cette configuration, les mises à jour de Sentinel sont automatiquement téléchargées de Sentinel sur Internet, à un rythme régulier.
    - Indépendant – l'Advisor est configuré comme un système isolé qui requiert une intervention manuelle pour recevoir des mises à jour du Sentinel.

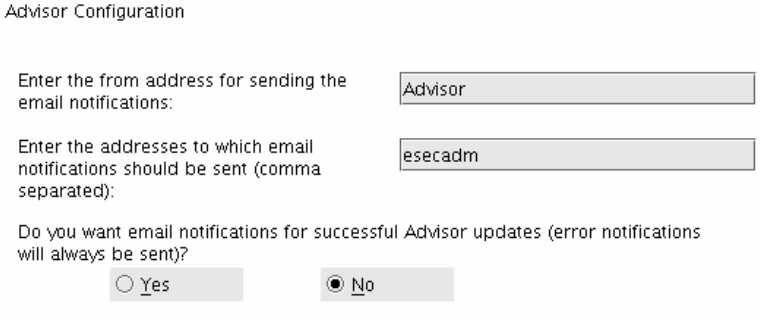
22. Si vous choisissez d'installer l'Advisor et sélectionnez l'option de téléchargement direct d'Internet, entrez le nom d'utilisateur de l'Advisor, le mot de passe, ainsi que le rythme souhaité des mises à jour de l'Advisor. S'il n'est pas possible de vérifier votre nom d'utilisateur ou votre mot de passe, lorsque vous cliquez sur *Suivant*, une invite vous demande si vous voulez continuer (déconseillé). Si vous choisissez de continuer, entrez de nouveau le mot de passe de l'Advisor dans la fenêtre Confirmation de mot de passe. Sinon, corrigez le mot de passe de l'Advisor.



23. Si vous choisissez d'installer l'Advisor, entrez :
    - adresse expéditeur, qui apparaît dans les notifications par message électronique
    - adresse destinataire, pour l'envoi de notifications par message électronique :

REMARQUE : après l'installation, vous pouvez changer les adresses électroniques de l'Advisor, en éditant les fichiers attackcontainer.xml et alertcontainer.xml. dans le répertoire $ESEC_HOME/sentinel/config directory. Pour plus d'informations, voir *le chapitre 7, L'onglet Advisor* dans le *guide d'utilisateur Sentinel*.

    - Sélectionnez Oui si vous voulez recevoir des messages électroniques concernant les mises à jour réussies de l'Advisor, ou Non dans le cas contraire. Les notifications d'erreurs sont toujours envoyées.



24. Si vous choisissez d'installer HP OpenView Service Desk ou Remedy Integration, une invite vous demande des informations supplémentaires. Pour plus d'informations, voir le *guide du logiciel d'intégration tiers Sentinel*.
25. Lisez les informations sur les écrans qui apparaissent, avant de cliquer sur *Suivant*. Une fois l'installation terminée, une invite vous demande de redémarrer. Cliquez sur *Terminer* pour redémarrer le système.

26. Par défaut, le programme d'installation désactive l'Archivage de consignations. À des fins de récupération de bases de données, il est fortement recommandé d'activer l'Archivage de consignations après l'installation et avant de commencer à recevoir les données d'évènements de production. Vous devez aussi programmer la sauvegarde des archives de consignations pour libérer de l'espace dans le journal d'archive cible, sinon la base de données ne va plus accepter d'évènements.
27. Si vous prévoyez un taux d'évènements élevé (supérieur à 500 évènements par seconde), vous devez suivre les instructions de configuration supplémentaires de la section Configurer la stratégie d'insertion d'évènements d'objets de l'interface d'appel Oracle (OCI – Oracle Call Interface).

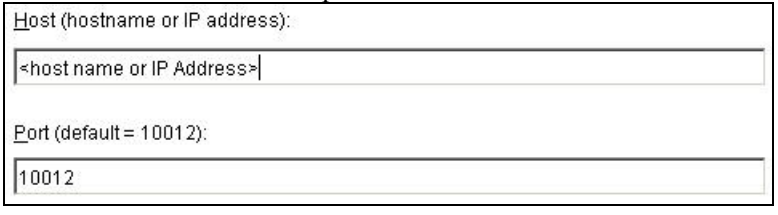
Installation de Sentinel Control Center et du générateur de collecteurs sous Windows

Installation de Sentinel Control Center et du générateur de collecteurs sous Windows

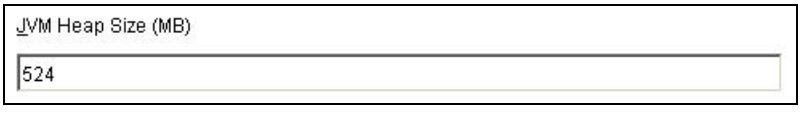
1. Insérez le CD d'installation Sentinel dans l'unité de CD-ROM.
2. Parcourez le CD et double-cliquez sur *setup.bat*.

   REMARQUE : l'installation en mode de console n'est pas prise en charge sous Windows.
3. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
4. Acceptez l'accord de licence utilisateur final, puis cliquez sur *Suivant*.
5. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* afin d'indiquer l'emplacement de l'installation. Cliquez sur *Suivant.*

6. Sélectionnez les fonctions à installer.
7. Entrez l'adresse d'hôte et le port où le serveur de communication est installé.



8. Si vous sélectionnez l'installation de Sentinel Control Center, une invite JVM (Java Virtual Machine) apparaît :
   - taille heap JVM (Mo) - par défaut, elle est définie comme la moitié de la taille de la mémoire physique détectée sur la machine, au maximum 1 024 Mo. Elle correspond au maximum de taille heap JVM seulement utilisée par Sentinel Control Center.



   Cliquez sur *Suivant.*

9. Cliquez sur *Installer*.
10. Lisez les informations sur les écrans qui apparaissent, avant de cliquer sur *Suivant*. Cliquez sur *Terminer*.

Post-Installation de Sentinel 5 pour Oracle

Mise à jour du courrier électronique Sentinel pour l'authentification SMTP

Si le système requiert une authentification SMTP, vous devez mettre à jour le fichier execution.properties. Ce fichier est sur la machine où le DAS est installé. Il est localisé à $ESEC_HOME/sentinel/config. Pour configurer ce fichier, exécutez mailconfig.sh pour changer le fichier et mailconfigtest.sh pour tester ces changements.

Pour configurer le fichier execution.properties

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfig de la façon suivante :

   ```
   ./mailconfig.sh -host <serveur SMTP> -from <adresse
      électronique source> -user <utilisateur
      authentification courrier électronique> –password
   ```

   Exemple :

   ```
   mailconfig.bat -host 10.0.1.14 -from nom@domaine.com -
      user nom_utilisateur –password
   ```

   Après cette commande, une invite vous demande d'entrer un nouveau mot de passe.

   ```
   Entrez le mot de passe :*********
   Confirmez le mot de passe :*********
   ```

REMARQUE : lors de l'utilisation de l'option de mot de passe, ce doit être le dernier argument.

Pour tester la configuration d'execution.properties

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfigtest de la façon suivante :

   ```
   ./mailconfigtest.sh -to <adresse électronique cible>
   ```

   Si l'envoi du message électronique a abouti, vous obtenez le résultat suivant sur l'écran et le message est reçu à l'adresse cible.

   ```
   Message électronique envoyé avec succès !
   ```

   Vérifiez la boîte aux lettres de l'adresse cible pour confirmer la réception du message. La ligne d'objet et le contenu devraient être les suivants :

```
Objet : Test des propriétés du courrier électronique
   Sentinel

Test de configuration des propriétés du courrier
   électronique Sentinel. Si ce message apparaît, les
   propriétés du courrier électronique Sentinel ont été
   correctement configurées pour envoyer des messages.
```

Base de données Sentinel

Après l'installation de la base de données Sentinel, la base de données contient les utilisateurs suivants par défaut :

- esecdba – propriétaire de schéma de la base de données. Le privilège DBA n'est pas attribué à esecdba pour des raisons de sécurité. Pour utiliser l'Enterprise Manager, créez un utilisateur avec des privilèges DBA.
- esecapp – utilisateur de l'application de la base de données. C'est l'utilisateur de l'application utilisé pour la connexion avec la base de données.
- esecadm – utilisateur de la base de données qui est l'administrateur Sentinel. Ce n'est pas le même compte utilisateur que celui de l'utilisateur du système d'exploitation esecadm.
- esecrpt – utilisateur de rapports de la base de données
- SYS – utilisateur de la base de données SYS
- SYSTEM – utilisateur de la base de données SYSTEM

Service de collecteurs

Lors de l'installation du service de collecteurs, les collecteurs suivants sont installés et chacun possède un port de collecteur pour son exécution.

Produit	**Nom de collecteur**
Collecteurs démo	
Test de téléchargement d'actifs, travaille avec le collecteur DemoEvents	DemoAssetUpload
Test d'évènements démo, travaille avec les collecteurs DemoAssetUpload et DemoVulnerabilityUpload	DemoEvents
Test de téléchargement de vulnérabilité, travaille avec le collecteur DemoEvents	DemoVulnerabilityUpload
Test d'envoi d'un évènement	SendOneEvent
Test d'envoi de plusieurs évènements	SendMultipleEvents

REMARQUE : pour plus d'informations sur la configuration des collecteurs démo, voir le *chapitre 12, Tester l'installation*.

REMARQUE : pour plus de collecteurs, veuillez consulter le Sentinel Customer Portal afin d'obtenir le Service Pack le plus récent, pour la version que vous venez d'installer. Le Service Pack le plus récent pour l'édition que vous utilisez contient l'ensemble complet des derniers collecteurs disponibles pour la version de Sentinel que vous utilisez.

Pour plus d'informations (y compris la configuration), voir la documentation fournie avec chaque collecteur à :

$WORKBENCH_HOME/Elements/<nom_collecteur>/Docs/

Pour installer d'autres collecteurs, exécutez le script Service Pack sur le CD Service Pack. Ce script installe les collecteurs localement.

Sous Windows :

```
.\service_pack.bat
```

Sur UNIX :

```
./service_pack.sh
```

Pour lire les instructions d'installation du Service Pack et la liste des collecteurs, voir les *notes de publication du Service Pack.*

Mise à jour de la clé de licence

Comment mettre à jour la clé de licence (Linux)

1. Loguez-vous comme utilisateur esecadm.
2. Insérez et montez le CD d'installation de Sentinel.
3. Dans le cd, allez à disque1/utilities/linux.
4. Entrez la commande suivante :

   ```
   ./softwarekey
   ```

5. Entrez le numéro 1 pour entrer la clé principale. Appuyez sur Enter.

Création d'une instance Oracle pour la base de données Sentinel

REMARQUE : cette procédure est fournie comme exemple si vous voulez créer des espaces de table à l'aide de la fonction de création d'espaces de table incluse sur le CD d'installation. Les valeurs de la taille peuvent varier en fonction de la configuration et des conditions requises du système. Les espaces de table doivent être nommés exactement comme suit.

Sur l'instance Oracle, vous devez configurer :

- les paramètres
- les espaces de table

Création d'une instance Oracle

1. Loguez-vous comme utilisateur oracle.
2. À l'aide du GUI assistant de la base de données Oracle, créez ce qui suit :

REMARQUE : les valeurs peuvent varier en fonction de la configuration et des conditions requises du système.

Paramètres minimaux recommandés pour la configuration Linux	
Paramètres	**Taille (octets ou tout autre indiqué)**
db_cache_size	1 Go
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 Mo
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAIRE
hash_join_enabled	VRAI
optimizer_index_caching	50
optimizer_index_cost_adj	55

Taille minimale recommandée pour les espaces de table Linux		
Espace de table	**Taille exemple**	**Remarques**
REDO	3 x 100M	Valeur minimale. Vous devez créer des journaux de répétition plus grands si vous avez un EPS élevé.
SYSTEM	500M	Valeur minimum
TEMP	1G	Valeur minimum
UNDO	1G	Valeur minimum
ESENTD	5G	Valeur minimum Pour des données d'évènements
ESENTD2	500M	Valeur minimum Données pour configuration, actifs, vulnérabilité et associations (extension automatique activée)
ESENTWFD	250M	Pour données iTrac (extension automatique activée)
ESENTWFX	250M	Pour index iTrac (extension automatique activée)
ESENTX	3G	Valeur minimum Pour index d'évènements
ESENTX2	500M	Valeur minimum Index pour configuration, actifs, vulnérabilité et associations (extension automatique activée)

Taille minimale recommandée pour les espaces de table Linux		
Espace de table	**Taille exemple**	**Remarques**
SENT_ADVISORD	200M	Valeur minimum Pour données Advisor (extension automatique activée)
SENT_ADVISORX	100M	Valeur minimum Pour index Advisor (extension automatique activée)
SENT_LOBS	100M	Valeur minimum Pour grands objets de base de données (extension automatique activée)
SENT_SMRYD	3G	Valeur minimum Pour regroupement, données récapitulatives
SENT_SMRYX	2G	Valeur minimum Pour regroupement, index récapitulatif

3. Exécutez le script createEsecdba.sh qui se trouve dans le répertoire sentinel\dbsetup\bin sur le CD d'installation Sentinel. Ce script créé l'utilisateur esecdba qui est nécessaire pour ajouter des objets de la base de données à l'aide du programme d'installation Sentinel.
4. Sauvegardez la base de données.

Configuration de la stratégie d'insertion d'évènements de l'interface d'appel Oracle (OCI – Oracle Call Interface)

Sentinel 5.1 fournit une structure pour l'intégration de différentes stratégies afin d'insérer des évènements dans une base de données. Sentinel 5.1 fournit deux stratégies pour insérer des évènements dans la base de données Oracle.

- JDBCLoadStrategy
- OCILoadStrategy

La stratégie à utiliser pour l'insertion d'évènements est régie par la propriété insert.strategy du composant EventStoreService dans das_binary.xml.

La stratégie JDBC est la stratégie par défaut configurée au départ.

La stratégie OCI est une stratégie d'insertion native pour insérer les évènements plus rapidement. Cette stratégie requiert l'installation des bibliothèques Oracle OCI sur la machine où le composant DAS est exécuté. La stratégie OCI doit être utilisée dans les configurations qui requièrent un taux d'évènements élevé.

Le nombre d'évènements à regrouper pour être insérés dans la base de données est régi par la propriété insert.batchsize. Cette propriété insert.batchsize est utilisée par toutes les stratégies d'insertion d'évènements.

Pour changer de stratégie d'insertion d'évènements de Sentinel en passant de la stratégie d'insertion JDBC par défaut à la stratégie d'insertion OCI, il faut exécuter certaines étapes.

Passer de la stratégie d'insertion d'évènements JDBC à la stratégie d'insertion OCI

1. Vérifiez que les bibliothèques Oracle OCI sont installées sur la machine où le composant Sentinel DAS est exécuté. Vous devrez connaître le chemin d'ORACLE_HOME dans les étapes suivantes.
2. Loguez-vous sur la machine dès l'étape 1 comme utilisateur esecadm.
3. Créez un « bash_profil » dans le répertoire privé de l'utilisateur esecadm. Entrez le texte suivant dans ce fichier (modifiez le chemin d'ORACLE_HOME pour être conforme à l'installation) :

   ```
   ORACLE_HOME=/build/home/oracle/OraHome
   export ORACLE_HOME
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
   export LD_LIBRARY_PATH
   ```

4. Ouvrez le fichier $ESEC_HOME/sentinel/config/das_binary.xml pour l'édition dans un éditeur de texte, quel qu'il soit.
5. Effectuez une recherche du texte suivant :

   ```
   JDBCLoadStrategy
   ```

6. Transformez le texte en :

   ```
   OCILoadStrategy
   ```

7. Enregistrez ce changement dans le fichier das_binary.xml.
8. Redémarrez l'application DAS Binary. (La manière la plus facile d'effectuer cette opération consiste à exécuter « ps –ef | grep DAS_Binary » pour obtenir l'ID de processus, détruire le processus puis permettre à l'application de surveillance Sentinel de le redémarrer.)

   Après le redémarrage de l'application DAS Binary, la bibliothèque $ESEC_HOME/sentinel/lib/libocievent.so est chargée et utilisée pour effectuer les insertions d'évènements dans la base de données via OCI.

Options supplémentaires d'insertion d'évènements OCI

Outre la spécification du « OCILoadStrategy » dans le fichier das_binary.xml, plusieurs autres options liées à l'OCI peuvent être configurées.

- insert.batchsize – ce paramètre vous permet de configurer le maximum d'évènements à insérer dans une base de données en une seule fois.
- insert.oci.workerCount – ce paramètre vous permet de configurer le nombre de threads utilisés pour insérer des données d'évènements dans la base de données.
- insert.oci.queueWaitTime – ce paramètre indique l'attente maximum en secondes avant d'insérer les données depuis la file d'attente entrante dans la base de données. Lorsqu'un lot complet d'évènements est reçu, tout le lot est inséré. Mais si le flux entrant d'évènements est lent, la période d'attente est utilisée pour déterminer le moment de l'insertion de la base de données (même si un lot complet d'évènements n'a pas encore été reçu).
- insert.oci.highWatermark – le haut filigrane de la file d'attente d'évènements entrants.
- insert.oci.lowWatermark – le bas filigrane de la file d'attente d'évènements entrants.
- insert.oci.optimizationFlag – drapeau d'optimisation « actif » ou « inactif »

Conseils de débogage OCI

L'interface OCI enregistre des messages dans le fichier $ESEC_HOME/sentinel/log/ocievent.log. Les messages initiaux enregistrés dans le fichier journal incluent des messages de connexion à la base de données réussis (ou échoués)… C'est le lieu adéquat pour vérifiez si la bibliothèque OCI a été correctement chargée et configurée.

L'interface OCI enregistre aussi les erreurs dans le fichier journal das_binary localisé dans le répertoire $ESEC_HOME/sentinel/log. Les erreurs enregistrées dans le fichier journal das_binary comprennent les échecs de localisation/chargement de la bibliothèque libocievent.so, les échecs de connexion à la base de données et les échecs d'insertions d'évènements et d'associations d'évènements.

Si les messages d'erreur indiquent que le fichier « libocievent.so » n'est pas localisé ni chargé, il faut vérifier trois éléments :

1. Assurez-vous que les bibliothèques Oracle OCI sont installées.
2. Assurez-vous que le fichier « libocievent.so » est localisé dans le répertoire $ESEC_HOME/sentinel/lib.
3. Assurez-vous que le répertoire $ESEC_HOME/sentinel/lib est dans le chemin « LD_LIBRARY_PATH » de l'utilisateur « esecadm ». Sinon, vous pouvez mettre à jour le LD_LIBRARY_PATH dans le profil de l'utilisateur « esecadm ».
4. Assurez-vous que les variables d'environnement ORACLE_HOME et LD_LIBRARY_PATH sont correctement mises à jour dans les variables d'environnement de l'utilisateur esecadm, comme mentionné dans la section « Passer de la stratégie d'insertion d'évènements JDBC à la stratégie d'insertion OCI ».

5 Installation de Sentinel 5 pour MS SQL

REMARQUE : le terme « agent » est échangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Ce chapitre décrit le mode d'installation de Sentinel Enterprise Security Management Sentinel 5 pour MS SQL

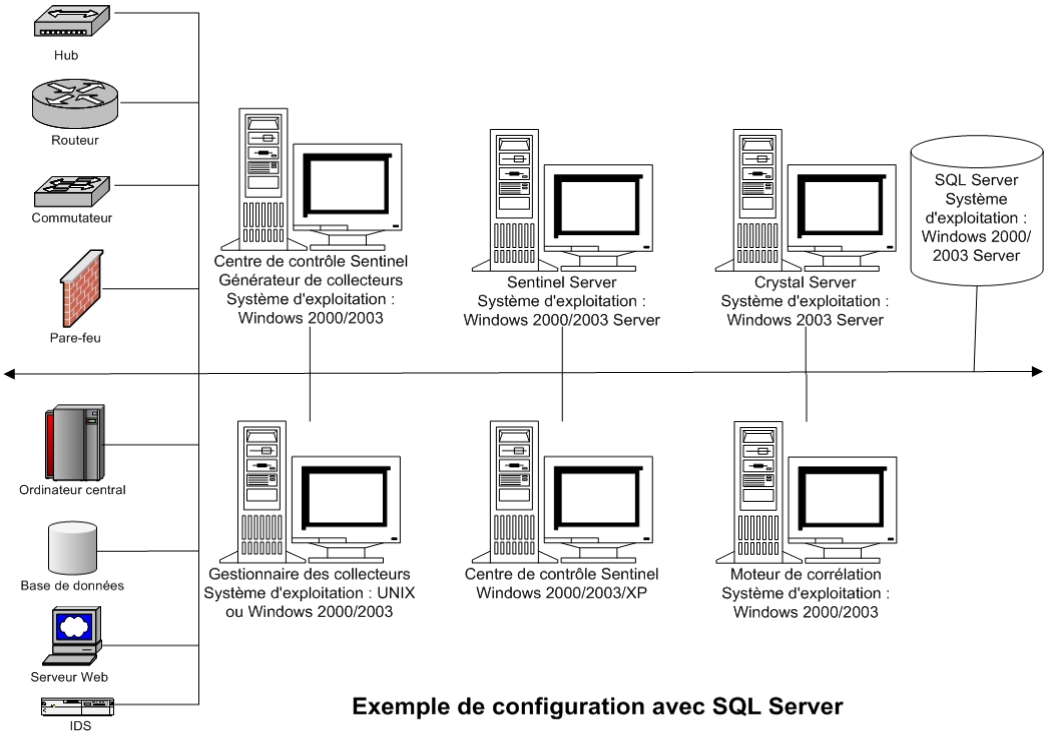
Préinstallation de Sentinel 5 pour MSSQL

REMARQUE : avant l'installation, vérifiez que les machines sont bien conformes à la configuration système minimale requise et que le système d'exploitation a été renforcé selon les bonnes pratiques de sécurité actuelles.

REMARQUE : Sentinel ne prend pas en charge pas la mise en grappe MS ni la haute disponibilité pour Windows.

REMARQUE : si vous effectuez une nouvelle installation de Sentinel sur un ordinateur sur lequel une version précédente de Sentinel avait été installée, vous devrez supprimer certains fichiers et paramètres système qui peuvent toujours subsister Si ces fichiers ou paramètres ne sont pas éliminés, la toute nouvelle installation peut échouer. Vous devriez le faire sur chaque machine où vous exécutez une nouvelle installation. Pour plus d'informations, voir *l'annexe E*.

Vous trouverez ci-dessous une configuration type de Sentinel. Votre configuration peut être différente, en fonction de l'environnement. Indépendamment de la configuration choisie, vous devez d'abord installer la base de données.



Exemple de configuration avec SQL Server

REMARQUE : pour plus d'informations concernant les systèmes d'exploitation pris en charge, voir le chapitre 1 *Introduction, plates-formes prises en charge pour le serveur Sentinel sous Windows.*

Obtention d'une clé de licence

Le Database Access Service (DAS) du serveur Sentinel exige que vous ayez une clé de licence valide afin d'installer et exécuter le service. Cette clé de licence est verrouillée à la machine où le DAS est installé. Une clé de licence délivrée pour une machine ne marche pas sur une autre.

Pour obtenir la clé de licence, vous devez déterminer le numéro de ID d'hôte et passer cette information à Novell qui vous attribuera une clé de licence.

Pour déterminer l'ID d'hôte :

1. Insérez le CD d'installation Sentinel sur l'unité de CD-ROM.
2. Parcourez le répertoire d'outils sur le CD.
3. Exécutez le fichier exécutable :

   ```
   hostid.exe
   ```

4. Donnez ce numéro d'ID d'hôte au support technique de Novell. Il vous fournira une clé de licence.

Base de données Sentinel

Avant d'installer le serveur Sentinel, vous avez besoin de :

- Pour connaître la configuration matérielle requise, voir les *chapitres 1 et 2*.

- Windows 2000 Server avec Service Patch 4 ou Windows 2003 Server avec Service Patch1
- SQL Server 2000 Enterprise Edition Service Pack 3a ou SQL Server 2005 Enterprise Addition (Sentinel v5.1.1 SP1 et versions ultérieures) installé et en exécution.

REMARQUE : pour des raisons de performance, il est FORTEMENT recommandé que le journal des transactions soit ciblé sur le disque d'écriture disponible le plus rapide, si vous installez en RAID et si l'environnement RAID le permet.

REMARQUE : si vous avez installé SQL Server avec l'authentification en mode mixte, vous pouvez vous loguer avec le login Windows ou à l'aide de l'authentification de SQL Server. Pour le mode non-mixe, vous devez vous loguer para l'authentification Windows.

Pour changer les paramètres du mode d'authentification, dans SQL Enterprise Manager, cliquez avec le bouton droit sur le serveur dont vous souhaitez modifier les paramètres (par défaut : (local)(Windows NT)), sélectionnez *propriétés*, cliquez sur l'onglet Sécurité et sélectionnez *SQL Server et Windows* ou *Seulement Windows* pour l'authentification. Le compte de service de démarrage devrait être défini comme *Compte du système*.

- nom de l'instance de SQL Server cible – (défaut recommandé).

REMARQUE : si vous avez déjà nommé l'instance pendant l'installation de SQL Server, utilisez ce nom à l'invite pour le nom de l'instance de SQL Server, lors de l'installation de la base de données et/ou des composants DAS. Si vous n'avez pas nommé l'instance pendant l'installation de SQL Server, laissez le nom de l'instance en blanc pendant l'installation (c'est-à-dire que si vous insérez le nom d'hôte, n'ajoutez pas « \<nom_instance> » au nom d'hôte de la base de données.

- numéro de port de l'instance de SQL Server cible – (par défaut 1433).
- Si vous utilisez l'authentification Windows pour un ou plusieurs utilisateurs Sentinel, le domaine Windows correspondant doit exister avant d'installer la base de données Sentinel. Les utilisateurs Sentinel suivants peuvent être attribués à un utilisateur de domaine Windows :
  - Sentinel Database Administrator – utilisateur de schéma de base de données (par ex. esecdba)
  - Sentinel Application User – utilisé par les applications Sentinel pour se connecter à la base de données (par ex. esecapp)
  - Sentinel Administrator – administrateur pour consignation dans l'application Sentinel Control Center (par ex. esecadm)
  - Sentinel Report User – utilisé pour la création de rapports (par ex. esecrpt)

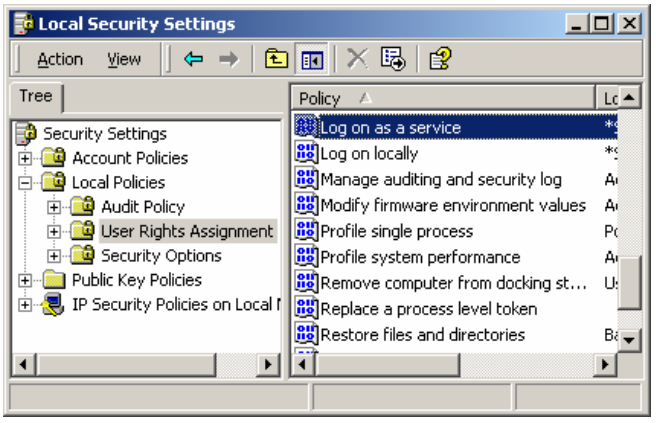
Serveur Sentinel

REMARQUE : si vous n'installez pas la base de données Sentinel et le serveur Sentinel en même temps, la base de données Sentinel doit être installée en premier.

Avant d'installer le serveur Sentinel, vous avez besoin de :

- Pour connaître la configuration matérielle requise, voir les *chapitres 1 et 2*.
- Windows 2000 Server avec Service Patch 4 ou Windows Server 2003 avec Service Patch 1
- Le numéro de série de Sentinel 5 et la clé de licence (pour DAS). Pour plus d'informations, voir Obtention d'une clé de licence.
- Si vous installez le DAS et utilisez le compte utilisateur de domaine Windows pour l'utilisateur de l'application Sentinel, vous devez donner à cet utilisateur le privilège de

« se loguer comme un service ». À cet effet, ouvrez le panneau de configuration « Stratégie de sécurité locale » sur la machine où vous allez installer le DAS *(Démarrer > Paramètres > Panneau de configuration > Outils administratifs > Stratégie de sécurité locale).* Sur la fenêtre Stratégie de sécurité locale, allez à *Stratégies locales > Assignation des droits d'utilisateur.* Ouvrez la stratégie *Se loguer comme un service* et ajoutez l'utilisateur.



- serveur SMTP – nécessaire pour envoyer un message électronique à partir de Sentinel.

Sentinel Control Center et Wizard

Avant d'installer le serveur Sentinel, vous avez besoin de :

- Pour connaître la configuration matérielle requise, voir les *chapitres 1 et 2*.
- Windows 2000 Server avec Service Patch 4 ou Windows 2003 Server avec Service Patch 1

Advisor

Pour installer l'Advisor, il vous faut obtenir un ID Advisor et un mot de passe de Novell. Le téléchargement direct d'Internet utilise le port 443.

REMARQUE : si vous pensez n'utiliser l'Advisor que pour la détection d'exploits, il n'est pas nécessaire d'installer le logiciel Crystal Enterprise. Cela n'est nécessaire que si vous avez l'intention d'utiliser les rapports Crystal pour Sentinel. Voir le *chapitre 10, Configuration de l'Advisor*, pour plus d'informations.

Installation de Sentinel 5 pour MS SQL

Sentinel 5 prend en charge deux types d'installation. À savoir :

- simple – option d'installation tout en un : services Windows Sentinel, service collecteur et applications avec le serveur MS SQL, tout sur la même machine. Il ne prend en charge que l'authentification de SQL Server). Ce type d'installation ne sert qu'à des fins de démonstration.
- personnalisée – elle permet une installation totalement distribuée.

REMARQUE : par défaut, le programme d'installation définit les groupes de fichiers suivants pour NE PAS croître automatiquement : ESENTD, ESENTX, SENT_SMRYD et SENT_SMRYX. Tous les autres groupes de fichiers sont définis pour grandir automatiquement. Les espaces de tables ESENTD, ESENTX, SENT_SMRYD et SENT_SMRYX ne peuvent pas croître automatiquement parce qu'ils contiennent des évènements et des données d'évènements récapitulatives. L'utilisation de l'espace des évènements et des résumés peut être très dynamique.

Ces groupes de fichiers d'évènements devraient être contrôlés et élargis de façon contrôlée selon la configuration du système de fichiers et en respectant l'équilibre E/S et la sauvegarde et récupération de la base de données.

La gestion de partitions SDM (archivage, déplacement et ajout des partitions) devrait être programmée pour maintenir les données d'évènements à une taille contrôlée.

Installation simple

Cette installation installe tous les composants (y compris la base de données) sur une seule plate-forme et ne prend en charge que l'authentification de SQL Server. Elle sert surtout à des fins de démonstration. Elle n'est pas recommandée pour des tests ou une utilisation en production.

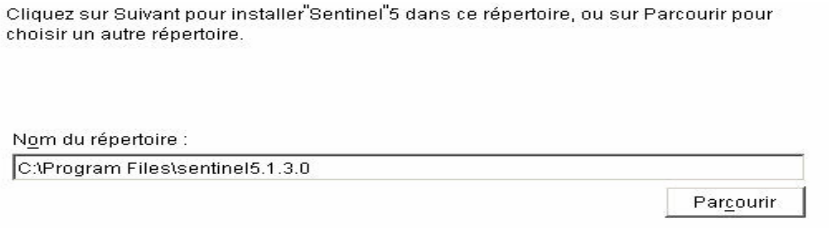
REMARQUE : l'installation simple ne prend pas en charge l'authentification du mot de passe du gestionnaire de collecteurs.

Installation simple de Sentinel

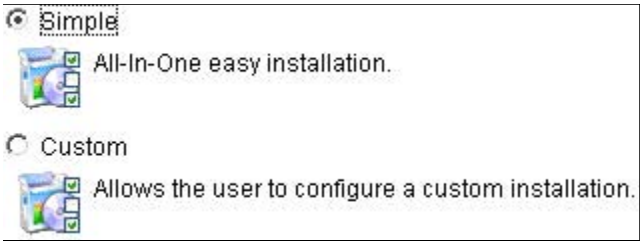
1. Vérifiez que vous avez collecté les informations, réalisé les tâches et rempli toutes les conditions définies à la section Préinstallation de Sentinel 5 pour MSSQL pour les composants à installer.
2. Insérez le CD d'installation Sentinel dans l'unité de CD-ROM.
3. Parcourez le CD et double-cliquez sur *setup.bat*.

REMARQUE : l'installation en mode de console n'est pas prise en charge sous Windows.

4. Cliquez sur la flèche bas et sélectionnez une des langues suivantes au choix.
   - anglais
   - français
   - allemand
   - italien
   - portugais
   - espagnol
5. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
6. Acceptez l'accord de licence utilisateur final, puis cliquez sur *Suivant.*
7. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* afin d'indiquer l'emplacement de l'installation. Cliquez sur *Suivant.*



8. Sélectionnez *Simple*. Cliquez sur *Suivant.*

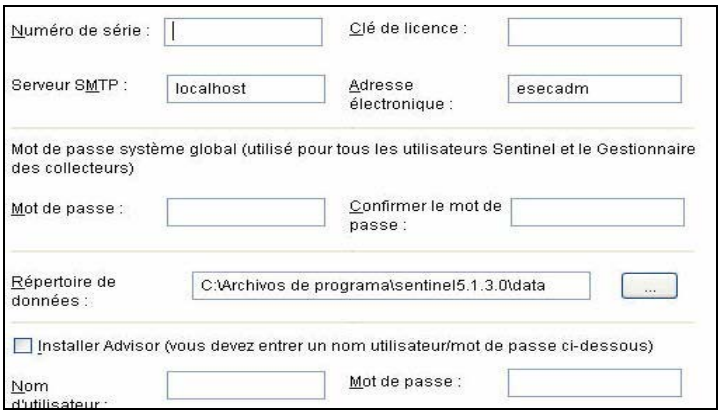


9. Entrez les informations de configuration.
   - numéro de série et clé de licence
   - serveur SMTP (nom DNS ou adresse IP), si vous voulez que Sentinel soit capable d'envoyer des messages électroniques.
   - courrier électronique – entrez une adresse électronique valide où les messages de notification de l'Advisor doivent être envoyés (par ex. Sent_Server@myserver.com).
   - mot de passe global du système – entrez le mot de passe et le mot de passe de confirmation correspondant. Celui-ci devient le mot de passe pour tous les utilisateurs par défaut, y compris l'utilisateur du système d'exploitation esecadm et les utilisateurs de la base de données. Consultez Base de données Sentinel, à la section Préinstallation de Sentinel 5 pour MSSQL, pour voir la liste des utilisateurs de la base de données créée par défaut lors de l'installation.
   - répertoire de données – l'emplacement de tous les fichiers de données de la base de données et de la base de données de l'Advisor. Pour changer l'emplacement par défaut, cliquez sur le bouton … et sélectionnez un emplacement. Par défaut correspond à %ESEC_HOME%\data.

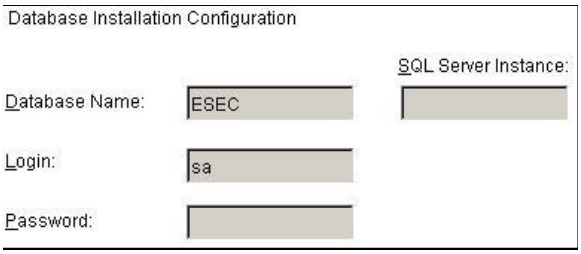
REMARQUE : si vous installez l'Advisor, l'installation simple configure l'Advisor pour utiliser le téléchargement direct d'Internet avec un intervalle de mise à jour de 12 heures et toutes les notifications par messages électroniques activées.

   - Pour installer l'Advisor, sélectionnez *Installer Advisor*. Entrez un nom d'utilisateur et un mot de passe. S'il n'est pas possible de vérifier votre nom d'utilisateur ou votre mot de passe, lorsque vous cliquez sur *Suivant*, une invite vous demande si vous voulez continuer (déconseillé). Si vous choisissez de continuer, entrez de nouveau le mot de passe de l'Advisor dans la fenêtre Confirmation de mot de passe. Sinon, corrigez le mot de passe de l'Advisor.

   Cliquez sur *Suivant.*



10. Pour la configuration de l'installation de la base de données, entrez :
    - nom d'utilisateur sa et mot de passe
    - si vous avez nommé l'instance de SQL Server, entrez le nom correspondant.



11. Lisez les informations sur les écrans qui apparaissent, avant de cliquer sur *Suivant*. Après avoir terminé l'installation, vous devez redémarrer le système.

REMARQUE : si vous voulez installer un logiciel d'intégration tiers (HP Service Desk ou Remedy Integration), après le redémarrage de la machine, exécutez de nouveau le programme d'installation et sélectionnez le logiciel d'intégration tiers que vous voulez installer. Pour plus d'informations, voir le guide du logiciel d'intégration tiers.

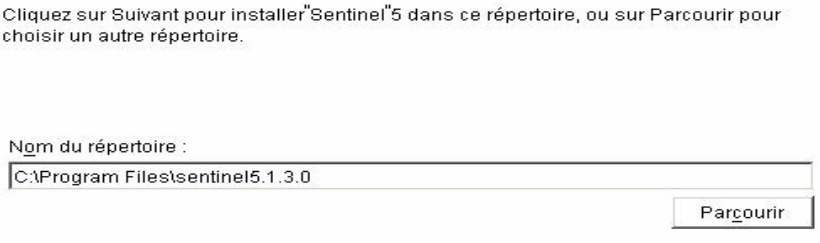
Installation personnalisée

Installation personnalisée de Sentinel

1. Vérifiez que vous avez collecté les informations, réalisé les tâches et rempli toutes les conditions définies à la section Préinstallation de Sentinel 5 pour MSSQL pour les composants à installer.
2. Insérez le CD d'installation Sentinel dans l'unité de CD-ROM.
3. Parcourez le CD et double-cliquez sur *setup.bat*.

REMARQUE : l'installation en mode de console n'est pas prise en charge sous Windows.

4. Cliquez sur la flèche bas et sélectionnez une des langues suivantes au choix.
   - anglais
   - français
   - allemand
   - italien
   - portugais
   - espagnol
5. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
6. Acceptez l'accord de licence utilisateur final, puis cliquez sur Suivant.
7. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* afin d'indiquer l'emplacement de l'installation. Cliquez sur *Suivant.*



8. Sélectionnez *Personnalisée* (par défaut). Cliquez sur *Suivant.*
9. Sélectionnez les fonctions à installer.

REMARQUE : pour plus d'informations concernant le composant qui peut être installé pour les différentes configurations, voir le *chapitre 1 Configuration système requise*.

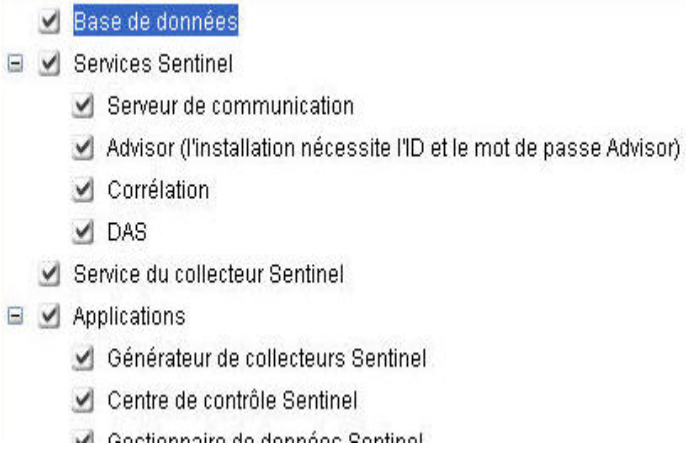
Les composants suivants peuvent être installés :

- base de données – il installe la base de données Sentinel
- serveur de communication – elle installe le bus de messages (iSCALE)
- Advisor
- moteur de corrélation
- DAS
- Service de collecteurs
- générateur de collecteurs
- Sentinel Control Center
- gestionnaire de données Sentinel
- HP OpenView Service Desk
- Remedy Integration

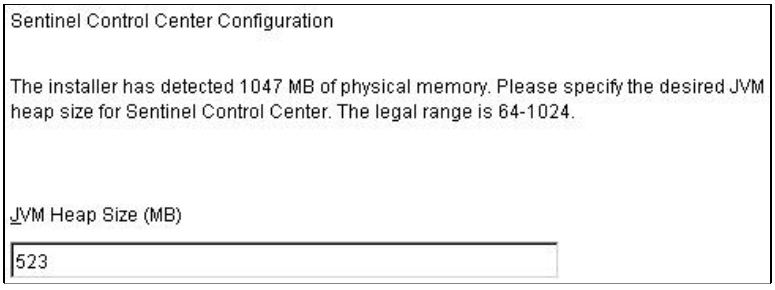
REMARQUE : pour plus d'informations sur l'installation de HP OpenView Service Desk ou Remedy Integration, voir le guide du logiciel d'intégration tiers.

REMARQUE : si aucune des fonctions enfants de *Sentinel Services* n'est sélectionnée, la fonction *Sentinel Services* doit elle aussi être désélectionnée. Elle apparaît en gris et cochée en blanc si elle est encore sélectionnée alors qu'aucune de ses fonctions enfants n'est sélectionnée.

REMARQUE : pendant l'installation du composant de la base de données Sentinel, le programme d'installation place les fichiers dans le dossier %ESEC_HOME%\utilities\db.



10. Si vous avez sélectionné l'installation du DAS, une invite vous demande :
    - le numéro de série
    - la clé de licence
11. Si vous avez sélectionné l'installation d'un logiciel d'intégration tiers (HP Service Desk ou Remedy Integration), vous devrez fournir un mot de passe pour déverrouiller le(s) composant(s) d'intégration tiers sélectionné(s). Pour plus d'informations, voir le *guide du logiciel d'intégration tiers*.
12. Si vous sélectionnez l'installation de Sentinel Control Center, une invite JVM (Java Virtual Machine) apparaît :
    - taille heap JVM (Mo) – par défaut, elle est définie comme la moitié de la taille de la mémoire physique détectée sur la machine, au maximum 1 024 Mo. Elle correspond au maximum de taille heap JVM seulement utilisée par Sentinel Control Center.



13. Si vous décidez d'installer le service de collecteurs, choisissez de protéger ou non le gestionnaire de collecteurs de l'assistant à l'aide d'un mot de passe. Si vous choisissez de protéger le gestionnaire de collecteurs de l'assistant, vous êtes invité à créer un mot de passe du gestionnaire de collecteurs de l'assistant.

REMARQUE : si vous protégez le collecteur avec un mot de passe, vous devez entrer ce mot de passe lors du téléchargement ou du débogage des collecteurs dans ce gestionnaire de collecteurs. Ce mot de passe est aussi nécessaire, en plus du nom d'utilisateur Sentinel et du mot de passe correspondant, pour se loguer au générateur de collecteurs de l'assistant.

REMARQUE : afin d'accomplir les configurations de sécurité rigoureuses exigées par la certification de critères communs, Sentinel requiert un mot de passe fort avec les caractéristiques suivantes :

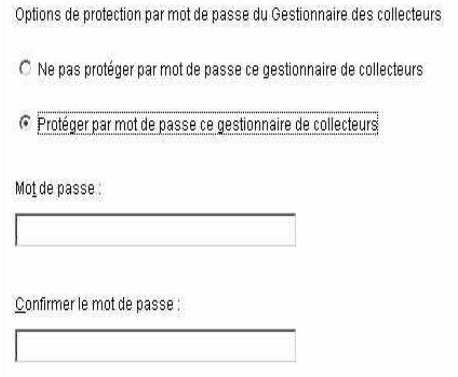
1. Choisissez des mots de passe comportant au moins 8 caractères qui incluent au moins un caractère en MAJUSCULE, un caractère en minuscule, un symbole spécial (!@#$%^&*()_+) et un caractère numérique (0 à 9).

2. Le mot de passe ne peut contenir ni votre adresse électronique, ni aucune partie de votre nom complet.

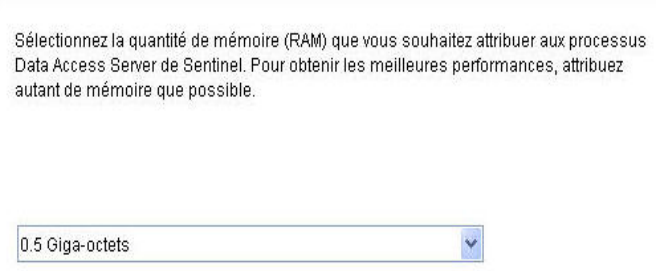
3. Le mot de passe ne doit pas être un nom commun (par exemple, ce ne doit pas être un mot du dictionnaire ou d'argot d'usage commun).

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

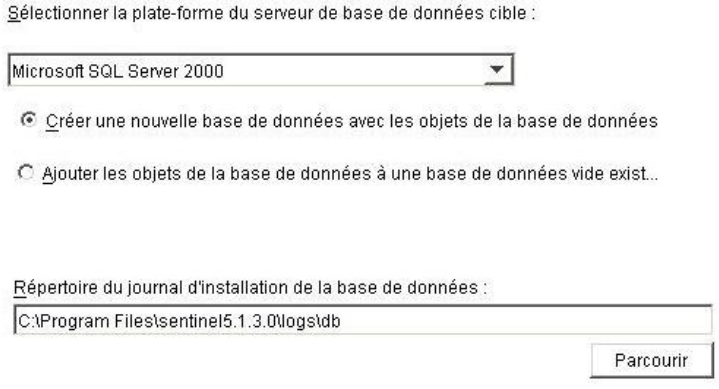
5. Vous devriez choisir un mot de passe facile à mémoriser mais complexe. Par exemple, Mea5!A (Mon enfant a 5 ans) OU JhaPdp5#a (J'habite à Paris depuis 5 ans).



14. Si vous choisissez d'installer le DAS, sélectionnez la quantité de RAM dans le système que vous voulez allouer au Data Access Service. Pour des environnements distribués, il est recommandé de sélectionner le maximum de mémoire (4 Go). Pour des environnements indépendants, il est recommandé de sélectionner la moitié de la mémoire RAM.



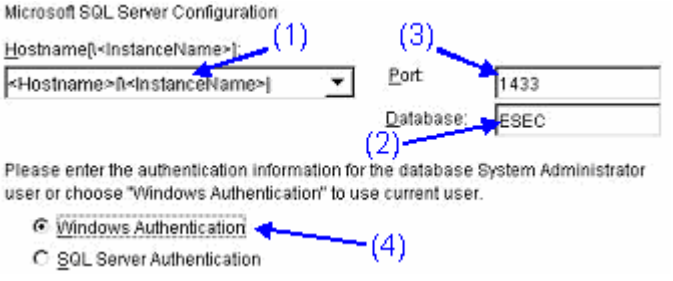
15. Pour l'installation de la base de données, vous avez les invites suivantes.
    a. Sélectionnez la plate-forme du serveur de la base de données cible comme Microsoft SQL Server 2000 ou 2005 et sélectionnez une des options suivantes :
        - créer une nouvelle base de données avec des objets de base de données – elle crée une nouvelle base de données MS SQL et remplit la nouvelle base de données avec des objets de base de données.
        - ajouter des objets de base de données à une base de données existante vide – il ajoute seulement la base de données à une base de données MS SQL existante. la base de données existante doit être vide.
    b. Entrez le répertoire journal d'installation de bases de données (par défaut : %ESEC_HOME%\logs\db). Acceptez le « Répertoire journal d'installation de la base de données » par défaut ou cliquez sur *Parcourir* afin d'indiquer un emplacement différent.



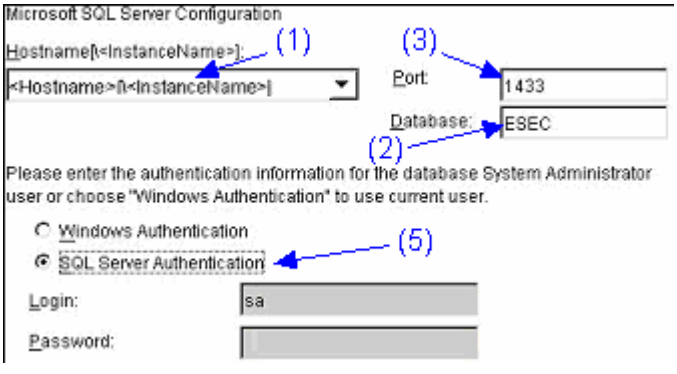
    c. Insérez les informations de configuration de SQL Server comme suit :
        - (1) nom d'hôte de la base de données ou adresse IP – Par défaut, la machine de l'hôte local apparaît, si SQL Server est installé localement. Si SQL Server que vous voulez installer n'apparaît pas dans la liste déroulante, sélectionnez à *Autre* dans la liste. une zone de texte est affichée pour que vous y tapiez le nom d'hôte. Le nom d'hôte inséré doit être complet (par ex. « sqlserver.sentinel.net » au lieu de seulement « sqlserver »). Si vous avez défini un nom d'instance pendant l'installation de SQL Server, vous devez ajouter « <nom_instance> » à la fin du nom d'hôte,

où <nom_instance> correspond au nom donné à l'instance lors de l'installation de SQL Server.

- (2) Database name (nouvelle base de données) – C'est le nom à donner à la nouvelle base de données de SQL Server. Outre la base de données nommée ici, une autre base de données nommée <nom_ma_bd>_WF est également créée afin d'être utilisée par l'iTRAC.
- (2) nom de la base de données (base de données existante) – c'est le nom de la base de données existante vide de SQL Server à laquelle vous voulez ajouter des objets de base de données. Utilisez le nom de la base de données qui ne contient pas le suffixe « _WF ».
- (3) port de la base de données (par défaut, 1433)
- Pour l'administrateur de la base de données du système, sélectionnez une des options suivantes:
- (4) Authentification Windows – celle-ci utilise le nom d'utilisateur employé pour exécuter le programme d'installation.
- (5) Authentification de SQL Server - entrez le mot de passe de l'utilisateur sa.



Authentification Windows

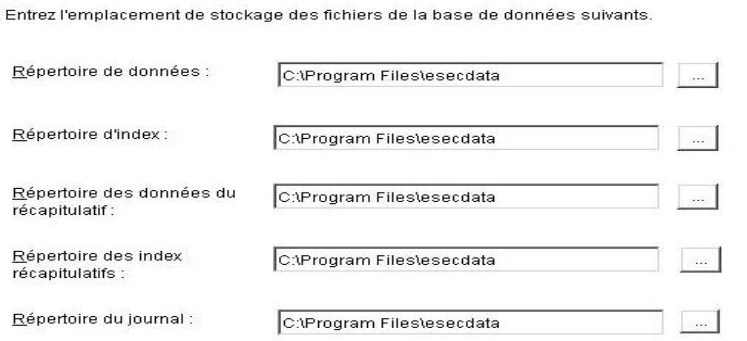


Authentification de SQL Server

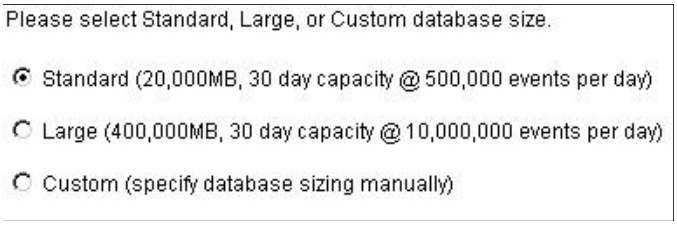
d. Si vous choisissez l'installation d'une nouvelle base de données, entrez l'emplacement des fichiers de base de données suivants :

REMARQUE : à des fins de récupération et de performance, nous recommandons que ces emplacements soient dans des périphériques E/S différents.

- fichiers de données
- fichiers d'index
- fichiers de données récapitulatifs
- fichiers d'index récapitulatifs
- fichiers journaux

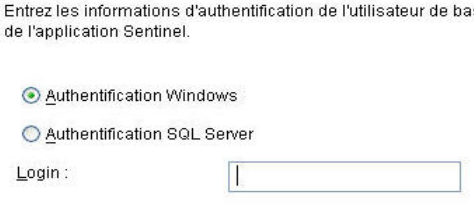


e. Si vous choisissez d'installer une nouvelle base de données, entrez la taille de la base de données :
   - standard (20 000Mo) – capacité de 30 jours avec 500 000 évènements par jour
   - grande (400 000Mo) – capacité de 30 jours avec 10 000 000 évènements par jour
   - personnalisée (indiquez la taille manuellement). Si vous sélectionnez cette option, une invite vous demande aussi :
     (1) la taille de la base de données en Mo (10 000 – 2 000 000)
     (2) la taille de chaque fichier journal en Mo (100 – 100 000)
     (3) la taille maximum de chaque fichier de la base de données en Mo (2 000 – 100 000)



f. Pour l'administrateur de la base de données Sentinel (DBA), sélectionnez une des options :
   - authentification Windows, entrez <nom_domaine>\<nom_utilisateur>
   - authentification SQL Server (esecdba), mot de passe et mot de passe de confirmation.

REMARQUE : si vous sélectionnez *Authentification SQL Server*, vous ne pouvez pas modifier le nom de login par défaut.



Authentification Windows

Authentification de SQL Server

g. Pour l'utilisateur de la base de données de application Sentinel, sélectionnez une des options suivantes :

REMARQUE : si vous utilisez un login de domaine Windows pour l'utilisateur de la base de données de l'application Sentinel, vous devez accorder à cet utilisateur le privilège de S*e loguer comme service* sur cette machine, comme mentionné à la section Serveur Sentinel, dans la section Préinstallation de Sentinel 5 pour MSSQL.

- authentification Windows, entrez <nom_domaine>\<nom_utilisateur>, mot de passe et mot de passe de confirmation
- authentification de SQL Server (esecapp), entrez le mot de passe et le mot de passe de confirmation.

REMARQUE : si vous sélectionnez *Authentification SQL Server*, vous ne pouvez pas modifier le nom de login par défaut.

Authentification Windows

Authentification de SQL Server

h. Pour l'utilisateur de l'administrateur Sentinel, sélectionnez une des options suivantes :
   - authentification Windows, entrez <nom_domaine>\<nom_utilisateur>
   - authentification SQL, entrez le nom d'utilisateur pour l'administrateur Sentinel (par défaut : esecadm), le mot de passe et le mot de passe de confirmation.

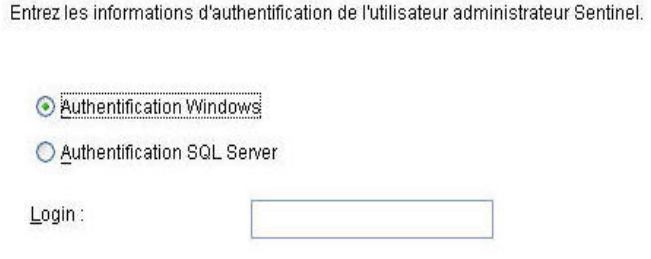
REMARQUE : si vous sélectionnez *Authentification SQL Server*, vous ne pouvez pas modifier le nom de login par défaut.

Authentification Windows

Authentification de SQL Server

i. Pour l'utilisateur de la création de rapport Sentinel, sélectionnez une des options suivantes :
   - authentification Windows, entrez <nom_domaine>\<nom_utilisateur>
   - authentification SQL (esecrpt), entrez le mot de passe et le mot de passe de confirmation.

REMARQUE : si vous sélectionnez *Authentification SQL Server*, vous ne pouvez pas modifier le nom de login par défaut.



Authentification Windows

Authentification de SQL Server

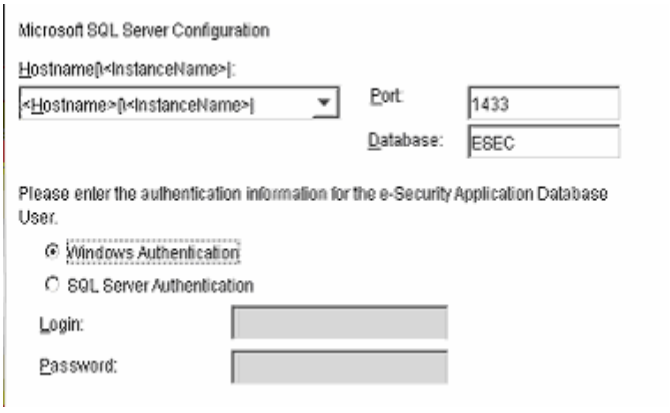
j. Cliquez sur *Suivant* dans la fenêtre récapitulative de l'installation de la base de données.

16. Si vous choisissez d'installer le DAS mais pas la base de données Sentinel, une invite vous demande les informations suivantes sur la base de données de SQL Server. Ces informations sont utilisées pour configurer le DAS afin qu'il soit ciblé sur la base de données Sentinel.

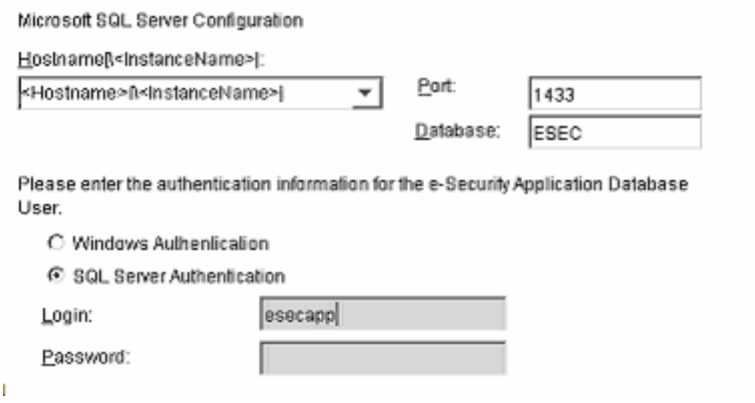
- nom d'hôte de la base de données ou adresse IP – par défaut, la machine de l'hôte local apparaît, si la base de données Sentinel de SQL Server est installée localement. si la base de données Sentinel de SQL Server à laquelle vous voulez connecter le DAS n'apparaît pas dans la liste déroulante, sélectionnez *Autre* dans la liste. une zone de texte est affichée pour que vous y tapiez le nom d'hôte. Le nom d'hôte inséré doit être complet (par ex. « sqlserver.sentinel.net » au lieu de seulement « sqlserver »). Si vous avez défini un nom d'instance pendant l'installation de SQL Server, vous devez ajouter « <nom_instance> » à la fin du nom d'hôte, où <nom_instance> correspond au nom donné à l'instance lors de l'installation de SQL Server.
- nom de la base de données – C'est le nom de la base de données existante de SQL Server à laquelle vous voulez connecter le DAS. Utilisez le nom de la base de données qui ne contient pas le suffixe « _WF ».
- port de la base de données (par défaut, 1433).
- Pour l'utilisateur de la base de données de l'application Sentinel, sélectionnez une des options suivantes :

REMARQUE : si vous utilisez un login de domaine Windows pour l'utilisateur de la base de données de l'application Sentinel, vous devez accorder à cet utilisateur le privilège de« se loguer comme service » sur cette machine, comme mentionné à la section Serveur Sentinel, dans la section Préinstallation de Sentinel 5 pour MSSQL.

  - authentification Windows – indiquez le login du domaine Windows donné à cet utilisateur lors de l'installation de la base de données Sentinel et entrez le mot de passe pour cet utilisateur. Ce mot de passe est nécessaire ici pour configurer Sentinel Windows Service pour « se loguer comme un service » comme login du domaine Windows.
  - authentification de SQL Server – indiquez le login « esecapp » et entrez le mot de passe donné à cet utilisateur lors de l'installation de la base de données Sentinel.

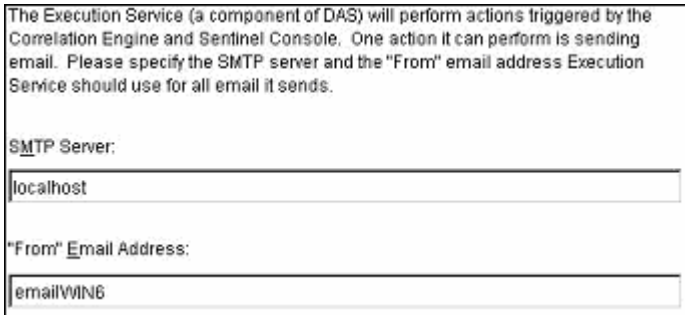


Authentification Windows



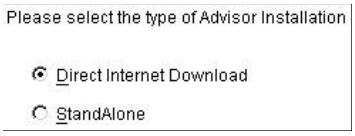
Authentification SQL

17. Si vous choisissez d'installer le DAS, configurez le support du courrier électronique Sentinel. Indiquez le serveur SMTP et l'adresse expéditeur que le Service exécution doit utiliser pour envoyer des messages (facultatif : cela peut être édité manuellement [%ESEC_HOME%\sentinel\config\execution.properties]) :

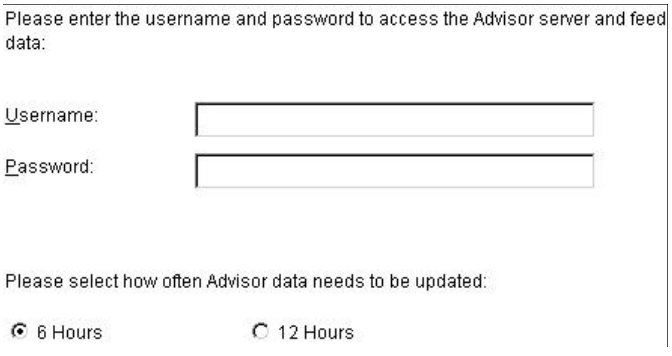


18. Si vous choisissez d'installer l'Advisor, l'invite suivante concernant le type d'installation apparaît :
    - Téléchargement direct d'Internet – la machine Advisor est directement connectée à Internet. Dans cette configuration, les mises à jour de Novell sont automatiquement téléchargées de Novell sur Internet, à un rythme régulier.

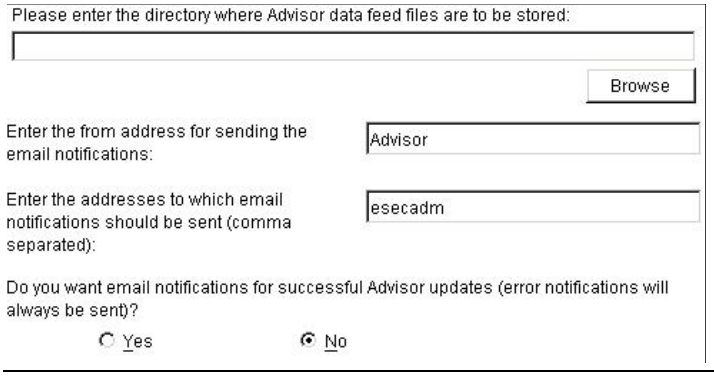
- Indépendant – l'Advisor est configuré comme un système isolé qui requiert une intervention manuelle pour recevoir des mises à jour du Sentinel.



19. Si vous choisissez d'installer l'Advisor et sélectionnez l'option de téléchargement direct d'Internet, entrez le nom d'utilisateur de l'Advisor, le mot de passe, ainsi que le rythme souhaité des mises à jour de l'Advisor. S'il n'est pas possible de vérifier votre nom d'utilisateur ou votre mot de passe, lorsque vous cliquez sur *Suivant*, une invite vous demande si vous voulez continuer (déconseillé). Si vous choisissez de continuer, entrez de nouveau le mot de passe de l'Advisor dans la fenêtre Confirmation de mot de passe. Sinon, corrigez le mot de passe de l'Advisor.



20. Si vous choisissez d'installer l'Advisor, entrez :
    - Le répertoire où les fichiers d'alimentation de données de l'Advisor sont archivés. C'est l'emplacement où les fichiers d'alimentation d'attaque et d'alerte sont enregistrés lors du téléchargement.
    - adresse destinataire, pour l'envoi de notifications par message électronique :
    - Sélectionnez Oui si vous voulez recevoir des messages électroniques concernant les mises à jour réussies de l'Advisor, ou Non dans le cas contraire. Les notifications d'erreurs sont toujours envoyées.



REMARQUE : après l'installation, vous pouvez changer les adresses électroniques de l'Advisor, en éditant les fichiers attackcontainer.xml et alertcontainer.xml. Pour plus d'informations, voir le *chapitre 9 « L'onglet Advisor » du guide de l'utilisateur Sentinel.*

21. Si vous choisissez d'installer HP OpenView Service Desk ou Remedy Integration, une invite vous demande des informations supplémentaires. Pour plus d'informations, voir le *guide du logiciel d'intégration tiers Sentinel*.
22. Lisez les informations sur les écrans qui apparaissent, avant de cliquer sur *Suivant*. Une fois l'installation terminée, une invite vous demande de redémarrer.
23. Cliquez sur *Terminer* pour redémarrer le système.
24. Si vous attendez un taux d'évènements élevé (supérieur à 800 évènements par seconde), vous devez suivre les instructions de configuration avancée à la section Configurer la stratégie d'insertion d'évènements d'objets de données actives (ADO – Active Data Objects).

Post-Installation de Sentinel 5 pour MS SQL

Mise à jour du courrier électronique Sentinel pour authentification SMTP

Si le système requiert une authentification SMTP, vous devez mettre à jour le fichier execution.properties. Ce fichier est sur la machine où le DAS est installé. Il est localisé à %$ESEC_HOME%/sentinel/config. Pour configurer ce fichier, exécutez mailconfig.bat afin de changer le fichier et mailconfigtest.bat afin de tester ces changements.

Pour configurer le fichier execution.properties.

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfig de la façon suivante :

   ```
   mailconfig.bat -host <serveur SMTP> -de <adresse
      électronique source> -utilisateur <utilisateur
      authentification courrier électronique> –mot de passe
   ```

   Exemple :

   ```
   mailconfig.bat -host 10.0.1.14 -from nom@domaine.com -
      user nom_utilisateur –password
   ```

   Après cette commande, une invite vous demande d'insérer un nouveau mot de passe.

   ```
   Entrez le mot de passe :*********
   Confirmez le mot de passe :*********
   ```

REMARQUE : lors de l'utilisation de l'option de mot de passe, ce doit être le dernier argument.

Pour tester la configuration d'execution.properties

1. Sur la machine où le DAS est installé, cd pour :

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

2. Exécutez mailconfigtest de la façon suivante :

   ```
   mailconfigtest.bat -to <adresse électronique cible>
   ```

Si l'envoi du message électronique a abouti, vous obtenez le résultat suivant sur l'écran et le message est reçu à l'adresse cible.

```
Message électronique envoyé avec succès !
```

Vérifiez la boîte aux lettres de l'adresse cible pour confirmer la réception du message. La ligne d'objet et le contenu devraient être les suivants :

```
Objet : Test des propriétés du courrier électronique
   Sentinel

Test de configuration des propriétés du courrier
   électronique Sentinel. Si ce message apparaît, les
   propriétés du courrier électronique Sentinel ont été
   correctement configurées pour envoyer des messages.
```

Base de données Sentinel

Après l'installation de la base de données Sentinel, la base de données contient les utilisateurs suivants par défaut :

- esecdba - utilisateur du schéma (si vous utilisez l'utilisateur du domaine Windows, il est configurable lors de l'installation)
- esecapp – le non d'utilisateur employé par les applications Sentinel pour se connecter à la base de données (si vous utilisez l'utilisateur du domaine Windows, il est configurable lors de l'installation)
- esecadm – administrateur Sentinel (si vous utilisez l'utilisateur du domaine Windows, il est configurable lors de l'installation)
- esecrpt - utilisateur de la création de rapport (si vous utilisez l'utilisateur du domaine Windows, il est configurable lors de l'installation)

Service de collecteurs

Lors de l'installation du service de collecteurs, les collecteurs suivants sont installés et chacun possède un port de collecteur pour son exécution.

Produit	**Nom de collecteur**
Collecteurs démo	
Test de téléchargement d'actifs, travaille avec le collecteur DemoEvents	DemoAssetUpload
Test d'évènements démo, travaille avec les collecteurs DemoAssetUpload et DemoVulnerabilityUpload	DemoEvents
Test de téléchargement de vulnérabilité, travaille avec le collecteur DemoEvents	DemoVulnerabilityUpload
Test d'envoi d'un évènement	SendOneEvent
Test d'envoi de plusieurs évènements	SendMultipleEvents

REMARQUE : pour plus d'informations sur la configuration des collecteurs démo, voir le *chapitre 12 Tester l'installation.*

REMARQUE : pour plus de collecteurs, veuillez consulter le Sentinel Customer Portal. Pour plus d'informations (y compris la configuration), voir la documentation fournie avec chaque collecteur à :

%WORKBENCH_HOME%\Elements\<nom_collecteur>\Docs\

Pour installer d'autres collecteurs, exécutez le script Service Pack sur le CD Service Pack.

Ce script installe les collecteurs localement.

Sous Windows :

```
.\service_pack.bat
```

Sur UNIX :

```
./service_pack.sh
```

Pour lire les instructions d'installation du Service Pack et la liste des collecteurs, voir les *notes de publication du Service Pack.*

Mise à jour de la clé de licence

Si la clé de licence a expiré et Novell vous en a délivré une autre, exécutez le programme clé du logiciel pour mettre à jour la clé de licence.

Comment mettre à jour la clé de licence

1. Loguez-vous comme utilisateur doté de droits administratifs.
2. Allez vers %ESEC_HOME%\utilities.
3. Entrez la commande suivante :

   ```
   softwarekey.exe
   ```

4. Entrez le numéro 1 pour entrer la clé principale. Appuyez sur Enter.

Instructions de configuration pour utiliser l'authentification Windows SQL Server avec le pilote DataDirect JDBC

REMARQUE : Vous trouverez ci-dessous un extrait du guide d'installation DataDirect Connect© pour JDBC©. Il est vivement conseillé de laisser l'administrateur du système effectuer les étapes suivantes.

Après l'installation de Connect pour JDBC, il faut configurer les composants suivants pour utiliser l'authentification Windows sur SQL Server :

- serveur de la base de données de SQL Server
- Contrôleur de domaine
- poste de travail client

Pour plus d'informations concernant l'authentification Windows et le pilote Connect pour JDBC sur SQL Server, veuillez consulter *DataDirect Connect for JDBC User's Guide and Reference*.

Serveur de la base de données de SQL Server

Cette section décrit la configuration requise par le serveur de la base de données de SQL Server pour utiliser l'authentification Windows avec le pilote Connect pour JDBC sur SQL Server.

Nom principal du service

Pour utiliser le protocole d'authentification Kerberos, il faut enregistrer un nom principal de service (SPN, Service Principal Name) pour chaque instance de SQL Server. Un SPN est un nom unique qui assigne le service de SQL Server à une machine spécifique et un port à un nom de compte utilisé pour démarrer un service (compte de démarrage du service). Un SPN est composé des éléments suivants :

- le nom de classe de service est toujours MSSQLSvc pour SQL Server
- le nom d'hôte est le nom DNS complet de la machine qui exécute SQL Server
- le port est le numéro de port sur lequel l'instance de SQL Server écoute

Par exemple : MSSQLSvc/DBServer.test:1433 est le SPN de l'instance de SQL Server exécutée sur la machine nommée DBServer dans le domaine de test et qui écoute sur le port 1433.

Listage des SPN

Vérifiez sur l'administrateur de la base de données ou du domaine que les SPN adéquats ont bien été enregistrés pour chaque instance de SQL Server. L'administrateur de la base de données ou du domaine peut utiliser la commande Windows ldifde pour faire la liste des SPN enregistrés.

Enregistrement des SPN

Si nécessaire, l'administrateur de la base de données ou du domaine peut enregistrer les SPN en utilisant l'outil Setspn disponible avec le kit de ressources Windows. Par exemple :

```
setspn -A MSSQLSvc/DBServer.test:1433 sqlsvc
```

il enregistre un SPN qui assigne le compte de démarrage du service nommé sqlsvc à une instance de SQL Server, celle-ci étant exécutée sur une machine nommée DBServer dans le domaine de test et écoutant sur le port 1433.

L'outil Setspn est disponible sur le site Web suivant : http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/setspn-o.asp.

Consultez la documentation Microsoft qui accompagne l'outil Setspn pour lire les instructions de son utilisation.

REMARQUE : si le compte de démarrage de SQL Server est changé, il faut supprimer les SPN et les enregistrer de nouveau.

Mode d'authentification

Pour utiliser l'authentification Windows, le mode d'authentification de SQL Server peut être défini d'une des deux façons suivantes :

- authentification Windows seulement
- authentification mixte

Si l'authentification de SQL Server doit être utilisée avec l'authentification Windows, le mode d'authentification doit être défini pour utiliser l'authentification mixte.

Contrôleur de domaine

Le pilote SQL Server prend en charge l'authentification Windows, lorsque Kerberos Key Distribution Center (KDC) est exécuté sur un contrôleur de domaine Windows 2000. Lors de la communication avec KDC, les messages transmis entre KDC et SQL Server sont codés.

Puisque SQL Server ne peut utiliser que l'algorithme de codage DES-CBC-MD5, le compte de démarrage du service de SQL Server sur le contrôleur de domaine doit inclure la propriété Active Directory « Utiliser les types de codage DES pour ce compte ». Vérifiez avec l'administrateur du domaine que cette propriété est définie pour le compte de démarrage du service de SQL Server. Le compte de service du démarrage de SQL Server ne peut pas être utilisé comme compte de login client.

Machine client

Cette section décrit la configuration requise par la machine cliente pour utiliser l'authentification Windows avec le pilote Connect pour JDBC de SQL Server.

Fichier de configuration Kerberos

Le module de login Kerberos requiert un nom de domaine Kerberos (nom de domaine Windows) et un nom KDC (nom de contrôleur de domaine Windows) pour ce domaine Kerberos. Lors de l'installation du Connect pour JDBC, un fichier de configuration est installé et il établit un domaine Kerberos général et un nom KDC. Ce fichier est nommé krb5.conf et installé dans le répertoire /lib du répertoire d'installation de Connect pour JDBC.

Il faut modifier le fichier krb5.conf pour spécifier le nom de domaine Kerberos et le nom KDC pour l'environnement. Si ce fichier n'est pas modifié pour inclure un domaine Kerberos et un nom KDC valides, l'erreur suivante est générée :

```
Message :[DataDirect][SQLServer JDBC Driver]Impossible
      d'établir une connexion avec sécurité intégrée :
      Aucune référence valide fournie
```

Le pilote Connect pour JDBC de SQL Server configure automatiquement le module de login Kerberos pour télécharger le fichier de configuration Kerberos krb5.conf, sauf si la propriété du système java.security.krb5.conf est déjà définie pour cibler un autre fichier de configuration. Vous pouvez remplacer le nom de domaine Kerberos et le nom KDC indiqués dans le fichier krb5.conf en définissant les propriétés de système suivantes : java.security.krb5.realm et java.security.krb5.kdc.

Configurer la stratégie d'insertion d'évènements d'objets de données actives (ADO – Active Data Objects)

Sentinel 5.1 fournit une structure pour l'intégration de différentes stratégies afin d'insérer des évènements dans une base de données. Le Sentinel 5.1 fournit deux stratégies pour insérer des évènements sur une base de données MS SQL.

- JDBCLoadStrategy
- ADOLoadStrategy

La stratégie à utiliser pour l'insertion d'évènements est régie par la propriété insert.strategy du composant EventStoreService dans das_binary.xml.

La stratégie JDBC est la stratégie par défaut configurée au départ.

La stratégie ADO est la stratégie d'insertion native pour insérer les évènements plus rapidement. Cette stratégie requiert l'installation des packages Windows supplémentaires sur la machine où le composant DAS est exécuté. Veuillez consulter la section ci-dessous, pour les informations concernant les packages à installer. La stratégie ADO doit être utilisée dans les configurations qui requièrent un taux d'évènements plus élevé.

Le nombre d'évènements à regrouper pour être insérés dans la base de données est régi par la propriété insert.batchsize. Cette propriété insert.batchsize est utilisée par toutes les stratégies d'insertion d'évènements.

Les sections ci-dessous décrivent comment passer à des stratégies de chargement d'ADO.

Conditions préalables pour ADOLoadStrategy

Le connecteur natif ADO requiert l'installation du net.framework et du J# Redistributable Package sur la machine où le DAS Binary est exécuté.

REMARQUE : Il faut désinstaller les versions anciennes du net.framework et du J# Redistributable Package et installer les versions listées dans l'ordre suivant :

- net framework 2.0 Beta 2 disponible sur : http://www.microsoft.com/downloads/details.aspx?FamilyID=7ABD8C8F-287E-4C7E-9A4A-A4ECFF40FC8E&displaylang=en
- visual J# version 2.0 Beta 2 disponible sur : http://www.microsoft.com/downloads/details.aspx?FamilyId=A2788A92-76AB-4BF4-893A-FA9FD5031F14&displaylang=en

Configuration de la stratégie d'insertion d'évènements de chargement d'ADO

Pour changer la stratégie d'insertion d'évènements de Sentinel en passant de la stratégie d'insertion JDBC par défaut à la stratégie d'insertion ADO, il faut exécuter certaines étapes.

Passer de la stratégie d'insertion JDBC à la stratégie d'insertion ADO

1. à l'aide d'un éditeur de texte, ouvrez %ESEC_HOME%\sentinel\config\das_binary.xml.
2. Effectuez une recherche du texte suivant :

   ```
   JDBCLoadStrategy
   ```

3. Transformez le texte en :

   ```
   ADOLoadStrategy
   ```

4. Enregistrez ce changement dans le fichier das_binary.xml.
5. Redémarrez l'application DAS Binary.

Lors du redémarrage de l'application DAS Binary, les fichiers %ESEC_HOME%\Sun-1.4.2\bin\ EventInsert.dll et EventJNICLIBridge.dll sont chargés et utilisés pour effectuer les insertions d'évènements dans la base de données via ADO.

Conseils de débogage ADO

L’interface ADO n'enregistre les messages d’erreurs que sur le fichier %ESEC_HOME%\sentinel\log\ADOEventStoreError.log. Les messages d’erreurs initiaux enregistrés sur le fichier journal peuvent contenir des messages d’échec de connexions de la base de données. Ce fichier enregistre aussi les exceptions survenues lors de l’insertion des évènements dans la base de données. À noter : seules les erreurs sont enregistrées sur ce fichier.

Pour vérifier que la connexion et le chargement de l'ADO ont été accomplis, consultez le fichier journal das_binary localisé dans le répertoire %ESEC_HOME%\sentinel\log.

L’interface ADO enregistre aussi les erreurs sur le fichier journal das_binary localisé dans le répertoire %ESEC_HOME%\sentinel\log. Les erreurs enregistrées dans le fichier journal das_binary comprennent les échecs de localisation/chargement de EventJNICLIBridge.dll, les échecs de connexion avec la base de données et les échecs d'insertion d'évènements et d'associations d'évènements.

Si les messages d’erreur indiquent que les connecteurs natifs n'ont pas été bien chargés, procédez aux vérifications suivantes :

- Assurez-vous que les versions correctes du net framework et du J# Redistributable Package sont installées la machine.
- Assurez-vous que les fichiers « EventJNICLIBridge.dll » et « EventInsert.dll » sont localisés dans le répertoire %ESEC_HOME%\Sun-1.4.2\bin\.

6 Migration et correctif de données pour Oracle sous Solaris

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Ce chapitre traite de :

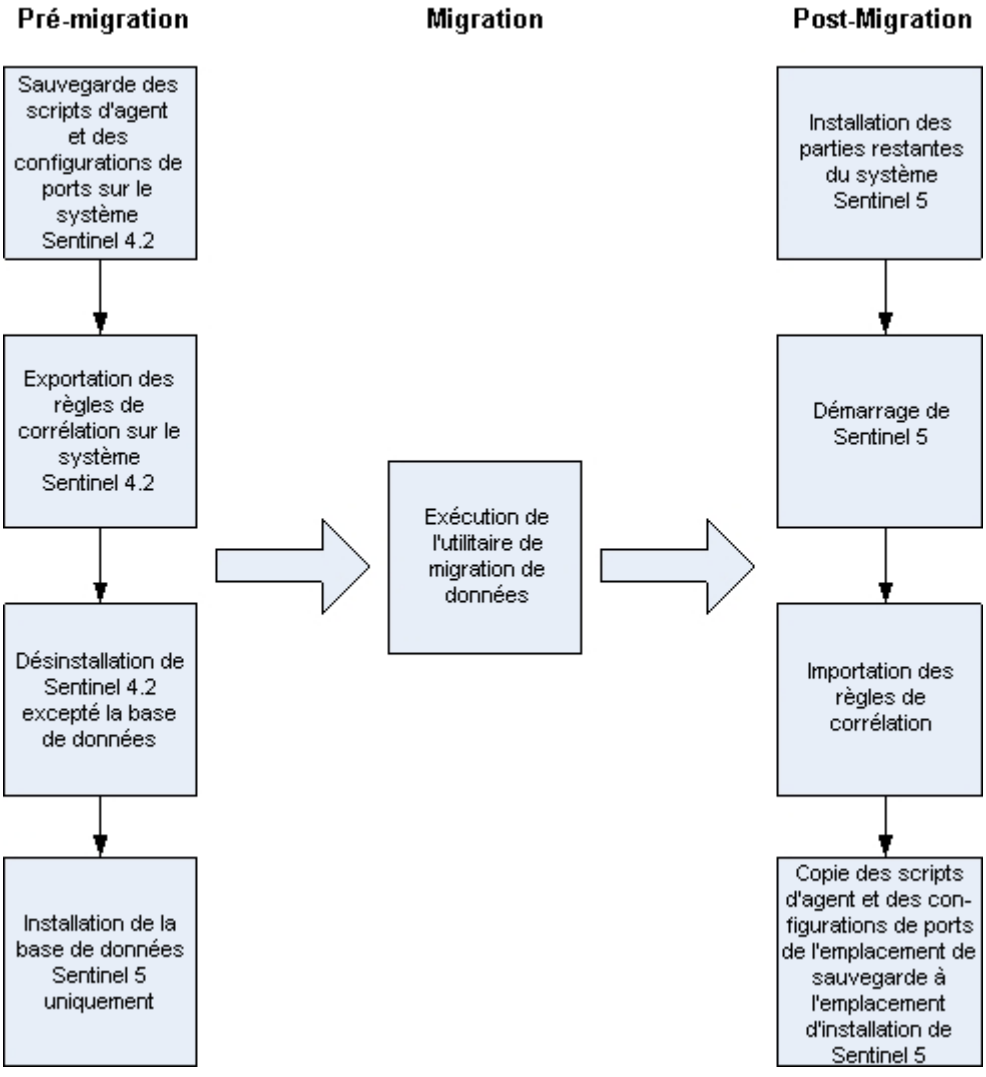
- migration et mise à jour des données de v4.2.0 vers v5.1.3
- Correctif de v5.x.x vers v5.1.3

Migration et mise à jour des données de v4.2 vers v5.1.3

Le processus de mise à jour de Sentinel 5 avec migration de données à partir de la version v4.2.0 consiste dans les étapes suivantes :

- Pré-migration
  - Sauvegarder l'instance de la base de données Sentinel : cette copie vous permet de restaurer la base de données v4.2, en cas d'échecs imprévus.
  - Sauvegarder toutes les commandes contextuelles du système ou tous les scripts sous le répertoire $ESEC_HOME
  - Exporter les règles de corrélation de Sentinel v4.2 (le cas échéant). Pour lire les instructions, consultez Pré-migration – Exportation des règles de corrélation.
  - Sauvegarder les scripts de collecteurs et les configurations de ports. Pour lire les instructions, consultez Pré-migration – Sauvegarde des scripts de collecteurs et des configurations de ports.
  - Sauf pour le composant de la base de données, désinstallez Sentinel v4.2. Pour lire les instructions, consultez Pré-migration – Désinstallation de v4.2.
  - Installer seulement la base de données Sentinel 5. Pour lire les instructions, consultez Pré-migration – installation de Sentinel 5.
- Migration
  - Exécuter l'utilitaire de migration de données. Pour lire les instructions, consultez Migration.
- Post-migration
  - Installer les composant restants de Sentinel 5. Pour lire les instructions, consultez Post-migration – installation de Sentinel 5.
  - Installer le Sentinel Service Pack le plus récent.
  - Démarrer Sentinel 5.
  - Importer les règles de corrélation (le cas échéant). Pour lire les instructions, consultez Post-migration – installation de Sentinel 5.
  - Copier les scripts de collecteurs et les configurations de ports à partir de l'emplacement de sauvegarde dans l'emplacement de l'installation Sentinel 5. Pour lire les instructions, consultez Post-migration – Reconfiguration des scripts de collecteurs et des configurations de ports.

- Reconfigurer les paramètres Oracle 9i Client liés à la création de rapport Crystal, pour cibler la base de données Sentinel 5 et importer les modèles Crystal Reports pour Sentinel 5. Pour lire les instructions, consultez Post-migration – Configuration de Sentinel 5 pour la création de rapport Crystal.



Serveur Sentinel

Sentinel 5 requiert la désinstallation de la version antérieure du logiciel, avant l'ajout des composants Sentinel 5. Ne désinstallez pas la version antérieure (v4.2) de la base de données, puisqu'elle est nécessaire à la migration de données de v4.2 vers Sentinel 5. Sauvegardez la machine du serveur Sentinel (répertoire d'installation $ESEC_HOME et unité root) avant la désinstallation. Cette copie vous permet de restaurer la v4.2, en cas d'échecs imprévus.

Vous trouverez ci-dessous des instructions détaillées sur la migration de données et sur la pré et post-installation.

Gestionnaire de collecteurs

Sentinel 5 requiert la désinstallation de tous les gestionnaires de collecteurs de la version v4.2 avant l'installation du logiciel du gestionnaire de collecteurs Sentinel 5. Sauvegardez la machine du gestionnaire de collecteurs v4.2 (répertoire d'installation $ESEC_HOME et unité root) avant la désinstallation.

Pour chaque machine exécutant le gestionnaire de collecteurs v4.2 avec au moins un port configuré, sauvegardez une copie des contenus des répertoires suivants dans un emplacement facile d'accès. Les contenus de ces répertoires seront utilisés pendant la post-migration afin de reconfigurer plus rapidement la définition des ports de collecteurs sur l'installation v4.2.

- $WORKBENCH_HOME/Agents – il contient les fichiers de configuration de ports.
- $WORKBENCH_HOME/Elements – il contient les scripts de collecteurs.
- Si vous ne faites pas de copie des contenus des répertoires ci-dessus, il vous faudra reconfigurer tous les scripts et ports de collecteurs depuis le début.

REMARQUE : le gestionnaire de collecteurs et le générateur de collecteurs de la version 4.2 ne sont pas compatibles avec les composants de la version 5.

Vous trouverez ci-dessous des instructions détaillées sur la migration de données et sur la pré et post-installation.

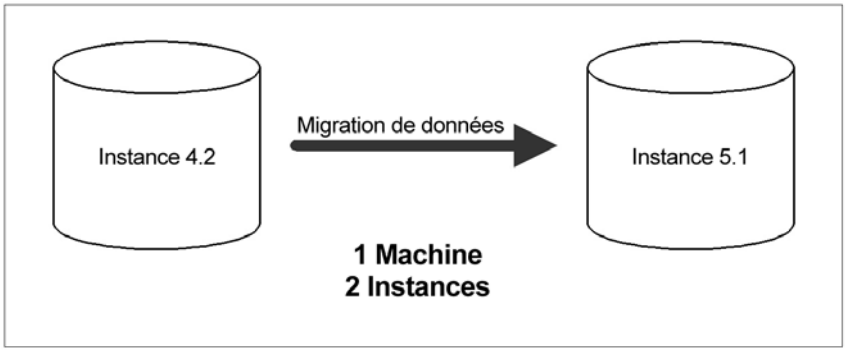
Serveur de création de rapport Crystal

Vous devez utiliser les rapports les plus récents du Service Pack le plus récent, après la mise à jour de Sentinel 5. Les nouveaux rapports sont configurés pour travailler avec le nouveau schéma de BD. Pour obtenir le Service Pack le plus récent, contactez le support technique Novell.

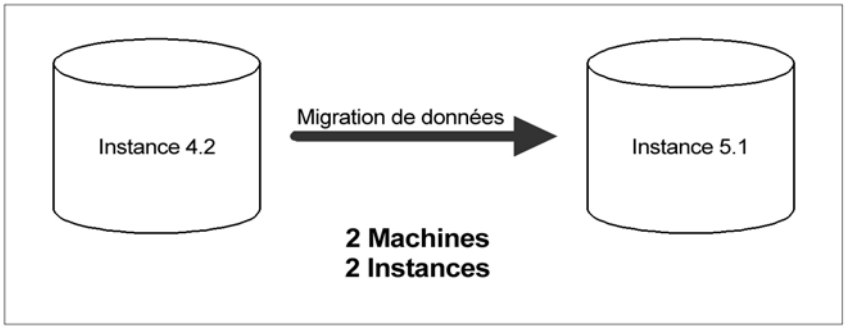
Serveurs de la base de données

Un utilitaire de migration de données Sentinel 5 est fourni pour copier les données d'une base de données Sentinel 4.2.0 sous Solaris 8/9 vers Sentinel 5.1.3. sous Solaris 9. L'utilitaire de migration de données prend en charge :

- 1 machine avec 2 instances de base de données



- 2 machines avec 1 instance de base de données sur chaque machine



Les données suivantes sont migrées par l'utilitaire :

- les utilisateurs et les autorisations assignées
- les filtres
- les options de configuration de menu contextuel.
- les balises CV renommées
- les configurations de partition et d'archives
- les cas de la version 4.2 sont copiés sur la version 5 comme incidents.
- les incidents et les évènements liés aux incidents

REMARQUE : l'utilitaire de migration de données NE fait PAS migrer les données d'évènement, à l'exception des données d'évènements liés aux incidents. Seules les données d'évènements liés aux incidents sont migrées.

REMARQUE : les données d'évènements d'incidents ne peuvent pas s'afficher dans Sentinel Control Center. Les données d'évènements d'incidents peuvent être vues à l'aide des rapports Crystal ou des requêtes SQL.

Vous trouverez ci-dessous des instructions détaillées sur la migration de données et sur la pré et post-installation.

Pré-migration – Exportation des règles de corrélation

Exportation d'un ensemble de règles de corrélation

1. Sur la console Sentinel v4.2, sous l'onglet Admin ouvrez la fenêtre Règles de corrélation.
2. Sélectionnez un ensemble de règles.
3. Cliquez sur *Exporter*. Un navigateur de fichiers est ouvert, recherchez le périphérique cible où écrire la règle et cliquez sur *OK*. L'ensemble de règles est exporté comme fichier xml.

Pré-migration – Sauvegarde des scripts de collecteurs et des configurations de ports

Sauvegarde des scripts de collecteurs et des configurations de ports

1. Sur toutes les machines Sentinel v4.2 qui exécutent le gestionnaire de collecteurs, créez un répertoire pour stocker les scripts de collecteurs et les configurations de ports de tous les collecteurs pour chaque machine.

2. Dans le répertoire créé, créez un fichier de texte listant les noms de tous les collecteurs utilisés par une configuration de port sur ce gestionnaire de collecteurs. Utilisez un générateur de collecteurs pour déterminer les collecteurs utilisés par ce gestionnaire de collecteurs. Si ce gestionnaire de collecteurs est sous Solaris, il vous faut utiliser un générateur de collecteurs sur une machine Windows (le générateur de collecteurs n'est pas pris en charge sous Solaris).
3. Copiez les répertoires suivants dans le répertoire que vous venez de créer.
   - $WORKBENCH_HOME/Agents
   - $WORKBENCH_HOME/Elements

Pré-migration – désinstallation de v4.2

Désinstallation de v4.2

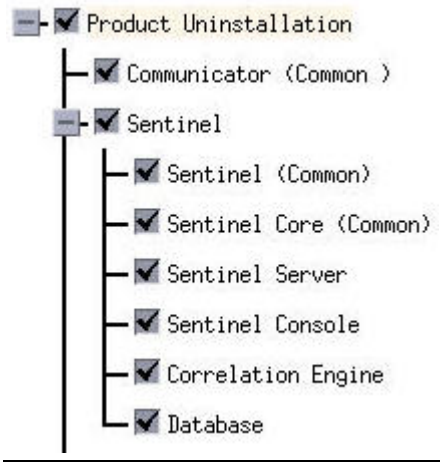
1. Sur la machine Sentinel v4.2 et sur toutes les machines clients, fermez toutes les consoles Sentinel et tous les générateurs de collecteurs Sentinel.
2. Loguez-vous comme utilisateur root.
3. Arrêtez le serveur Sentinel.
4. cd vers :

   ```
   $ESEC_HOME/_uninst
   ```

5. Entrez :

   ```
   ./uninstall.bin
   ```

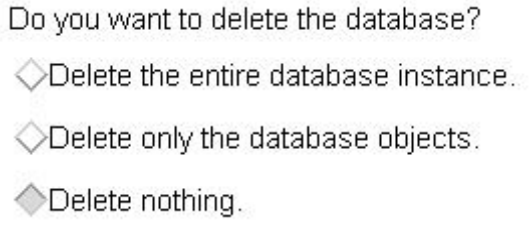
6. Suivez les invites d'écran. Sélectionnez les applications à désinstaller. Sélectionnez toutes les fonctions.



REMARQUE : si vous avez le logiciel d'intégration tiers, sélectionnez-le pour la désinstallation.

7. Cliquez sur les invites d'écran successives jusqu'à ce que la fenêtre Désinstallation de base de données s'affiche.

8. Dans la fenêtre Désinstallation de base de données, sélectionnez *Ne rien supprimer* :



9. Cliquez sur les fenêtres de désinstallation restantes.
10. Redémarrez le système.

Pré-migration – Installation de la base de données Sentinel 5

Installation de la base de données Sentinel 5

1. Vérifiez que vous avez collecté les informations, effectué les tâches et rempli toutes les conditions définies à la section Base de données Sentinel, au *chapitre 3 : Installation de Sentinel 5 pour Oracle, préinstallation de Sentinel 5 pour Oracle.*
2. Vérifiez la configuration Oracle en consultant la section sur la configuration Oracle au *Chapitre 3. Installation de Sentinel 5 pour Oracle, Préinstallation de Sentinel 5 pour Oracle.*
3. Loguez-vous comme utilisateur root.
4. Insérez et montez le CD d'installation de Sentinel.
5. Parcourez tout le répertoire sur le CD.
6. Démarrez le programme d'installation en accédant au répertoire d'installation sur le CD-ROM et entrez :

   En mode GUI :

   ```
   ./setup.sh
   ```

   ou

   En mode texte (« headless ») :

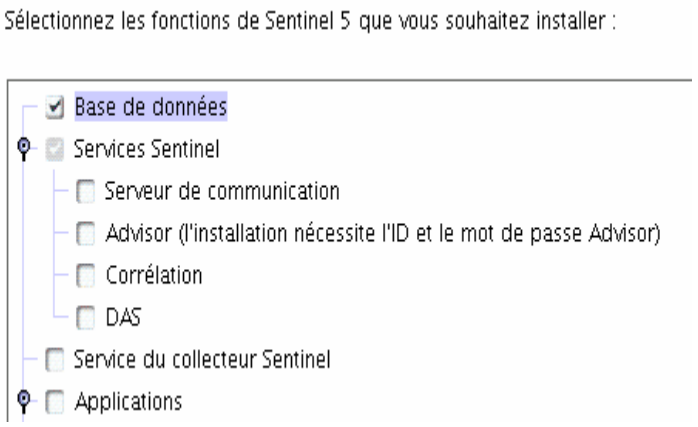
   ```
   ./setup.sh –console
   ```

7. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
8. Acceptez l'accord de licence utilisateur final, puis cliquez sur *Suivant*.
9. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* afin d'indiquer l'emplacement de l'installation. Cliquez sur *Suivant.*

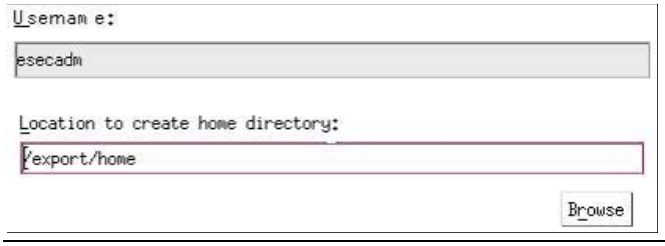
10. Sélectionnez *Personnalisée* (par défaut). Cliquez sur *Suivant.*

11. Pour choisir les fonctions à installer, désélectionnez toutes les fonctions et sélectionnez *Seulement base de données*. Cliquez sur *Suivant.*

REMARQUE : assurez-vous de désélectionner la fonction parent *Services Sentinel*. Elle apparaît en gris et cochée en blanc si elle est encore sélectionnée alors qu'aucune de ses fonctions enfants n'est sélectionnée.



12. Indiquez le nom d'utilisateur de l'administrateur Sentinel du système d'exploitation et l'emplacement de son répertoire privé. Il s'agit du nom d'utilisateur du propriétaire du produit Sentinel installé. Un utilisateur est créé, s'il n'en existe pas encore, ainsi qu'un répertoire privé dans le répertoire indiqué.
    - nom d'utilisateur de l'administrateur du SE – par défaut esecadm
    - répertoire privé de l'utilisateur de l'administrateur du SE – par défaut « /export/home » Si le nom d'utilisateur est esecadm, le répertoire privé de l'utilisateur est /export/home/esecadm.



REMARQUE : si un nouvel utilisateur est créé, son mot de passe doit être défini manuellement, hors du programme d'installation. Il est vivement conseillé de le faire directement en se loguant dans le système après l'installation du produit.

REMARQUE : afin d'accomplir les configurations de sécurité rigoureuses exigées par la certification de critères communs, Sentinel requiert un mot de passe fort avec les caractéristiques suivantes :

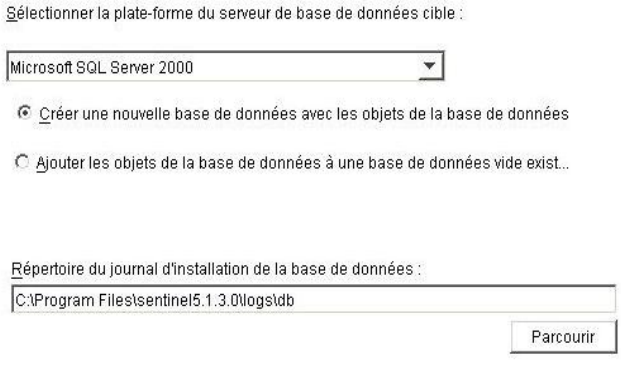
1. Choisissez des mots de passe comportant au moins 8 caractères qui incluent au moins un caractère en MAJUSCULE, un caractère en minuscule, un symbole spécial (#$_) et un caractère numérique (0 à 9). N'utilisez pas de vides.
2. Le mot de passe ne peut contenir ni votre adresse électronique, ni aucune partie de votre nom complet.

3. Le mot de passe ne doit pas être un nom commun (par exemple, ce ne doit pas être un mot du dictionnaire ou d'argot d'usage commun).

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

5. Vous devriez choisir un mot de passe facile à mémoriser mais complexe. Par exemple, Mea5 !A (Mon enfant a 5 ans) OU JhaPdp5#a (J'habite à Paris depuis 5 ans).

13. Entrez le nom d'hôte (ou IP) et le numéro de port (par défaut : 10012) pour le serveur de communication. Cliquez sur *Suivant.*
14. Sélectionnez Oracle comme plate-forme du serveur de la base de données cible et choisissez une des options suivantes :
    - créer une nouvelle base de données avec des objets de base de données - elle crée une nouvelle base de données Oracle et remplit la nouvelle instance avec des objets de base de données.
    - ajouter des objets de base de données à une base de données existante vide – elle ne fait qu'ajouter la base de données à une instance de la base de données Oracle existante. La base de données existante doit être vide, à l'exception de la présence de l'utilisateur esecdba.
15. Entrez le répertoire journal d'installation de bases de données (par défaut : $ESEC_HOME/logs/db). Acceptez le « Répertoire journal d'installation de la base de données » par défaut ou cliquez sur Parcourir afin de spécifier un emplacement différent.



16. Cliquez *OK* sur le nom d'utilisateur oracle par défaut.

17. Si vous choisissez de créer une nouvelle base de données, entrez les éléments suivants :
    - le chemin du fichier pilote Oracle JDBC (le nom type du fichier jar correspond à ojdbc14.jar). C'est le chemin complet vers le fichier jar, normalement $ORACLE_HOME/jdbc/lib/ojdbc14.jar (impossible d'utiliser des variables d'environnement dans ce champ).
    - nom d'hôte – le nom d'hôte de la machine pour installer la base de données Ce champ n'est pas configurable, si une nouvelle instance de base de données est créée.

- nom de la base de données – nom de l'instance de la base de données à installer.

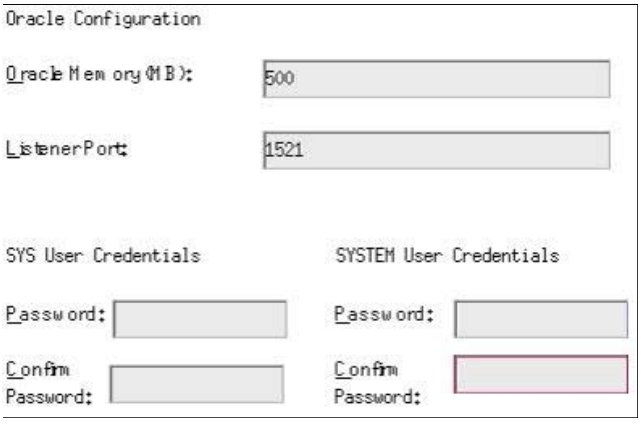
REMARQUE : vous devez nommer votre base de données avec un nom différent de celui spécifié lors de l'installation 4.2.

18. Si vous avez choisi d'ajouter des objets de la base de données à une base de données Oracle vide existante, une invite vous demande les informations suivantes :
    - le chemin du fichier pilote Oracle JDBC (le nom type du fichier jar correspond à ojdbc14.jar). C'est le chemin complet vers le fichier jar, normalement $ORACLE_HOME/jdbc/lib/ojdbc14.jar (impossible d'utiliser des variables d'environnement dans ce champ).
    - nom de la base de données ou adresse IP – le nom ou adresse IP de l'hôte où se trouve la base de données Oracle, à laquelle vous voulez ajouter des objets de base de données. Cela peut être le nom d'hôte local ou distant.
    - nom de la base de données – nom de l'instance de la base de données Oracle existante, vide,
      à laquelle vous voulez ajouter des objets de base de données (par défaut, ESEC, vous devez nommer votre base de données avec un nom différent de celui indiqué lors de l'installation 4.2). Ce nom de base de données doit s'afficher comme un nom de service dans le fichier tnsnames.ora (dans le répertoire $ORACLE_HOME/network/admin/) de la machine où le programme d'installation est exécuté.

REMARQUE : si le nom de la base de données n'est pas dans le fichier tnsnames.ora, le programme d'installation n'indique pas encore d'erreur à cette phase de l'installation (parce qu'il vérifie la connexion en utilisant une connexion directe JDBC), mais l'installation de la base de données échoue lorsque le programme d'installation de la base de données tente d'établir la connexion avec la base de données via sqlplus. Si l'installation de la base de données échoue à cette phase, sans quitter le programme d'installation, vous devez modifier le nom de service de cette base de données dans le fichier tnsnames.ora sur cette machine, puis retourner sur l'écran précédent dans le programme d'installation et avancer de nouveau. Cette démarche va réessayer l'installation de la base de données avec les nouvelles valeurs dans le fichier tnsnames.ora.

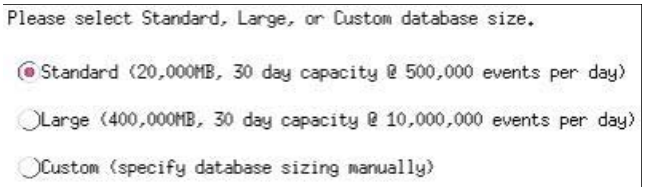
- port de la base de données (par défaut, 1521).
- Pour l'utilisateur de l'administrateur de la base de données Sentinel (DBA), spécifiez le mot de passe de l'utilisateur esecdba. Le mot de passe esecdba doit correspondre au mot de passe esecdba de votre l'installation v4.2. Le champ nom d'utilisateur de cette invite ne peut pas être édité.

19. Si vous choisissez de créer une nouvelle base de données, l'invite suivante s'affiche :
    - mémoire Oracle (Mo) – la quantité de RAM à allouer à cette instance de la base de données Oracle.
    - port du processus d'écoute – le port sur lequel est créé le processus d'écoute Oracle (par défaut, 1521)
    - mot de passe de l'utilisateur SYS et confirmation de mot de passe – SYS est l'utilisateur Oracle par défaut qui est créé dans la nouvelle instance de la base de données. Ce mot de passe d'utilisateur est défini avec la valeur indiquée ici.
    - mot de passe de l'utilisateur SYSTEM et confirmation de mot de passe – SYSTEM est l'utilisateur Oracle par défaut qui est créé dans la nouvelle instance de la base de données. Ce mot de passe d'utilisateur est défini avec la valeur indiquée ici.



20. Si vous choisissez de créer une nouvelle base de données, une invite vous demande d'entrer la taille de la base de données. Vous avez les options suivantes :
    - standard (20 Go)
    - grande (400 Go)
    - personnalisée (indiquez la taille manuellement). Si vous sélectionnez cette option, une invite vous demande :
        - taille initiale de chaque fichier de la base de données en Mo (de 100 à 10 000)
        - taille maximum de chaque fichier de la base de données en Mo (de 2 000 à 100 000)
        - taille de tous les fichiers de la base de données en Mo (de 7 000 à 2 000 000)

- taille de chaque fichier journal en Mo (de 100 à 100 000)



21. Si vous choisissez de créer une nouvelle base de données, une invite vous demande d'entrer l'emplacement d'archivage des fichiers de base de données suivants :

REMARQUE : à des fins de récupération et de performance, nous recommandons que ces emplacements soient dans des périphériques E/S différents.

Le programme d'installation ne crée pas ces répertoires, ils doivent donc être créés à l'extérieur avant de franchir cette étape.

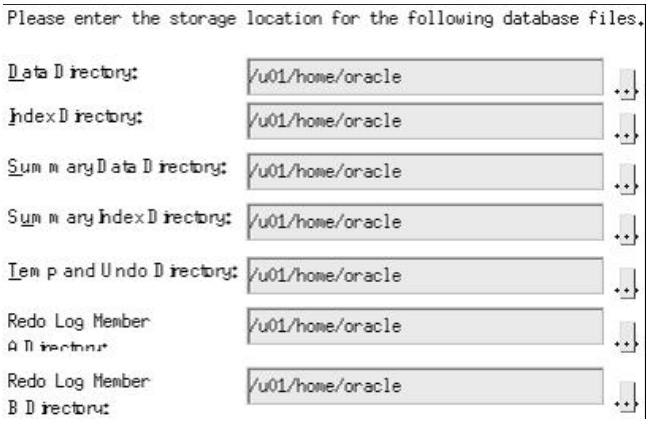
Ces répertoires doivent être accessibles en écriture pour l'utilisateur oracle. Pour que ces répertoires puissent être accessibles en écriture pour l'utilisateur oracle, exécutez les commandes suivantes pour chaque répertoire comme utilisateur root :

chown –R oracle:dba <chemin_répertoire>

chmod –R 770 <chemin_répertoire>

en partant du principe qu' « oracle » est le nom d'utilisateur Oracle et « dba » est le nom de groupe « oracle ».

- répertoire de données
- répertoire d'index
- répertoire de données récapitulatif
- répertoire d'index récapitulatif
- répertoire temporaire et d'annulation d'espaces de table
- journal des répétitions du répertoire du membre A
- journal des répétitions du répertoire du membre B



22. Si vous choisissez de créer une nouvelle base de données, entrez les informations d'authentification de l'administrateur de la base de données Sentinel. C'est esecdba, le propriétaire des objets de la base de données.
23. Entrez les informations d'authentification de l'utilisateur de la base de données de l'application Sentinel. C'est esecapp, le nom de l'utilisateur de l'application Sentinel que les procédures Sentinel utilisent pour se connecter à la base de données.

24. Entrez les informations d'authentification de l'utilisateur de la base de données de l'administrateur Sentinel. C'est esecadm, l'utilisateur de l'administrateur Sentinel.
25. Cliquez sur *Suivant* dans la fenêtre récapitulative de l'installation de la base de données.
26. Une fois l'installation terminée, une invite vous demande de redémarrer. Cliquez sur *Terminer* pour redémarrer le système.

Migration

L'utilitaire de migration de données ne fait migrer que les éléments suivants :

- les utilisateurs et les autorisations assignées
- les filtres
- les options de configuration de menu contextuel.
- les balises CV renommées
- les configurations de partition et d'archives
- les cas de la version 4.2 sont copiés sur la version 5 comme incidents.
- les incidents et les évènements liés aux incidents

REMARQUE : l'utilitaire de migration de données NE fait PAS migrer les données d'évènement, à l'exception des données d'évènements liés aux incidents. Seules les données d'évènements liés aux incidents sont migrées.

REMARQUE : les données d'évènements d'incidents ne peuvent pas s'afficher au moyen de Sentinel Control Center. Les données d'évènements d'incidents peuvent être vues à l'aide des rapports Crystal ou des requêtes SQL.

Pour les base de données Sentinel 4.2 qui n'utilisent pas esecdba comme propriétaire de schéma de la base de données Sentinel.

REMARQUE : cette procédure ajoute l'id esecdba à la base de données v4.2 afin de permettre la migration de données de v4.2 vers v5.

1. Pour Solaris, loguez-vous comme propriétaire du logiciel Oracle.
2. cd vers :

   ```
   $ESEC_HOME/utilities/db/scripts/ddl/oracle/Migration
   ```

3. À l'aide de SQL*Plus, effectuez une connexion à la base de données v4.2 comme SYSDBA.
4. À l'invite SQL (SQL>), entrez :

   ```
   @import_add_esecdba.sql
   ```

5. Quittez SQL*Plus.

REMARQUE : après l'exécution de la migration de données, vous pouvez utiliser Oracle Enterprise Manager pour supprimer l'utilisateur esecdba de la base de données Sentinel 4.2.

REMARQUE : sous Solaris, l'utilitaire de migration de données utilise Oracle*Net pour se connecter à la base de données Sentinel 5 et entre celle-ci et la base de données Sentinel 4.2. Assurez-vous que le fichier tnsnames.ora où vous exécutez l'utilitaire de migration de données contient des entrées pour la base de données Sentinel 5 et la base de données Sentinel 4.2, afin que les connexions Oracle*Net puissent être établies.

1. Loguez-vous comme utilisateur root.
2. Vérifiez les variables d'environnement pour vous assurer que java (version 1.4.2) est dans le CHEMIN. Vous pouvez le vérifier en exécutant la commande suivante sur la ligne de commande :

   ```
   java -version
   ```

   Si cette commande n'aboutit pas, localisez dans le système l'emplacement où java est installé ou téléchargez et installez java. Puis mettez à jour la variable d'environnement PATH afin d'inclure la version exécutable de java. Par exemple, si java est installé dans le répertoire :

   ```
   /opt/sentinel5.1.3.0/Sun-1.4.2
   ```

   Ajoutez ensuite les éléments suivants au début de la variable d'environnement PATH :

   ```
   /opt/sentinel5.1.3.0/Sun-1.4.2/bin:
   ```

3. Montez le CD d'installation du logiciel Sentinel 5 sur le serveur de la base de données où se trouve la base de données Sentinel 5.
4. cd vers le répertoire suivant sur le CD d'installation du logiciel Sentinel 5 :

   ```
   sentinel/dbsetup/bin
   ```

5. Exécutez la commande :

   ```
   ./MigrateDb.sh
   ```

6. Une invite vous demande les éléments suivants :
   - nom d'hôte de la base de données (où est exécutée la base de données Sentinel 5 vers laquelle vous migrez)
   - nom de la base de données cible (de la base de données Sentinel 5 vers laquelle vous migrez)
   - mot de passe esecdba (le mot de passe doit correspondre à l'utilisateur esecdba sur les bases de données Sentinel v4.2 et v5
   - nom de la base de données source, (nom de la base de données v4.2)
   - répertoire du journal (où les fichiers journaux de migration de données sont placés)
   - option de migration :
     - (1) paramètres du système
     - (2) incidents/cas
     - (3) les deux
     - (4) terminé

REMARQUE : les paramètres du système devront être migrés avec succès avant de passer à la migration des incidents et des cas.

REMARQUE : si la migration des paramètres du système échoue, désinstallez la base de données Sentinel 5 en sélectionnant l'option « Supprimer seulement les objets de la base de données ». Puis, réinstallez la base de données Sentinel 5 en sélectionnant l'option « Ajouter les objets de la base de données à une base de données vide existante ». Finalement, réessayez de suivre les instructions de migration de données.

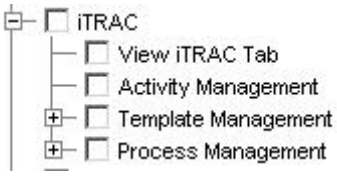
REMARQUE : si la migration d'incidents échoue, re-exécutez la migration d'incidents. L'utilitaire de migration redémarre à partir du point d'échec. Aucune tâche de nettoyage supplémentaire n'est requise.

REMARQUE : après l'exécution de la migration de données, vous pouvez utiliser Oracle Enterprise Manager pour supprimer l'utilisateur esecdba de la base de données Sentinel 4.2, si vous voulez l'ajouter à l'utilitaire de migration de données.

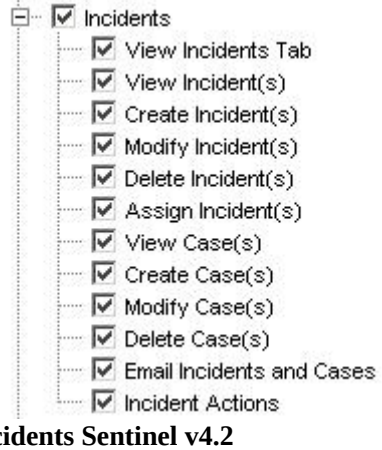
Post-migration – Installation de Sentinel 5

Dans le Sentinel 5, les fonctions suivantes sont nouvelles, différentes ou retirées.

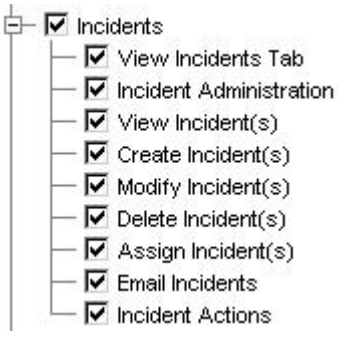
- iTRAC – une nouvelle fonctionnalité. Les autorisations d'utilisateur associées sont :



- incidents – administration des incidents ajoutés toute fonctionnalité liée à la casse retirée. Les autorisations d'utilisateur associées sont :



Incidents Sentinel v4.2



Incidents Sentinel v5

- gestion de collecteurs – dans la v4.2, c'est la surveillance de l'assistant. L'onglet « Affichage assistants » est remplacé par « Affichage collecteurs ». « Contrôler assistants et collecteur » est remplacé par « Contrôler collecteurs » et « Administration de collecteurs ». Les autorisations d'utilisateur associées sont :

Surveillance Wizard Sentinel v4.2

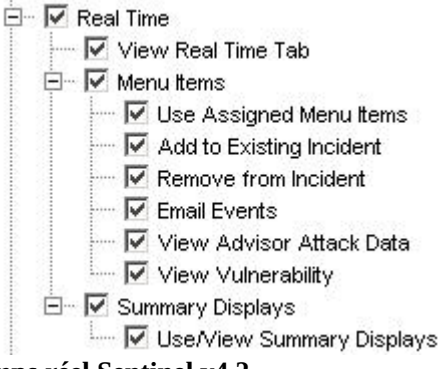
Gestion de collecteurs Sentinel v5

- administration – ajout de statistiques DAS, gestion de session d'utilisateur et gestion de rôle iTRAC Les « Règles de corrélation » ont été renommées « Corrélation ». La fonction Configuration d'évènements a été déplacée vers le gestionnaire de données Sentinel. La « Configuration d'utilisateur » a été renommée « Gestion d'utilisateur ». Les autorisations d'utilisateur associées sont :

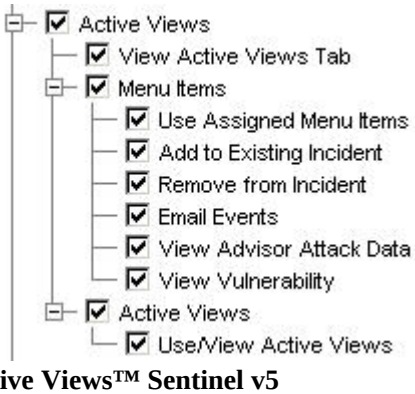
Administration Sentinel v4.2

Administration Sentinel v5

- ActiveViews™ – dans la v4.2, la fonction s'appelait Temps Réel. les « Écrans récapitulatifs » ont été renommés Active Views. Les autorisations d'utilisateur associées sont :



Temps réel Sentinel v4.2



Active Views™ Sentinel v5

- la fonctionnalité de présentation du système n'est pas disponible sous Sentinel 5.

Installation de Sentinel 5

1. Installez Sentinel 5, voir le chapitre « Installation de Sentinel pour Oracle ».
2. Installez le Sentinel Service Pack le plus récent.
3. Effectuez les étapes suivantes si vous voulez ajouter une nouvelle fonctionnalité à l'un des utilisateurs existants de la v4.2 :
   a. Assurez-vous que le serveur Sentinel est en cours d'exécution.
   b. Loguez-vous dans Sentinel Control Center comme un utilisateur doté d'autorisation Administration/Gestion d'utilisateurs (par ex. esecadm).
   c. Dans Sentinel Control Center, cliquez sur l'onglet Admin. Agrandissez Configuration d'utilisateurs dans le volet de navigation ou depuis la barre de navigation cliquez *Admin > Configuration de l'utilisateur*.

d. Cliquez avec le bouton droit sur l'utilisateur auquel vous voulez ajouter la fonctionnalité (par ex. esecadm) et sélectionnez *Détails de l'utilisateur*. Cliquez sur l'onglet *Autorisations*.
e. Agrandissez iTRAC et assignez les autorisations selon les besoins.
f. Agrandissez Incidents et assignez « Administration d'incidents » selon les besoins.
g. Agrandissez Gestion de collecteurs et assignez « Administration de collecteurs » selon les besoins.
h. Agrandissez Administration et assignez « Statistiques DAS », « Gestion de session d'utilisateur » ou « Gestion de rôle iTRAC » selon les besoins.
i. Cliquez sur l'onglet *Rôles* et assignez Admin ou Rôle du processus de travail de l'analyste selon les besoins.
j. Cliquez sur *OK*.

4. Le cas échéant, importez les règles de corrélation. Les ensembles de règles exportés de Sentinel 4.2 sont affichés comme Dossiers de règles lors de leur importation dans Sentinel 5.
5. Copiez à partir de la sauvegarde des scripts de collecteurs et des configurations de ports, en suivant les instructions de la section Post-migration – Reconfiguration des scripts de collecteurs et des configurations de ports.

Post-migration – Reconfiguration des scripts de collecteurs et des configurations de ports

Sur chaque machine où le service de collecteurs (gestionnaire de collecteurs) Sentinel 5 est installé, effectuez les étapes suivantes pour rétablir les scripts de collecteurs et les configurations de ports utilisées dans l'installation de Sentinel v4.2.

Pour rétablir les scripts de collecteurs et les configurations de ports

1. Arrêter le gestionnaire de collecteurs en exécutant la commande suivante comme utilisateur esecadm :

   ```
   $ESEC_HOME/wizard/agent-manager.sh stop
   ```

2. Depuis l'emplacement où vous avez placé la sauvegarde du répertoire $WORKBENCH_HOME/Agents de l'installation Sentinel v4.2, copiez les fichiers suivants dans le répertoire $WORKBENCH_HOME\Agents de l'installation actuelle Sentinel 5 (écrasez les fichiers, si nécessaire):
   - localhost_portcfg.dat
   - localhost_snmpcfg.dat
3. Lisez le fichier de texte créé pendant la pré-migration qui liste tous les collecteurs utilisés par l'installation du gestionnaire de collecteurs Sentinel v.4.2 sur cette machine. Vous devez connaître les noms de collecteurs pour l'étape suivante.
4. Depuis l'emplacement où vous avez placé la sauvegarde du répertoire $WORKBENCH_HOME\Elements de l'installation Sentinel 4.2, copiez les répertoires dont les noms correspondent aux noms des collecteurs dans le fichier de texte dans le répertoire $WORKBENCH_HOME\Elements de l'installation actuelle Sentinel 5 (écrasez les fichiers, si nécessaire).
5. Procurez-vous l'utilitaire UpgradePortCfgFile sur le site Web du support technique Sentinel (téléchargez ici).
6. Extrayez le fichier ZIP UpgradePortCfgFile .

7. Ouvrez une invite de commande et passez les répertoires dans le répertoire de l'utilitaire UpgradePortCfgFile extrait. Depuis ce répertoire, exécutez la commande :

   ```
   ./UpgradePortCfgFile.sh
   ```

8. Exécutez la commande suivante comme utilisateur root pour assurer que la propriété des fichiers copiés est dûment configurée:

   ```
   chown –R esecadm:esec $ESEC_HOME/wizard
   ```

9. Démarrer le gestionnaire de collecteurs en exécutant la commande suivante comme utilisateur esecadm :

   ```
   $ESEC_HOME/wizard/agent-manager.sh start
   ```

Post-migration – Configuration de Sentinel 5 pour la création de rapport Crystal

Si vous exécutez la création de rapport Crystal pour 4.2 et si vous voulez exécuter la création de rapport Crystal dans Sentinel 5, vous devez :

- modifier les paramètres Oracle 9i client liés à la création de rapport Crystal pour cibler la base de données Sentinel 5.
- importer les modèles de Crystal Report (y compris les modèles de migration de données) depuis le Service Pack le plus récent.

Voir le chapitre « Installation de Crystal Reports », pour plus d'informations.

Correctifs de v5.x.x vers v5.1.3

Effectuez cette procédure sur une machine où des composants Sentinel sont installés.

Si vous êtes en train d'exécuter le programme d'installation du correctif où vous avez initialement installé le composant de la base de données, vous devez connaître le mot de passe de l'utilisateur de l'administrateur de la base de données Sentinel (esecdba).

Mise à niveau de v5.x.x vers v5.1.3 pour Solaris

1. Loguez-vous comme utilisateur root.
2. Le cas échéant, faites une copie de sauvegarde de fichier syslog.conf.

   REMARQUE : Si vous exécutez v5.1.1sp1 ou des versions supérieures et que vous avez fait des modifications sur le fichier syslog.conf, vous devez faire une copie du fichier syslog.conf. Le programme d'installation du correctif écrase le fichier syslog.conf. Après la correction, modifiez ou écrasez le nouveau fichier syslog.conf pour qu'il corresponde au fichier syslog.conf original.

3. Insérez et montez le CD Correctif de Sentinel.
4. Démarrez le programme d'installation en allant au répertoire du correctif adéquat sur le CD-ROM et en exécutant la commande suivante :

   En mode GUI :

   ```
   ./setup.sh
   ```

ou

En mode texte (« headless ») :

```
./setup.sh –console
```

5. Cliquez *Suivant* sur l'écran d'accueil.
6. Acceptez l'accord de licence utilisateur final et cliquez sur *Suivant*.
7. Cliquez sur *Suivant* jusqu'à la fenêtre d'informations de bases de données.
8. Veillez à ce que le type de base de données soit correct. Sélectionnez l'emplacement du répertoire de journal d'installation de bases de données. Cliquez sur *Suivant.*
9. Veillez à ce que les informations concernant le serveur Oracle soient correctes. Entrez le mot de passe de esecdba. Suivez les invites restantes du programme d'installation.

Mise à jour du connecteur Syslog

Si vous utilisez les scripts du connecteur syslog d'une version Sentinel antérieure à 5.1.1.1 (par ex. 5.0, 5.0.1.0, 5.1.0.0 ou 5.1.1.0), vous devez commencer à utiliser les scripts du connecteur syslog mis à jour qui sont inclus dans le correctif. Afin de passer de l'utilisation de l'ancien script du connecteur syslog à celle des nouveaux scripts du connecteur syslog, déplacez l'ancien script et installez un nouveau script.

Le connecteur syslog est installé avec des scripts qui sont exécutés sous Windows et UNIX avec des fichiers de configuration améliorés. En outre, l'installation du serveur proxy syslog comme service a été simplifiée.

Pour déplacer le connecteur Syslog

1. Loguez-vous comme utilisateur root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

Pour installer le connecteur Syslog

1. Loguez-vous comme utilisateur root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh install
4. Si vous avez fait des modifications sur le fichier syslog.conf de l'installation originale, vous devez modifier ou écraser le nouveau fichier syslog.conf afin de refléter le fichier syslog.conf original, localisé à :

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

Mise à jour supplémentaire de v5.0.x vers v5.1.3

Après l'installation des correctifs de v5.0.x vers v5.1.3, vous devez mettre à jour les autorisations de gestion d'utilisateurs et les options de configuration de menu. Vous pouvez optionnellement mettre à jour l'autorisation Vues de serveurs.

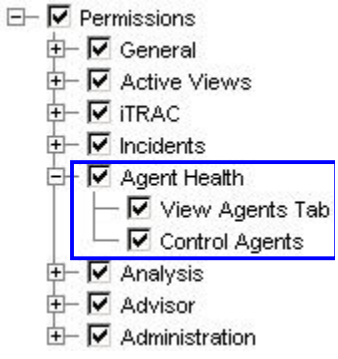
Mise à jour des autorisations de gestion d'utilisateurs de v5.0.x vers v5.1.3

Lors de la mise à jour de v5.0.x vers v5.1.3, l'état de santé des collecteurs est remplacée par la gestion de collecteurs, avec une fonctionnalité supplémentaire d'administration de collecteurs.

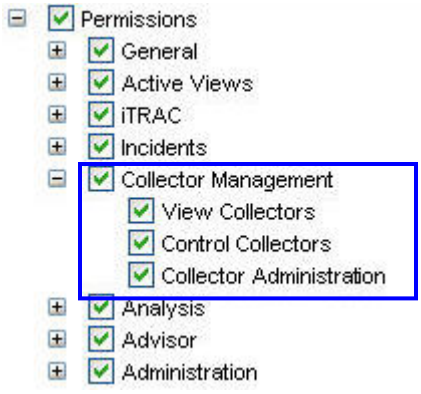
Mise à jour des autorisations de gestion d'utilisateurs

1. Loguez-vous dans Sentinel Control Center comme un utilisateur doté d'autorisation Administration/Gestion d'utilisateurs.

   Dans la v5.1, l'état de santé des collecteurs sous Autorisations est passé de l'« Etat de santé des collecteurs » à la « Gestion de collecteurs » avec une autorisation supplémentaire ajoutée.



Autorisation d'utilisateur Sentinel v5.0



Autorisation d'utilisateur Sentinel v5.1

2. Dans Sentinel Control Center, cliquez sur l'onglet Admin. Agrandissez Configuration d'utilisateurs dans le volet de navigation ou depuis la barre de navigation cliquez sur *Admin* > *Configuration de l'utilisateur*.
3. Cliquez avec le bouton droit sur un utilisateur Admin (c.-à-d. esecadm ou tout autre utilisateur admin) > *Détails de l'utilisateur*. Cliquez sur l'onglet *Autorisations*.
4. Agrandissez *Gestion de collecteurs* et assignez *Administration de collecteurs*. Cliquez sur *OK*.

Mise à jour des options de configuration de menu de v5.0.x vers v5.1.3

Si des entrées supplémentaires ont été créées dans la configuration de menus avant la mise à jour vers v5.1, les chemins des commandes doivent être mis à jour. À partir de la version 5.1.0.0, sous Solaris, la commande à exécuter dans la configuration de menus doit exister dans le répertoire $ESEC_HOME/sentinel/exec. En plus, tous les chemins vers les commandes exécutées dans la configuration de menus sont toujours liés au répertoire $ESEC_HOME/sentinel/exec. Vous devez exécuter une commande en dehors du système de fichiers et puis créer une liaison symbolique depuis un emplacement sous $ESEC_HOME/sentinel/exec vers la commande à exécuter.

La configuration de menus pour traceroute doit être modifiée manuellement, « tracert » étant remplacé par « traceroute », afin qu'elle fonctionne correctement.

Pour ajouter une option au menu de configuration de menu

1. Loguez-vous dans Sentinel Control Center comme un utilisateur doté d'autorisation Administration/Gestion d'utilisateurs.
2. Cliquez sur l'onglet *Admin*.
3. Dans le navigateur Admin, cliquez sur *Admin* > *Configuration de menu.*
4. Sur la fenêtre Configuration de menu, cliquez sur *Modifier* et sélectionnez un élément du menu à mettre à jour. Cliquez sur *Détails*.
5. Dans la boîte de dialogue Configuration de menu, faites le nécessaire dans :

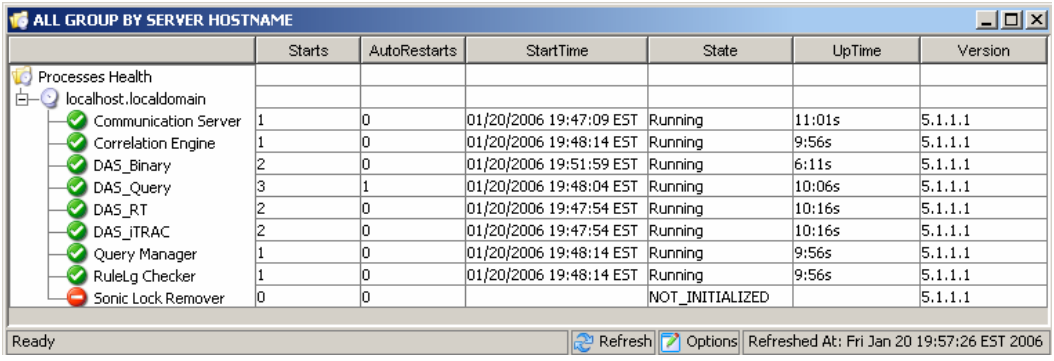
- ligne de commande/URL
- paramètres – ils doivent être entre deux signes de pourcentage (par ex, %EventName%).

REMARQUE : Pour voir une liste des balises disponibles que vous pouvez utiliser pour définir les paramètres, cliquez sur Aide de la boîte de dialogue Configuration du menu
ou consultez le chapitre sur les meta-balises dans le Guide de références de l'utilisateur Sentinel.

6. Cliquez sur *OK*.
7. Cliquez sur *Enregistrer*.

Mise à jour des options de vues de serveur de v5.0.x vers v5.1.3

Afin d'utiliser l'écran Vue de serveur après l'installation du correctif, vous devez donner l'autorisation « Vues de serveur » à l'utilisateur Sentinel, à l'aide du gestionnaire d'utilisateurs. Le gestionnaire d'utilisateurs est localisé sous l'onglet Admin de Sentinel Control Center.



Serveur de création de rapport Crystal

Après la mise à niveau vers Sentinel 5.1.3, y compris l'application du Service Pack le plus récent, vous devez importer les rapports du Service Pack le plus récent. Pour plus d'informations, voir le chapitre sur *Crystal Reports* dans le *guide d'installation Sentinel*.

Mise à jour du courrier électronique Sentinel pour l'authentification SMTP

Si le système requiert une authentification SMTP, vous devez mettre à jour le fichier execution.properties. Ce fichier est sur la machine où le DAS est installé. Il est localisé à

$ESEC_HOME/sentinel/config. Pour configurer ce fichier, exécutez mailconfig.sh, afin de changer le fichier et mailconfigtest.sh pour tester ces changements.

Pour configurer le fichier execution.properties

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfig de la façon suivante :

   ```
   ./mailconfig.sh -host <serveur SMTP> -from <adresse
         électronique source> -user <utilisateur
         authentification courrier électronique> –password
   ```

   Exemple :

   ```
   ./mailconfig.sh -host 192.0.2.14 -from nom@domaine.com -
         user nom_utilisateur –password
   ```

   Après cette commande, une invite vous demande d'entrer un nouveau mot de passe.

   ```
   Entrez le mot de passe :*********

   Confirmez le mot de passe :*********
   ```

   REMARQUE : lors de l'utilisation de l'option de mot de passe, ce doit être le dernier argument.

Pour tester la configuration d'execution.properties

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfigtest de la façon suivante :

   ```
   ./mailconfigtest.sh -to <adresse électronique cible>
   ```

   Si l'envoi du message électronique a abouti, vous obtenez le résultat suivant sur l'écran et le message est reçu à l'adresse cible.

   ```
   Message électronique envoyé avec succès !
   ```

   Vérifiez la boîte aux lettres de l'adresse cible pour confirmer la réception du message. La ligne d'objet et le contenu devraient être les suivants :

   ```
   Objet : Test des propriétés du courrier électronique
         Sentinel

   Test de configuration des propriétés du courrier
         électronique Sentinel. Si ce message apparaît, les
         propriétés du courrier électronique Sentinel ont été
         correctement configurées pour envoyer des messages.
   ```

7 Migration et correctif de données pour MS SQL

REMARQUE : le terme « agent » est échangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Ce chapitre traite de la migration et de la mise à jour des données concernant :

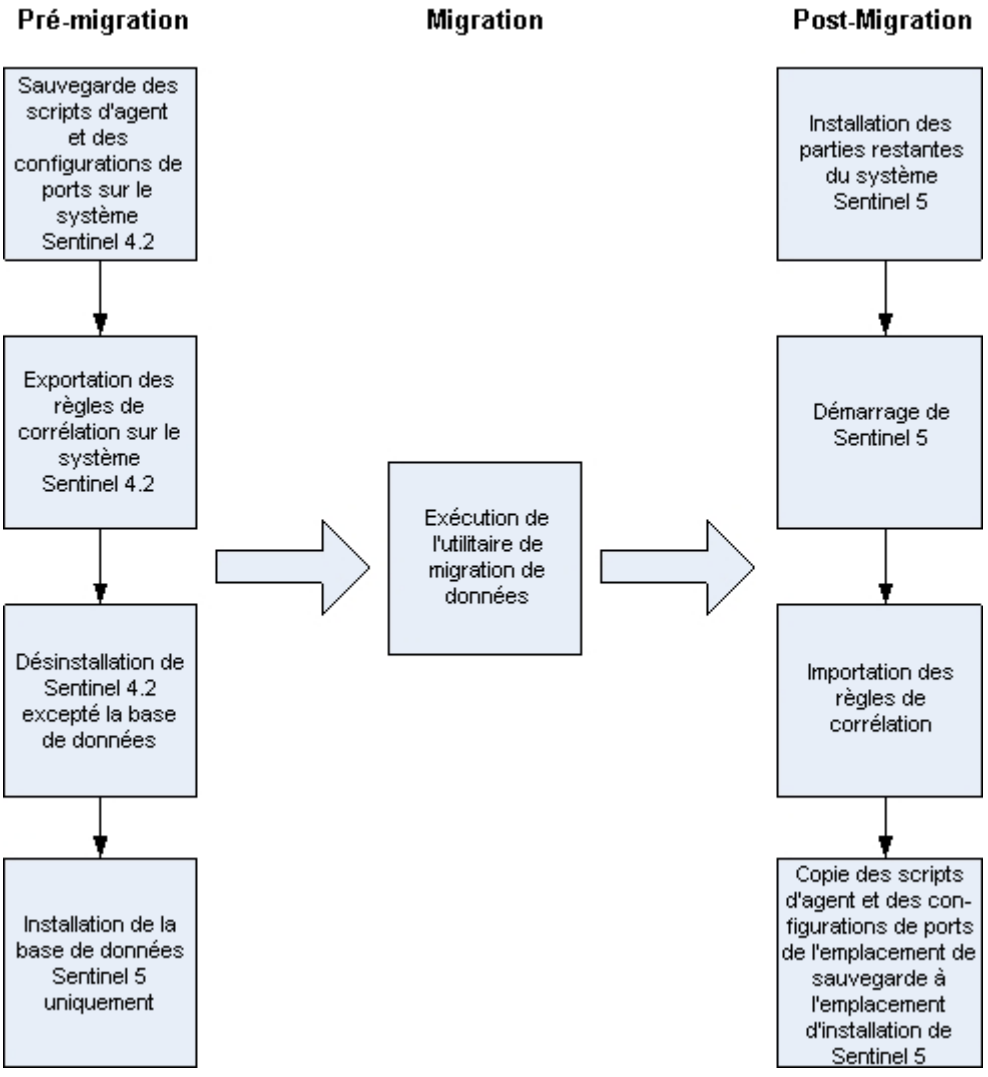
- la migration et la mise à jour des données de v4.2.1 à v5.1.3.
- le correctif de v5.x.x à v5.1.3

Migration et mise à jour des données de v4.2 vers v5.1.3.

Le processus de mise à jour de Sentinel 5 avec migration de données à partir de la version v4.2.0 consiste dans les étapes suivantes :

- pré-migration
  - Sauvegarder l'instance de la base de données du serveur Sentinel : Cette copie vous permet de restaurer la base de données v4.2, en cas d' échecs imprévus.
  - Sauvegardez toutes les commandes contextuelles du système ou tous les scripts sous le répertoire %ESEC_HOME%
  - Exportez les règles de corrélation de Sentinel v4.2 (le cas échéant). Pour lire les instructions, consultez Pré-migration – Exportation des règles de corrélation.
  - Sauvegardez les scripts de collecteurs et les configurations de ports. Pour lire les instructions, consultez Pré-migration – Sauvegarde des scripts de collecteurs et des configurations de ports.
  - Sauf pour le composant de la base de données, désinstallez Sentinel v4.2. Pour lire les instructions, consultez Pré-migration – Désinstallation de v4.2.
  - Installez seulement la base de données Sentinel 5. Consultez Pré-migration – Installation de la base de données Sentinel 5 pour lire les instructions.
- migration
  - Exécutez l'utilitaire de migration de données. Pour lire les instructions, consultez Migration.
- post-migration
  - Installez les composant restants de Sentinel 5. Pour lire les instructions, consultez Post-migration – installation de Sentinel 5.
  - Installez le Sentinel Service Pack le plus récent.
  - Démarrez Sentinel 5.
  - Importez les règles de corrélation (le cas échéant). Pour lire les instructions, consultez Post-migration – installation de Sentinel 5.
  - Copiez les scripts de collecteurs et les configurations de ports à partir de l'emplacement de sauvegarde dans l'emplacement de l'installation Sentinel 5. Pour lire les instructions, consultez Post-migration – Reconfiguration des scripts de collecteurs et des configurations de ports.

- Si vous exécutez le serveur Crystal Server avec Sentinel, importez les modèles de Sentinel 5 Crystal Reports. Pour lire les instructions, consultez Post-migration – Configuration de Sentinel 5 pour la création de rapport Crystal.



Serveur Sentinel

Sentinel 5 requiert la désinstallation de la version antérieure du logiciel, avant l'ajout des composants Sentinel 5. Ne désinstallez pas la version antérieure (v4.2) de la base de données, puisqu'elle est nécessaire à la migration de données de v4.2 vers Sentinel 5. Sauvegardez la machine du serveur Sentinel (répertoire d'installation %ESEC_HOME% et unité root) avant la désinstallation. Cette copie vous permet de restaurer la v4.2, en cas d' échecs imprévus.

Vous trouverez ci-dessous des instructions détaillées sur la migration de données et sur la pré et post-installation.

Gestionnaire de collecteurs

Sentinel 5 requiert la désinstallation de tous les gestionnaires de collecteurs de la version v4.2 avant l'installation du logiciel du gestionnaire de collecteurs Sentinel 5. Sauvegardez la machine du gestionnaire de collecteurs v4.2 (répertoire d'installation %ESEC_HOME% et unité root) avant la désinstallation.

Pour chaque machine exécutant le gestionnaire de collecteurs v4.2 avec au moins un port configuré, sauvegardez une copie des contenus des répertoires suivants dans un emplacement facile d'accès. Les contenus de ces répertoires seront utilisés pendant la post-migration afin de reconfigurer plus rapidement la définition des ports de collecteurs sur l'installation v4.2.

- %WORKBENCH_HOME%/Agents – il contient les fichiers de configuration de ports.
- %WORKBENCH_HOME%/Elements – il contient les scripts de collecteurs.
- Si vous ne faites pas de copie des contenus des répertoires ci-dessus, il vous faudra reconfigurer tous les scripts et ports de collecteurs depuis le début.

REMARQUE : le gestionnaire de collecteurs et le générateur de collecteurs de la version 4.2 ne sont pas compatibles avec les composants de la version 5.

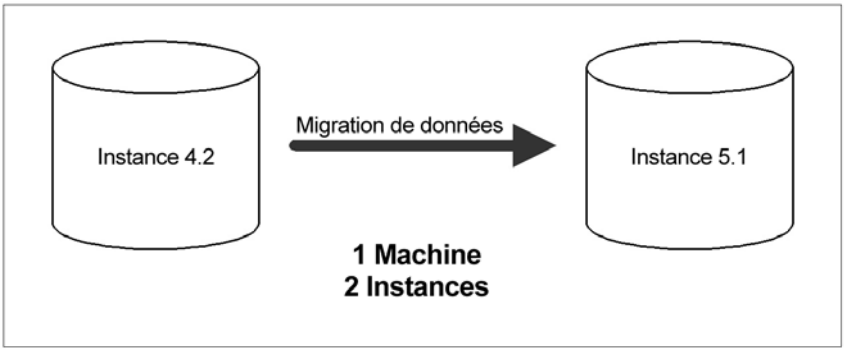
Vous trouverez ci-dessous des instructions détaillées sur la migration de données et sur la pré et post-installation.

Serveur de création de rapport Crystal

Vous devez utiliser les rapports les plus récents du Service Pack le plus récent, après la mise à jour de Sentinel 5. Les nouveaux rapports sont configurés pour travailler avec le nouveau schéma de BD. Pour obtenir le Service Pack le plus récent, contactez le support technique Sentinel.

Serveurs de la base de données

Un utilitaire de migration de données Sentinel 5 est fourni pour copier les données de Sentinel v4.2.1 vers Sentinel v5.1.3. L'utilitaire de migration de données ne prend en charge la migration que si les deux bases de données Sentinel 4.2.1 et Sentinel 5.1.3 se trouvent sur la même machine et dans la même instance de SQL Server, mais chacune sur une base de données différente.



Les éléments suivants migrés :

- les utilisateurs et les autorisations assignées
- les filtres
- les options de configuration de menu contextuel.

- les balises CV renommées
- les configurations de partition et d'archives
- les cas de la version 4.2 sont copiés sur la version 5 comme incidents.
- les incidents et les évènements liés aux incidents

REMARQUE : l'utilitaire de migration de données NE fait PAS migrer les données d'évènement, à l'exception des données d'évènements liés aux incidents. Seules les données d'évènements liés aux incidents sont migrées.

REMARQUE : les données d'évènements d'incidents ne peuvent pas s'afficher au moyen de Sentinel Control Center. Les données d'évènements d'incidents peuvent être vues à l'aide des rapports Crystal ou des requêtes SQL.

Pré-migration – Exportation des règles de corrélation

Importation ou Exportation d'un ensemble de règles de corrélation

1. Sur la console Sentinel v4.2, sous l'onglet Admin ouvrez la fenêtre Règles de corrélation.
2. Sélectionnez un ensemble de règles.
3. Cliquez sur *Exporter*. Un navigateur de fichiers est ouvert, recherchez le périphérique cible où écrire la règle et cliquez sur *OK*. L'ensemble de règles est exporté comme fichier xml.

Pré-migration – Sauvegarde des scripts de collecteurs et des configurations de ports

Sauvegarde des scripts de collecteurs et des configurations de ports

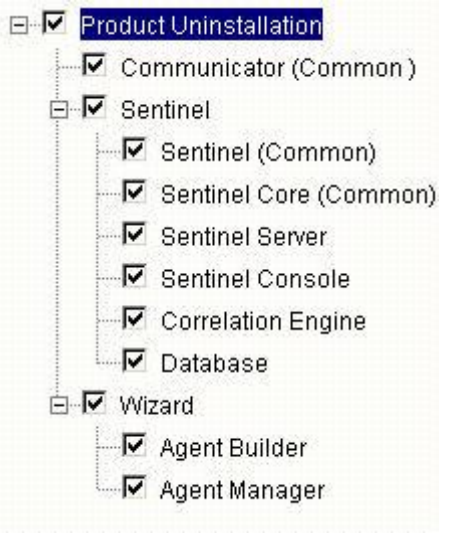
1. Sur toutes les machines Sentinel v4.2 qui exécutent le gestionnaire de collecteurs, créez un répertoire pour stocker les scripts de collecteurs et les configurations de ports de tous les collecteurs pour chaque machine.
2. Dans le répertoire créé, créez un fichier de texte listant les noms de tous les collecteurs utilisés par une configuration de port sur ce gestionnaire de collecteurs. Utilisez un générateur de collecteurs pour déterminer les collecteurs utilisés par ce gestionnaire de collecteurs. Si le gestionnaire de collecteurs est sur UNIX, il vous faut utiliser un générateur de collecteurs sur une machine Windows (le générateur de collecteurs n'est pas pris en charge sur UNIX).
3. Copiez les répertoires suivants dans le répertoire qui vous venez de créer.
   - %WORKBENCH_HOME%\Agents
   - %WORKBENCH_HOME%\Elements

Pré-migration – désinstallation de v4.2

Désinstallation de v4.2

1. Sur la machine Sentinel v4.2 :
   - fermez toutes les consoles et tous les générateurs de collecteurs Sentinel.
   - cliquez *Démarrer* > *Programmes* > *Sentinel* > *Désinstaller Sentinel 4.2.1.x*.

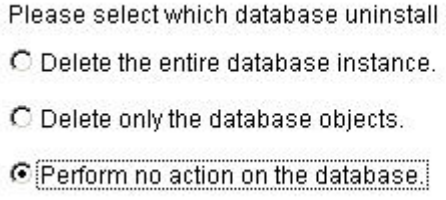
2. Cliquez sur les invites d'écran successives jusqu'à ce que la fenêtre Désinstallation s'affiche. Sélectionnez toutes les fonctionnalités.



REMARQUE : dans l'exemple ci-dessus, le logiciel d'intégration tiers n'est pas présenté. Si vous avez le logiciel d'intégration tiers, sélectionnez-le pour la désinstallation.

Cliquez sur les invites d'écran successives jusqu'à ce que la fenêtre Désinstallation de base de données s'affiche.

3. Dans la fenêtre Désinstallation de base de données, sélectionnez *N'effectuer aucune opération sur la base de données*.



4. Cliquez sur les fenêtres de désinstallation restantes.

Pré-migration – Installation de la base de données Sentinel 5

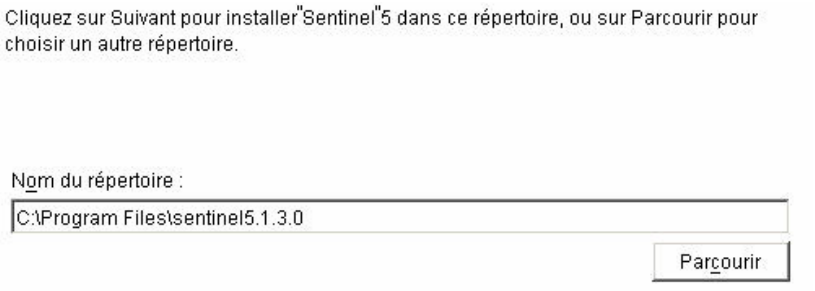
Installation de la base de données Sentinel 5

1. Vérifiez que la variable d'environnement ne se réfère pas à 4.2. Dans ce cas, éliminez-la. Les variables d'environnement suivantes ne devraient pas apparaître :
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME

2. Vérifiez que vous avez collecté les informations, effectué les tâches et rempli toutes les conditions définies à la section Base de données Sentinel 4, au *chapitre 4 : Installation de Sentinel 5 pour MS SQL, Préinstallation de Sentinel 5 pour MS SQL*.
3. Insérez le CD d'installation Sentinel dans l'unité de CD-ROM.
4. Parcourrez le CD et double-cliquez sur *setup.bat*.

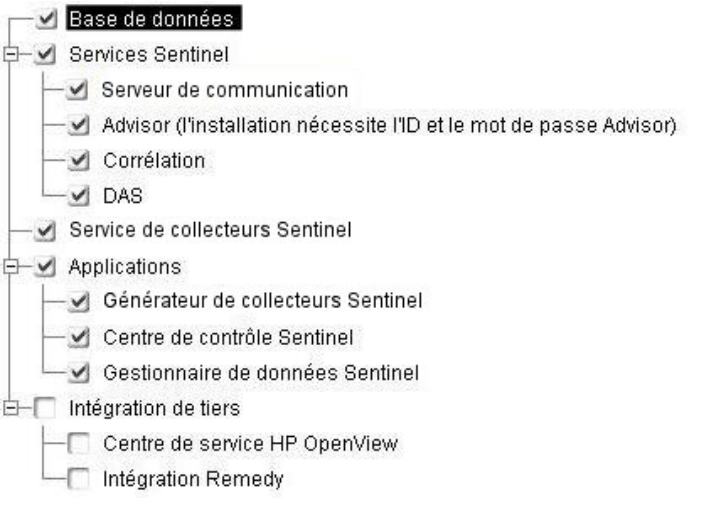
REMARQUE : l'installation en mode de console n'est pas prise en charge sous Windows.

5. Cliquez sur la flèche bas et sélectionnez une des langues suivantes au choix.
   - anglais
   - français
   - allemand
   - italian
   - portugais
   - espagnol
6. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
7. Acceptez l'accord de licence utilisateur final, puis cliquez sur *Suivant*.
8. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* afin de spécifier un autre emplacement. Cliquez sur *Suivant*.

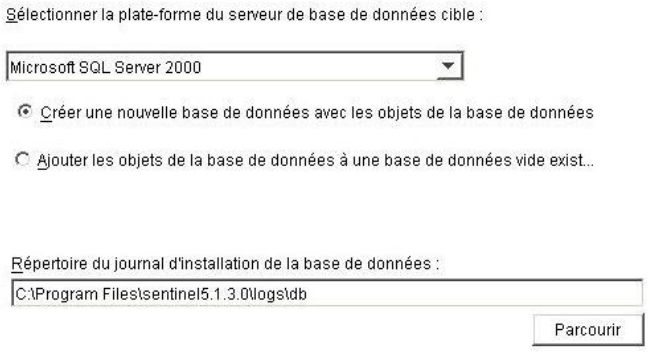


9. Pour le type d'installation, sélectionnez *Personnalisée* (par défaut). Cliquez sur *Suivant*.
10. Pour choisir les fonctions à installer, désélectionnez toutes les fonctions et sélectionnez *Seulement base de données*. Cliquez sur *Suivant*.

REMARQUE : assurez-vous de désélectionner la fonction parent « Services Sentinel ». Elle apparaît en gris et cochée en blanc si elle est encore sélectionnée alors qu'aucune de ses fonctions enfants n'est sélectionnée.



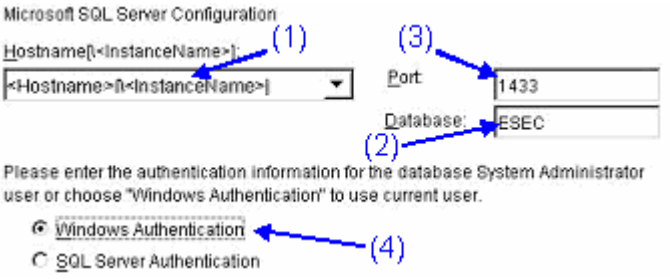
11. Entrez le nom d'hôte (ou IP) et le numéro de port (par défaut : 10012) pour le serveur de communication. Cliquez sur *Suivant*.
12. Sélectionnez *Microsoft SQL Server* comme plate-forme de base de données cible et sélectionnez *Créer une nouvelle base de données avec les objets de la base de données*. Entrez également le répertoire journal d'installation de bases de données (par défaut : %ESEC_HOME%\logs\db). Acceptez le *Répertoire journal d'installation de la base de données* par défaut ou cliquez sur *Parcourir* afin de spécifier un emplacement différent. Cliquez sur *Suivant*.



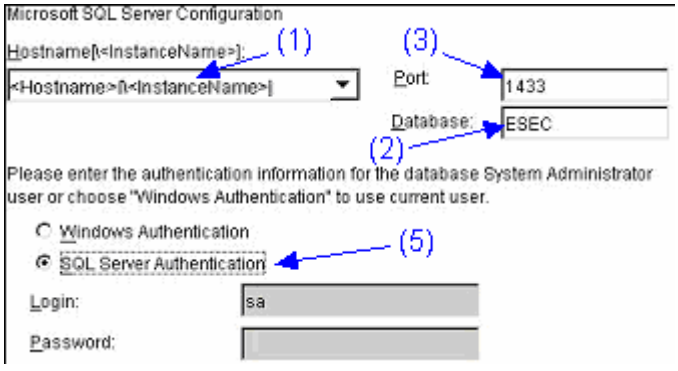
13. Entrez les informations de configuration de SQL Server :
    - (1) nom d'hôte de la base de données ou adresse IP – Par défaut, la machine de l'hôte local apparaît, si SQL Server est installé localement. Si le serveur SQL Server que vous voulez installer n'apparaît pas dans la liste déroulante, sélectionnez *Autre* sur la liste. une zone de texte est affichée pour que vous y tapiez le nom d'hôte. Le nom d'hôte inséré doit être complet (par ex. « sqlserver.sentinel.net » au lieu de seulement « sqlserver »). Si vous avez défini un nom d'instance pendant l'installation de SQL Server, vous devez ajouter « <nom_instance> » à la fin du nom d'hôte, où <nom_instance> correspond au nom donné à l'instance lors de l'installation de SQL.Server
    - (2) nom à donner à la nouvelle base de données SQL Server. Outre la base de données nommée ici, une autre base de données nommée <nom_ma_bd>_WF est également créée afin d'être utilisée par l'iTRAC.

REMARQUE : vous devez nommer votre base de données avec un nom différent de celui indiqué lors de l'installation 4.2.

    - (3) port de la base de données (par défaut, 1433)
    - Pour l'administrateur de la base de données du système, sélectionnez une des options suivantes :
        - (4) authentification Windows (elle utilise le nom d'utilisateur employé pour exécuter le programme d'installation)
        - (5) authentification SQL Server et entrez le mot de passe de l'utilisateur sa.



Authentification Windows

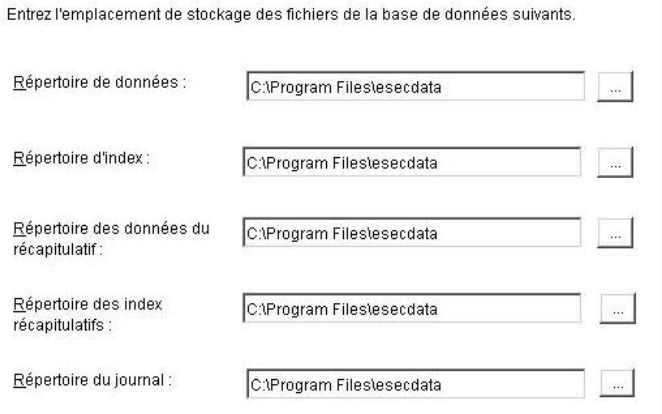


Authentification SQL Server

14. Entrez l'emplacement des fichiers de la base de données suivants :

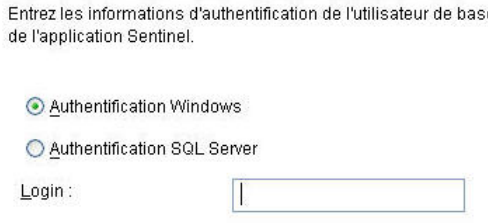
REMARQUE : à des fins de récupération et de performance, nous recommandons que ces emplacements soient dans des périphériques E/S différents.

- fichiers de données
- fichiers d'index
- fichiers de données récapitulatifs
- fichiers d'index récapitulatifs
- fichiers journaux



15. Entrez la taille de la base de données :
    - standard (20 000Mo) – capacité de 30 jours avec 500 000 événements par jour
    - grande (400 000Mo) – capacité de 30 jours avec 10 000 000 évènements par jour
    - personnalisée (indiquez la taille manuellement). Si vous sélectionnez cette option, une invite vous demande :
      (1) la taille de la base de données en Mo (10 000 – 2 000 000)
      (2) la taille de chaque fichier journal en Mo (100 – 100 000)
      (3) la taille maximum de chaque fichier de la base de données en Mo (2 000 – 100 000)
16. Pour l'administrateur de la base de données Sentinel (DBA), sélectionnez une des options suivantes :
    - authentification SQL Server (esecdba), mot de passe et mot de passe de confirmation
    - authentification Windows, entrez <nom_domaine>\<nom_utilisateur>

REMARQUE : si vous avez sélectionné *Authentification SQL Server*, vous ne pouvez pas modifier le nom de login par défaut.



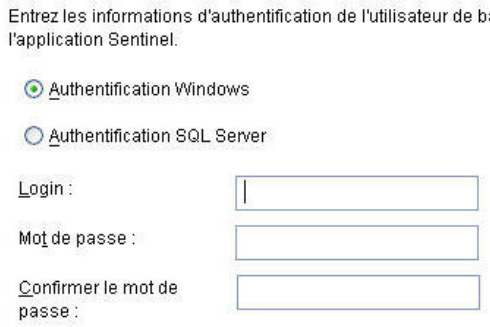
Authentification Windows

Authentification SQL Server

REMARQUE : pour l'authentification SQL, le programme d'installation ne continue que si le mot de passe esecdba correspond au mot de passe esecdba de v4.2.

17. Pour l'utilisateur de la base de données de l'application Sentinel : Sélectionnez une des options suivantes :
    - *authentification SQL Server* (esecapp), entrez le mot de passe et mot de passe de confirmation
    - *authentification Windows*, entrez <nom_domaine>\<nom_utilisateur>, le mot de passe et le mot de passe de confirmation

REMARQUE : si vous sélectionnez *Authentification SQL Server*, vous ne pouvez pas modifier le nom de login par défaut.



Authentification Windows

Authentification SQL Server

18. Pour l'utilisateur de l'administrateur Sentinel : Sélectionnez une des options suivantes :
    - *Authentification SQL*, entrez le nom d'utilisateur pour l'administrateur Sentinel (par défaut : esecadm), le mot de passe et le mot de passe de confirmation
    - *authentification Windows*, entrez <nom_domaine>\<nom_utilisateur>

REMARQUE : si vous sélectionnez *Authentification SQL Server*, vous ne pouvez pas modifier le nom de login par défaut.

Authentification Windows

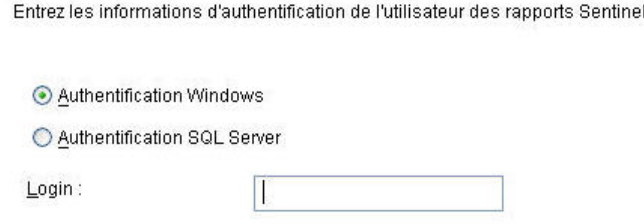
Authentification SQL Server

19. Pour l'utilisateur de création de rapport Sentinel. Sélectionnez une des options suivantes :

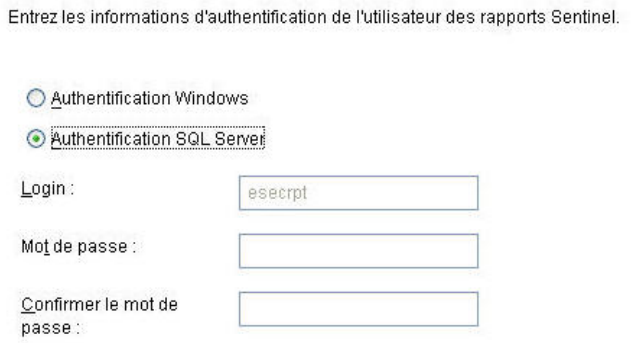
REMARQUE : pour la création de rapport Sentinel, l'authentification Windows requiert l'exécution de Crystal Enterprise Professional. Ce logiciel vous permet de créer différents comptes et assignations selon les besoins. Si vous utilisez Standard, sélectionnez *Authentification SQL*.

- authentification SQL (esecrpt), entrez le mot de passe et le mot de passe de confirmation
- *authentification Windows*, entrez <nom_domaine>\<nom_utilisateur>

REMARQUE : si vous sélectionnez *Authentification SQL Server*, vous ne pouvez pas modifier le nom de login par défaut.



Authentification Windows



Authentification SQL Server

20. Cliquez sur *Suivant* dans la fenêtre récapitulative de l'installation de la base de données.
21. Une fois l'installation terminée, une invite vous demande de redémarrer. Cliquez sur *Terminer* pour redémarrer le système.

Migration

L'utilitaire de migration de données ne fait migrer que les éléments suivants :

- les utilisateurs et les autorisations assignées
- les filtres
- les options de configuration de menu contextuel
- les balises CV renommées
- les configurations de partition et d'archives
- les cas de la version 4.2 sont copiés sur la version 5 comme incidents
- les incidents et les évènements liés aux incidents

REMARQUE : l'utilitaire de migration de données NE fait PAS migrer les données d'évènement, à l'exception des données d'évènements liés aux incidents. Seules les données d'évènements liés aux incidents sont migrées.

REMARQUE : les données d'évènements d'incidents ne peuvent pas s'afficher au moyen de Sentinel Control Center. Les données d'évènements d'incidents peuvent être vues à l'aide des rapports Crystal ou des requêtes SQL.

Migration de données pour la base de données Sentinel 5, lorsque l'administrateur de la base de données Sentinel est l'utilisateur d'authentification Windows.

REMARQUE : cette procédure est destinée aux installations de la base de données Sentinel 5 lorsque l'administrateur de la base de données Sentinel (équivalent à esecdba) est un utilisateur d'authentification Windows. Cette procédure ajoute un utilisateur d'authentification SQL esecdba à la base de données Sentinel 5, afin que les données puissent être migrées vers la version v5.

1. Loguez-vous comme utilisateur doté de droits administratifs.
2. Démarrez l'analyseur de requêtes MS SQL Server. Loguez-vous comme utilisateur sa ou comme utilisateur équivalent à l'authentification Windows.
3. Cliquez sur *Fichier* > *Ouvrir*. Naviguez vers :

   ```
   %ESEC_HOME%\utilities\db\scripts\ddl\mssql\Migration
   ```

4. Sélectionnez import_add_esecdba.sql.
5. Cliquez sur *Ouvrir*.
6. Cliquez sur *Interroger* > *Exécuter*.
7. Quant le script est terminé, quittez l'analyseur de requêtes.

REMARQUE : après l'exécution de la migration de données, vous pouvez utilisez MS SQL Server Enterprise Manager pour supprimer cet utilisateur d'authentification SQL esecdba de la base de données Sentinel 5.

Migration de données

1. Loguez-vous comme utilisateur doté de droits administratifs.
2. Vérifiez les variables d'environnement pour vous assurer que java (version 1.4.2) est dans le CHEMIN. Vous pouvez le vérifier en exécutant la commande suivante sur la ligne de commande :

   ```
   java -version
   ```

   Si cette commande ne marche pas, localisez dans le système l'emplacement où java est installé ou téléchargez et installez java. Puis mettez à jour la variable d'environnement PATH afin d'inclure la version exécutable de java. Par exemple, si java est installé dans le répertoire :

   ```
   C:\Program Files\sentinel5.1.3.0\Sun-1.4.2
   ```

   Ajoutez ensuite les éléments suivants au début de la variable d'environnement PATH :

   ```
   C:\Program Files\sentinel5.1.3.0\Sun-1.4.2\bin;
   ```

3. À l'invite de commande, cd vers le répertoire suivant sur le CD d'installation du logiciel Sentinel 5 :

   ```
   sentinel\dbsetup\bin
   ```

4. Exécutez la commande :

   ```
   .\MigrateDb.bat
   ```

5. Un invite vous demande les éléments suivants :
   - nom d'hôte de la base de données (où les bases de donnés Sentinel 4.2 et Sentinel 5 sont exécutées)
   - nom de la base de données cible (de la base de données Sentinel 5 vers laquelle vous migrez)
   - mot de passe esecdba (le mot de passe doit correspondre à l'utilisateur esecdba sur les bases de données Sentinel v4.2 et v5
   - nom de la base de données source, (nom de la base de données v4.2)
   - répertoire du journal (où les fichiers journaux de migration de données sont placés)

- option de migration :
  - (1) paramètres du système
  - (2) Incidents/cas
  - (3) les deux
  - (4) terminé

REMARQUE : les paramètres du système devont être migrés avec succès avant de passer à la migration des incidents et des cas.

REMARQUE : si la migration des paramètres du système échoue, désinstallez la base de données Sentinel 5 en sélectionnant l'option *Supprimer seulement les objets de la base de données*. Puis, réinstallez la base de données Sentinel 5 en sélectionnant l'option *Ajouter les objets de la base de données à une base de données vide existante*. Finalement, réessayez de suivre les instructions de migration de données.

REMARQUE : si la migration d'incidents échoue, re-exécutez la migration d'incidents. L'utilitaire de migration redémarre à partir du point d'échec. Aucune tâche de nettoyage supplémentaire n'est requise.

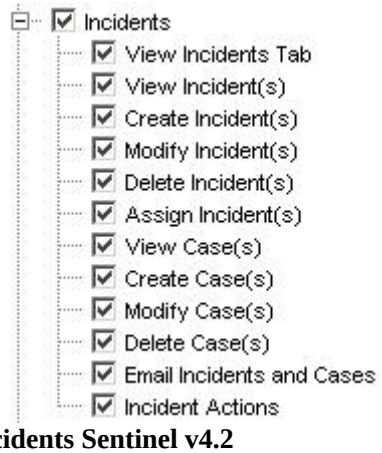
REMARQUE : après l'exécution de la migration de données, vous pouvez utilisez MS SQL Server Enterprise Manager pour supprimer l'utilisateur d'authentification SQL esecdba de la base de données Sentinel 5, si vous voulez l'ajouter à l'utilitaire de migration de données.

Post-migration – Installation de Sentinel 5

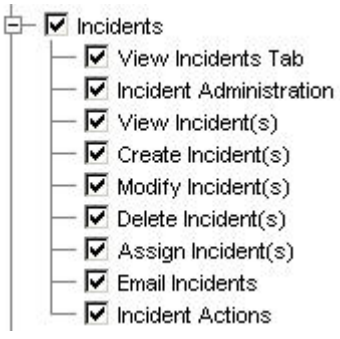
Dans le Sentinel 5, les fonctions suivantes sont nouvelles, différentes ou retirées.

- iTRAC – une nouvelle fonctionnalité. Les autorisations d'utilisateur associées sont :

- incidents – administration des incidents ajoutés toute fonctionnalité liée à la casse retirée. Les autorisations d'utilisateur associées sont :



Incidents Sentinel v4.2



Incidents Sentinel v5

- gestion de collecteurs – dans la v4.2 , c'est la surveillance de l'assistant. L'onglet *Affichage assistants* est remplacé par *Affichage collecteurs*. *Contrôler assistants et collecteur* est remplacé par *Contrôler collecteurs* et *Administration de collecteurs.* Les autorisations d'utilisateur associées sont :

Surveillance Wizard Sentinel v4.2

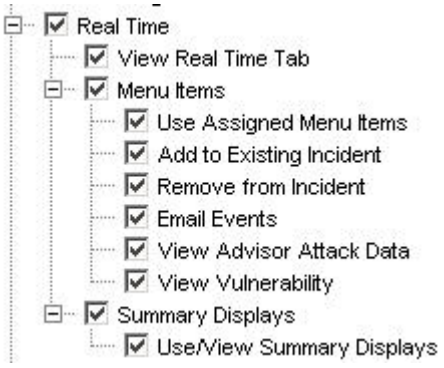
Gestion de collecteurs Sentinel v5

- administration – ajout de statistiques DAS, gestion de session d'utilisateur et gestion de rôle iTRAC Les *Règles de corrélation* ont été renommées *Corrélation*. La fonction Configuration d'évènements a été déplacée vers le gestionnaire de données Sentinel. La *Configuration d'utilisateur* a été renommée *Gestion d'utilisateur*. Les autorisations d'utilisateur associées sont :

Administration Sentinel v4.2

Administration Sentinel v5

- ActiveViews™ – dans la v4.2, la fonction s'appelait Temps Réel. *les Écrans récapitulatifs* ont été renommés *Vues Actives*. Les autorisations d'utilisateur associées sont :



Temps réel Sentinel v4.2

Active Views™ Sentinel v5

- la fonctionnalité de présentation du système n'est pas disponible sous Sentinel 5.

Installation de Sentinel 5

1. Installez Sentinel 5, voir le chapitre *Installation de Sentinel sous Windows*.
2. Installez le Sentinel Service Pack le plus récent.
3. Effectuez les étapes suivantes si vous voulez ajouter une nouvelle fonctionnalité à l'un des utilisateurs existants de la v4.2 :
   a. Assurez-vous que le *serveur Sentinel* est en exécution.
   b. Loguez-vous au Sentinel Control Center comme un utilisateur doté d'autorisation Administration/Gestion d'utilisateurs (par ex. esecadm).
   c. Dans Sentinel Control Center, cliquez sur l'onglet Admin. Agrandissez la configuration d'utilisateurs dans le volet de navigation ou depuis la barre de navigation cliquez *Admin* > *Configuration de l'utilisateur*.
   d. Cliquez avec le bouton droit sur l'utilisateur auquel vous voulez ajouter la fonctionnalité (par ex. esecadm) et sélectionnez *Détails de l'utilisateur*. Cliquez sur l'onglet *Autorisations*.
   e. Agrandissez iTRAC et assignez les autorisations selon les besoins.
   f. Agrandissez *Incidents* et assignez *Administration d'incidents* selon les besoins.
   g. Agrandissez *Gestion de collecteurs* et assignez *Administration de collecteurs* selon les besoins.
   h. Agrandissez *Administration* et assignez *Statistiques DAS, Gestion de session d'utilisateur* ou *Gestion de rôle iTRAC* selon les besoins.
   i. Cliquez sur l'onglet *Rôles* et assignez *Admin* ou *Rôle du processus de travail de l'analyste* selon les besoins.
   j. Cliquez sur *OK*.
4. Le cas échéant, importez les règles de corrélation. Les ensembles de règles exportés de Sentinel 4.2 sont affichés comme Dossiers de règles lors de leur importation dans Sentinel 5.
5. Copiez à partir de la sauvegarde des scripts de collecteurs et des configurations de ports, en suivant les instructions de la section Post-migration – Reconfiguration des scripts de collecteurs et des configurations de ports.

Post-migration – Reconfiguration des scripts de collecteurs et des configurations de ports

Sur chaque machine où le service de collecteurs (gestionnaire de collecteurs) Sentinel 5 est installé, effectuez les étapes suivantes pour rétablir les scripts de collecteurs et les configurations de ports utilisées dans l'installation de Sentinel v4.2.

Pour rétablir les scripts de collecteurs et les configurations de ports

1. Arrêtez le service Windows gestionnaire de collecteurs.
2. Depuis l'emplacement où vous avez placé la copie de sauvegarde du répertoire %WORKBENCH_HOME%\Agents de l'installation Sentinel 4.2, copiez les fichiers suivants dans le répertoire %WORKBENCH_HOME%\Agents de l'installation actuelle Sentinel 5 (écrasez les fichiers, si nécessaire) :
   - localhost_portcfg.dat
   - localhost_snmpcfg.dat
3. Lisez le fichier de texte créé pendant la pré-migration qui liste tous les collecteurs utilisés par l'installation du gestionnaire de collecteurs Sentinel v.4.2 sur cette machine. Vous devez connaître les noms de collecteurs pour l'étape suivante.
4. Depuis l'emplacement où vous avez placé la copie de sauvegarde du répertoire %WORKBENCH_HOME%\Elements de l'installation Sentinel 4.2, copiez les répertoires dont les noms correspondent aux noms des collecteurs dans le fichier de texte dans le répertoire %WORKBENCH_HOME%\Elements de l'installation actuelle Sentinel 5 (écrasez les fichiers, si nécessaire).
5. Procurez-vous l'utilitaire UpgradePortCfgFilesur le site Web du support technique Sentinel (téléchargez ici).
6. Extrayez le fichier ZIP UpgradePortCfgFile.
7. Ouvrez une invite de commande et passez les répertoires dans le répertoire de l'utilitaire UpgradePortCfgFile extrait. Depuis ce répertoire, exécutez la commande :

   ```
   .\UpgradePortCfgFile.bat
   ```

8. Démarrez le service *Gestionnaire de collecteurs*.

Post-migration – Configuration de Sentinel 5 pour la création de rapport Crystal

Si vous exécutez la création de rapport Crystal pour Sentinel 4.2 et si vous voulez exécuter la création de rapport Crystal pour Sentinel 5, vous devez :

- modifier les paramètres ODBC liés à la création de rapport Crystal pour cibler la base de données Sentinel 5.
- importer les modèles de Crystal Report (y compris les modèles de migration de données) depuis le Service Pack le plus récent.

Voir le chapitre sur *Crystal Reports*, pour plus d'informations.

Correctifs de v5.x.x à v5.1.3

Effectuez cette procédure sur une machine où des composants Sentinel sont installés.

Correctif Sentinel de v5.x.x à v5.1.3 lorsque l'administrateur de la base de données Sentinel (esecdba) est un login d'authentification SQL Server

Mise à niveau de v5.x.x vers v5.1.3 pour l'authentification SQL Server

REMARQUE : Si vous exécutez v5.1.1sp1 ou des versions supérieures et que vous avez fait des modifications sur le fichier syslog.conf, vous devez faire une copie du fichier syslog.conf. Le programme d'installation du correctif écrase le fichier syslog.conf. Après la correction, modifiez ou écrasez le nouveau fichier syslog.conf pour qu'il corresponde au fichier syslog.conf original.

1. Fermez tous les *Sentinel Control Centers, gestionnaires de données et générateurs de collecteurs Sentinel* ouverts.
2. Insérez le CD d'installation de correctif Sentinel dans l'unité de CD-ROM.
3. Naviguez vers le répertoire de correctifs adéquat.
4. Double-cliquez sur *setup.bat* dans le répertoire du correctif.

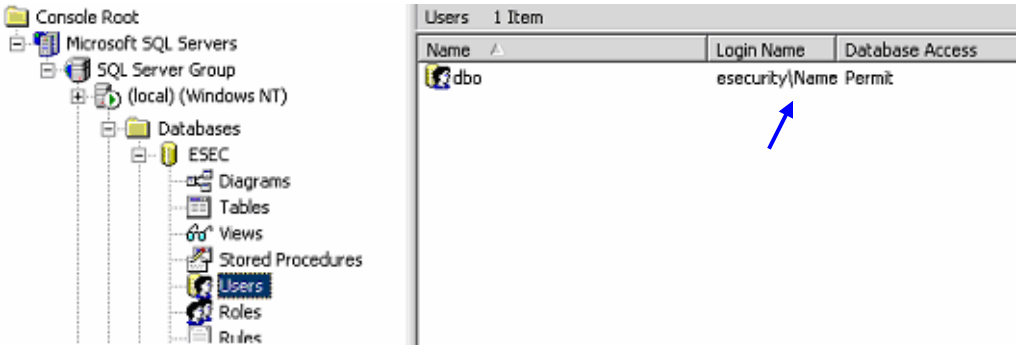
REMARQUE : l'installation en mode de console n'est actuellement pas prise en charge sous Windows.

5. Cliquez *Suivant* sur l'écran d'accueil.
6. Acceptez l'accord de licence utilisateur final et cliquez sur *Suivant*.
7. Cliquez sur *Suivant* jusqu'à la fenêtre d'informations de bases de données.
8. Veillez à ce que le type de base de données soit correct. Sélectionnez l'emplacement du répertoire de journal d'installation de bases de données. Cliquez sur *Suivant*.
9. Veillez à ce que les informations concernant MS SQL Server soient correctes. Sélectionnez *l'authentification SQL Server* Entrez le mot de passe du nom d'utilisateur esecdba. Cliquez sur *Suivant*.
10. Cliquez sur *Installer*. Un invite peut vous demander de redémarrer la machine. Dans le cas contraire, redémarrez les services Sentinel *(gestionnaire de collecteurs, Sentinel et communications Sentinel)*.

Correctif Sentinel de v5.x.x vers v5.1.3 lorsque l'administrateur de la base de données Sentinel est d'authentification Windows

Pour l'authentification Windows, le correctif InstallShield n'est pas appliqué au correctif de la base de données. Le programme d'installation du correctif de base de données doit être exécuté comme utilisateur du domaine Windows esecdba pour la base de données Sentinel.

Lorsque vous exécutez le programme d'installation du correctif sur la machine où vous avez initialement installé le composant de la base de données, vous devez connaître le nom d'utilisateur et le mot de passe de l'utilisateur de l'administrateur de la base de données Sentinel (esecdba). Vous pouvez découvrir l'utilisateur esecdba en cherchant le nom de login pour l'utilisateur dbo de la base de données Sentinel, à l'aide de SQL Server Enterprise Manager, comme illustré ci-dessous.



Pendant le processus de correction, vous recevez un message contextuel déclarant que le correctif de la base de données doit être effectué via la ligne de commande, comme expliqué ci-dessous.Correction de v5.x.x vers v5.1.3 pour Authentification Windows

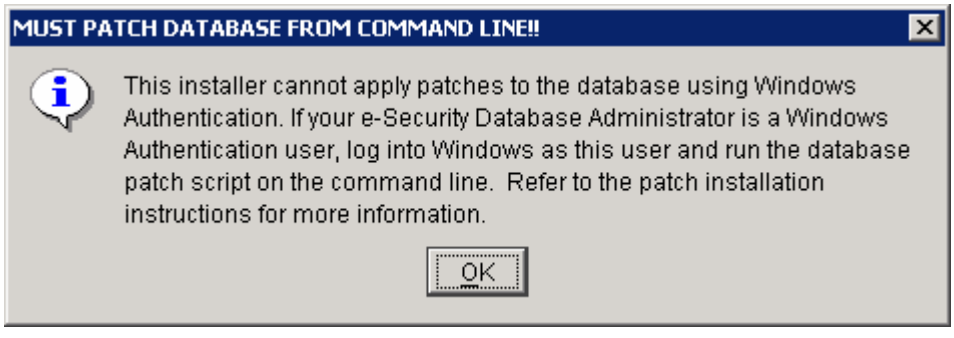
REMARQUE : Si vous exécutez v5.1.1sp1 ou des versions supérieures et que vous avez fait des modifications sur le fichier syslog.conf, vous devez faire une copie du fichier syslog.conf. Le programme d'installation du correctif écrase le fichier syslog.conf. Après la correction, modifiez ou écrasez le nouveau fichier syslog.conf pour qu'il corresponde au fichier syslog.conf original.

1. Fermez tous les *Sentinel Control Centers, gestionnaires de données et générateurs de collecteurs Sentinel ouverts*.
2. Insérez le CD d'installation de correctif Sentinel sur l'unité de CD-ROM.
3. Naviguez vers le répertoire de correctifs adéquat.
4. Double-cliquez sur *setup.bat* dans le répertoire du correctif.

REMARQUE : l'installation en mode de console n'est actuellement pas prise en charge sous Windows.

5. Cliquez *Suivant* sur l'écran d'accueil.
6. Acceptez l'accord de licence utilisateur final et cliquez sur *Suivant*.
7. Cliquez sur *Suivant* jusqu'à la fenêtre d'informations de bases de données.
8. Veillez à ce que le type et le nom de la base de données soient corrects. Sélectionnez l'emplacement du répertoire de journal d'installation de bases de données. Cliquez sur *Suivant*.

   Vous recevez le message contextuel suivant. Lisez le message et puis cliquez sur *OK* pour continuer.



9. Veillez à ce que les informations concernant MS SQL Server soient correctes. Sélectionnez *Authentification Windows*. Entrez le mot de passe de votre nom d'utilisateur pour l'utilisateur de l'application Sentinel. Cliquez sur *Suivant*.

   ATTENTION : Pour la machine de la base de données, NE REDÉMARREZ PAS À LA FIN DE L'INSTALLATION.

10. Dans la fenêtre récapitulative cliquez *Installer*.
11. Sur la machine de la base de données, sans redémarrer, quittez InstallShield.
12. Sur la machine de la base de données, loguez-vous comme utilisateur de l'administrateur du domaine Windows esecdba, si vous ne l'avez pas encore fait.
13. Ouvrez une invite de commande.
14. Vérifiez les variables d'environnement pour vous assurer que java (version 1.4.2) est dans le CHEMIN. Vous pouvez le vérifier en exécutant la commande suivante sur la ligne de commande :

    ```
    java -version
    ```

    Si cette commande n'aboutit pas, localisez dans le système l'emplacement où java est installé ou téléchargez et installez java. Puis mettez à jour la variable d'environnement PATH, afin d'inclure la version exécutable de java. Par exemple, si java est installé dans le répertoire :

    ```
    C:\Program Files\sentinel5.1.3.0\Sun-1.4.2
    ```

    Ajoutez ensuite les éléments suivants au début de la variable d'environnement PATH :

    ```
    C:\Program Files\sentinel5.1.3.0\Sun-1.4.2\bin;
    ```

15. À l'invite de commande, passez les répertoires dans le répertoire suivant sur le CD d'installation Sentinel :

    ```
    <Patch Directory>\sentinel\dbsetup\bin
    ```

16. Entrez la commande :

    ```
    .\PatchDb.bat
    ```

17. À l'invite, entrez le nom d'hôte ou l'adresse IP statique de SQL Server de la base de données Sentinel que vous voulez corriger.
18. À l'invite, entrez le nom de la base de données Sentinel de SQL Server que vous voulez corriger.
19. À l'invite, entrez l'option 1 pour l'authentification Windows. Le script vérifie toutes les informations entrées et commence la correction de la base de données.
20. Après que le script a fini d'appliquer le correctif, redémarrez les services.

Mise à jour du connecteur Syslog

Si vous utilisez les scripts du connecteur syslog d'une version Sentinel antérieure à 5.1.1.1 (par ex. 5.0, 5.0.1.0, 5.1.0.0 ou 5.1.1.0), vous devez commencer à utiliser les scripts du connecteur syslog mis à jour qui sont inclus dans le correctif. Afin de passer de l'utilisation de l'ancien script du connecteur syslog à celle des nouveaux scripts du connecteur syslog, déplacez l'ancien script et installez un nouveau script.

Le connecteur syslog est installé avec des scripts qui sont exécutés sous Windows et UNIX avec des fichiers de configuration améliorés. En outre, l'installation du serveur proxy syslog comme service a été simplifiée.

Pour déplacer le connecteur Syslog

1. Loguez-vous comme Administrateur.
2. cd d/ %ESEC_HOME%\wizard\/syslog
3. Entrez :

```
.\syslog-server.bat remove
```

Pour installer le connecteur Syslog

1. Loguez-vous comme Administrateur.
2. cd d/ %ESEC_HOME\wizard\syslog
3. .\syslog-server.bat install
4. Si vous avez fait des modifications sur le fichier syslog.conf de l'installation originale, vous devez modifier ou écraser le nouveau fichier syslog.conf afin de refléter le fichier syslog.conf original. syslog.conf est localisé à :

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

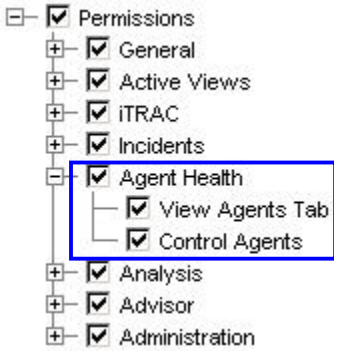
Mise à jour des autorisations d'utilisateur de v5.0.x vers v5.1.3

Lors de la mise à jour de v5 ou v5.0.1 à v5.1.3, l'état de santé des collecteurs est remplacée par la gestion de collecteurs, avec une fonctionnalité supplémentaire d'administration de collecteurs. La fonctionnalité Vues de serveurs a aussi été ajoutée. Vous pouvez optionnellement donner cette autorisation.

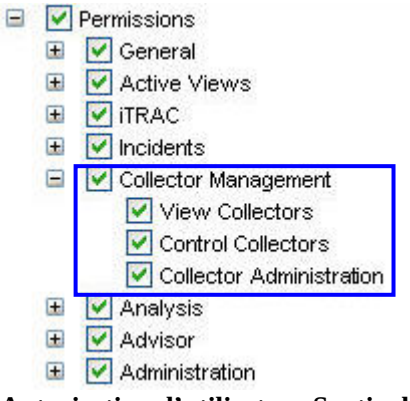
Mise à jour des autorisation de gestion d'utilisateurs

1. Loguez-vous au Sentinel Control Center comme un utilisateur doté d'autorisation Administration/Gestion d'utilisateurs.

   Dans la v5.1, l'état de santé des collecteurs sous Autorisations est passé de l'*Etat de santé des collecteurs* à la *Gestion de collecteurs* avec une autorisation supplémentaire ajoutée.



Autorisation d'utilisateur Sentinel v5.0



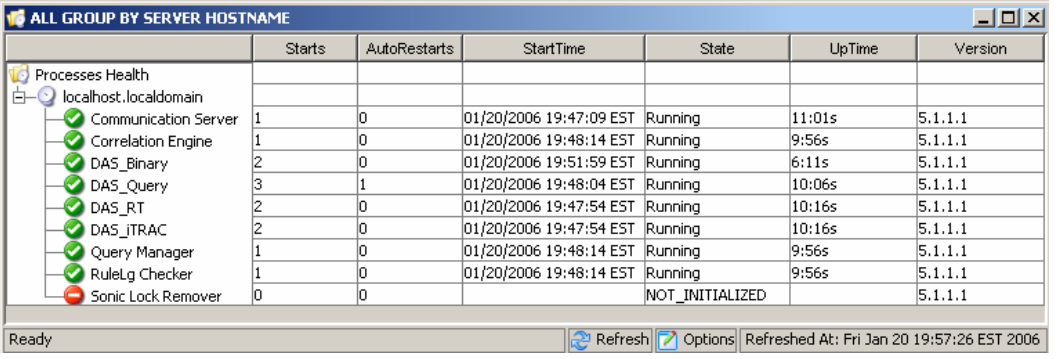
Autorisation d'utilisateur Sentinel v5.1

2. Dans Sentinel Control Center, cliquez sur l'onglet *Admin*. Agrandissez Configuration d'utilisateurs dans le volet de navigation ou depuis la barre de navigation cliquez *Admin* > *Configuration de l'utilisateur*.

3. Cliquez avec le bouton droit sur un utilisateur Admin (c.-à-d. esecadm ou tout autre utilisateur admin) > *Détails de l'utilisateur*. Cliquez sur l'onglet *Autorisations*.
4. Agrandissez *Gestion de collecteurs* et assignez *Administration de collecteurs*. Cliquez sur *OK*.

Mise à jour des autorisations de vues de serveur

Afin d'utiliser l'écran Vue de serveur après l'installation du correctif, vous devez donner l'autorisation *Vues de serveur* à l'utilisateur Sentinel, à l'aide du gestionnaire d'utilisateurs. Le gestionnaire d'utilisateurs est localisé sous l'onglet *Admin* de Sentinel Control Center.



Serveur de création de rapport Crystal

Après la mise à niveau vers Sentinel 5.1.3, y compris l'application du Service Pack le plus récent, vous devez importer les rapports du Service Pack le plus récent. Pour plus d'informations, voir le chapitre sur Crystal Reports dans le guide d'installation.

Mise à jour du courrier électronique Sentinel pour l'authentification SMTP

Si le système requiert une authentification SMTP, vous devez mettre à jour le fichier execution.properties. Ce fichier est sur la machine où le DAS est installé. Il est localisé à %$ESEC_HOME%/sentinel/config. Pour configurer ce fichier, exécutez mailconfig.bat afin de changer le fichier et mailconfigtest.bat afin de tester ces changements.

Pour configurer le fichier execution.properties.

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfig de la façon suivante :

   ```
   mailconfig.bat -host <serveur SMTP> -de <adresse
      électronique source> -utilisateur <utilisateur
      authentification courrier électronique> –mot de passe
   ```

   Exemple :

   ```
   mailconfig.bat -host 10.0.1.14 -from nom@domaine.com -
      user nom_utilisateur –password
   ```

   Après cette commande, une invite vous demande d'entrer un nouveau mot de passe.

```
Entrez le mot de passe : *********
Confirmez le mot de passe : *********
```

REMARQUE : lors de l'utilisation de l'option de mot de passe, ce doit être le dernier argument.

Pour tester la configuration d'execution.properties

1. Sur la machine où le DAS est installé, cd vers :

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

2. Exécutez mailconfigtest de la façon suivante :

   ```
   mailconfigtest.bat -to <adresse électronique cible>
   ```

   Si l'envoi du message électronique a abouti, vous obtenez le résultat suivant sur l'écran et le message est reçu à l'adresse cible.

   ```
   Message électronique envoyé avec succès !
   ```

   Vérifiez la boîte aux lettres de l'adresse cible pour confirmer la réception du message. La ligne d'objet et le contenu devraient être les suivants :

   ```
   Objet : Test des propriétés du courrier électronique
      Sentinel

   Test de configuration des propriétés du courrier
      électronique Sentinel. Si ce message apparaît, les
      propriétés du courrier électronique Sentinel ont été
      correctement configurées pour envoyer des messages.
   ```

8 Correctif pour Oracle sous Linux

REMARQUE : le terme « agent » est échangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Ce chapitre traite des correctifs de v5.1.1.1 à v5.1.3

Correctif de v5.1.1.1 à v5.1.3

Effectuez cette procédure sur une machine où des composants Sentinel sont installés.

Si vous êtes en train d'exécuter le programme d'installation du correctif où vous avez initialement installé le composant de la base de données, vous devez connaître le mot de passe de l'utilisateur de l'administrateur de la base de données Sentinel (esecdba).

Mise à niveau de v5.1.1.1 à v5.1.3 pour Linux

1. Loguez-vous comme utilisateur root.

   REMARQUE : Si vous avez fait des modifications sur le fichier syslog.conf dans l'installation v5.1.1.1, vous devez faire une copie du fichier syslog.conf. Le programme d'installation du correctif écrase le fichier syslog.conf. Après la correction, modifiez ou écrasez le nouveau fichier syslog.conf pour qu'il corresponde au fichier syslog.conf original.

2. Insérez et montez le CD Correctif de Sentinel.
3. Démarrez le programme d'installation en allant au répertoire du correctif adéquat sur le CD-ROM et en exécutant la commande suivante :

   En mode GUI :

   ```
   ./setup.sh
   ```

   ou

   En mode texte (« headless ») :

   ```
   ./setup.sh –console
   ```

4. Cliquez *Suivant* sur l'écran d'accueil.
5. Acceptez l'accord de licence utilisateur final et cliquez sur *Suivant*.
6. Cliquez sur *Suivant* jusqu'à la fenêtre d'informations de bases de données.
7. Veillez à ce que le type de base de données soit correct. Sélectionnez l'emplacement du répertoire de journal d'installation de bases de données. Cliquez sur *Suivant.*
8. Veillez à ce que les informations concernant le serveur Oracle soient correctes. Entrez le mot de passe de esecdba. Suivez les invites restantes du programme d'installation

Mise à jour du connecteur Syslog

Si vous utilisez les scripts du connecteur syslog d'une version Sentinel antérieure à 5.1.1.1 (par ex. 5.0, 5.0.1.0, 5.1.0.0 ou 5.1.1.0), vous devez commencer à utiliser les scripts du connecteur syslog mis à jour qui sont inclus dans le correctif. Afin de passer de l'utilisation de l'ancien script du connecteur syslog à celle des nouveaux scripts du connecteur syslog, déplacez l'ancien script et installez un nouveau script.

Le connecteur syslog est installé avec des scripts qui sont exécutés sous Windows et UNIX avec des fichiers de configuration améliorés. En outre, l'installation du serveur proxy syslog comme service a été simplifiée.

Pour déplacer le connecteur Syslog

1. Loguez-vous comme utilisateur root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

Pour installer le connecteur Syslog

1. Loguez-vous comme utilisateur root.
2. cd $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh install
4. Si vous avez fait des modifications sur le fichier syslog.conf de l'installation originale, vous devez modifier ou écraser le nouveau fichier syslog.conf afin de refléter le fichier syslog.conf original. syslog.conf est localisé à :

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

Serveur de création de rapport Crystal

Après la mise à niveau à Sentinel 5.1.3, y compris l'application du Service Pack le plus récent (le cas échéant), vous devez importer les rapports du Service Pack le plus récent. Pour plus d'informations, voir le chapitre sur Crystal Reports dans le guide d'installation.

Mise à jour du courrier électronique Sentinel pour l'authentification SMTP

Si le système requiert une authentification SMTP, vous devez mettre à jour le fichier execution.properties. Ce fichier est sur la machine où le DAS est installé. Il est localisé à $ESEC_HOME/sentinel/config. Pour configurer ce fichier, exécutez mailconfig.sh afin de changer le fichier et mailconfigtest.sh afin de tester ces changements.

Pour configurer le fichier execution.properties.

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfig de la façon suivante :

   ```
   ./mailconfig.sh -host <serveur SMTP> -from
      <adresse électronique source> -user <utilisateur
      authentification courrier électronique> –password
   ```

Exemple :

```
./mailconfig.sh -host 192.0.2.14 -from nom@domaine.com
   -user nom_utilisateur –password
```

Après cette commande, une invite vous demande d'entrer un nouveau mot de passe.

```
Entrez le mot de passe : *********
Confirmez le mot de passe : *********
```

REMARQUE : lors de l'utilisation de l'option de mot de passe, ce doit être le dernier argument.

Pour tester la configuration d'execution.properties

1. Sur la machine où le DAS est installé, loguez-vous comme esecadm et cd vers :

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

2. Exécutez mailconfigtest de la façon suivante :

   ```
   ./mailconfigtest.sh -to <adresse électronique cible>
   ```

   Si l'envoi du message électronique a abouti, vous obtenez le résultat suivant sur l'écran et le message est reçu à l'adresse cible.

   ```
   Message électronique envoyé avec succès !
   ```

   Vérifiez la boîte aux lettres de l'adresse cible pour confirmer la réception du message. La ligne d'objet et le contenu devraient être les suivants :

   ```
   Objet : Test des propriétés du courrier électronique
      Sentinel

   Test de configuration des propriétés du courrier
      électronique Sentinel. Si ce message apparaît, les
      propriétés du courrier électronique Sentinel ont été
      correctement configurées pour envoyer des messages.
   ```

9 Crystal Reports pour Windows et Solaris

REMARQUE : le terme « agent » est échangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

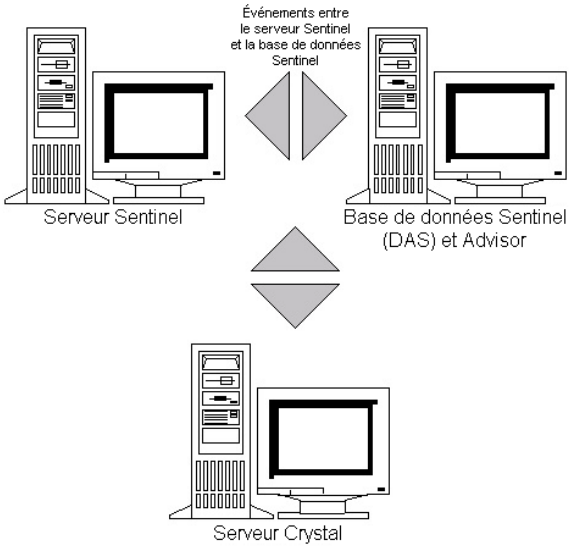
Crystal BusinessObjects Enterprise™ 11 est un outil de création de rapport.

Ce chapitre traite de la configuration de l'installation de Crystal Reports Server pour Sentinel. L'installation devrait être faite dans l'ordre indiqué ci-dessous :

- installer Microsoft IIS et ASP.NET
- installer MS SQL (en fonction de la configuration comme authentification Windows ou authentification MS SQL Server)
- installer Crystal Server
  - configurer ODBC (Open Database Connectivity) pour l'authentification SQL

  ou

  - Installation et configuration du logiciel Oracle 9i Client
- configurer inetmgr
- correctif Crystal Reports
- publication (importation) de Crystal Reports
- configuration du compte « utilisateur nommé »
- test de la connectivité serveur Web
- activation du Top 10 des rapports (facultative)
- maximisation de la création de rapport d'évènements (recommandée)
- configuration de Sentinel pour Crystal Enterprise Server



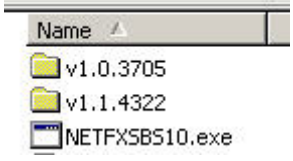
Présentation

Crystal Reports Server requiert une base de données pour stocker les informations concernant le système et ses utilisateurs. Cette base de données est connue comme base de données CMS (Central Management Server). CMS est un serveur qui stocke les informations concernant le système de Crystal Reports Server. D'autres composants Crystal Reports Server peuvent accéder à ces informations, le cas échéant.

La base de données CMS doit être configurée sur une base de données de MS SQL 2000 Server local. Le programme d'installation de Crystal Reports Server vous permet de configurer la base de données CMS sur une base de données MSDE, si un serveur local MS SQL 2000 Server n'est pas installé. Sentinel 5 ne prend pas en charge de configuration MSDE.

Configuration système requise

- Windows® 2003 Server avec SP1 avec une partition formatée NTFS avec IIS (Microsoft Internet Information Server) et NET.ASP installés Sentinel 5 ne prend pas en charge Crystal XI sur Windows® 2000 Server.
- .NET Framework 1.1 (installée par défaut sur Windows 2003. BusinessObjects Enterprise™ 11 ne prend pas en charge.NET Framework 2.0). Pour savoir quelle version de .NET Framework est sur la machine, allez à %SystemRoot%\Microsoft.NET\Framework. Le dossier numérique le plus élevé ne devrait pas être supérieur à v.1.1.xxxx. Par exemple :

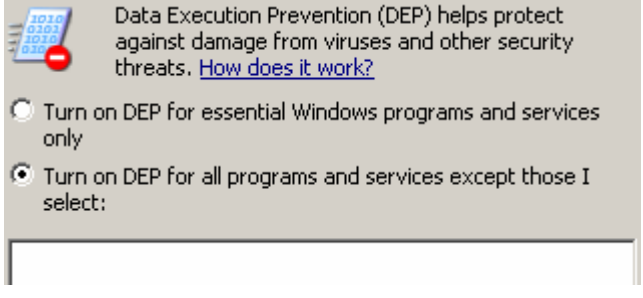


Configuration requise

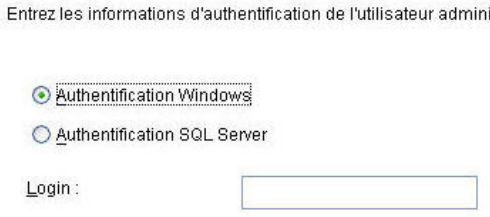
1. Assurez-vous que le compte utilisé pour installer Crystal Reports Server a les droits d'administrateurs locaux.
2. Configurez DEP (Data Execution Prevention) pour l'exécution dans les programmes et services sélectionnés. C'est notamment utile pour éviter l'« erreur 1920. Service « Crystal Report Cache Server » sous Windows 2003 ».

   Pour accéder à DEP, sélectionnez Panneau de configuration > Système > onglet Avancés > Paramètres de performance > Prévention d'exécution des données (DEP – Data Execution Prevention).

   Sélectionnez Activer DEP pour tous les programmes et services sauf ceux sélectionnés.



3. Si vous voulez exécuter les rapports Sentinel à l'aide de l'authentification Windows NT, vérifiez que le compte de domaine Windows pour les rapports Sentinel existe déjà dans la base de données Sentinel. Cela est fait pendant l'installation Sentinel en sélectionnant l'authentification Windows, lors de la configuration de la *méthode d'authentification pour l'utilisateur des rapports Sentinel*, comme illustré ci-dessous.



4. Si vous voulez exécuter les rapports Sentinel à l'aide de l'authentification SQL Server (également requis pour les installations Sentinel Oracle), vérifiez que le login de SQL Server (esecrpt) existe déjà dans la base de données Sentinel.
   - Pour la base de données Sentinel MS SQL, cela est fait pendant l'installation Sentinel pour MS SQL, en sélectionnant l'*authentification SQL Server* lors de la configuration de la *Méthode d'authentification pour l'utilisateur de Sentinel Report*, comme illustré ci-dessous.

   - Pour la base de données Sentinel Oracle, cela est fait pendant l'installation de Sentinel pour Oracle ; esecrpt assume le même mot de passe que esecadm.
5. Pour Oracle - Oracle 9i Client Release 2 (9.2.0.1.0), installez-le avant d'installer Crystal BusinessObjects Enterprise™ 11.
6. Pour MS SQL Server, installez MS SQL 2000 sp3a avant d'installer Crystal Reports Server 11.
7. Résolution vidéo de 1 024 x 768 ou supérieure
8. Installez Microsoft Internet Information Server (IIS) et ASP.NET

REMARQUE : Sentinel 5 ne prend pas en charge MSDE. Installez MS SQL 2000 sp3a avant d'installer Crystal Reports Server 11.

Installation de Microsoft Internet Information Server (IIS) et d'ASP.NET

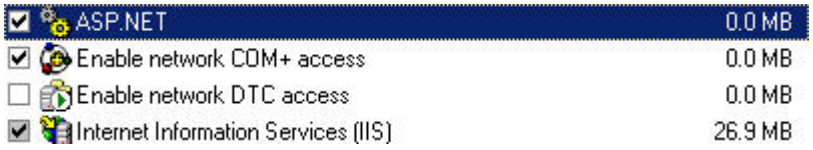
Pour ajouter les composants Windows, le CD d'installation de Windows 2003 Server peut s'avérer nécessaire.

Installation IIS et ASP.NET

1. Sous Windows, allez au *Panneau de configuration > Ajouter/déplacer programmes*

2. Sur le panneau vertical gauche, cliquez sur *Ajouter/déplacer composants Windows*.
3. Sélectionnez *Serveur d'applications*.

4. Cliquez sur *Détails*.
5. Sélectionnez *ASP.NET et Internet Information Server (IIS)*.



6. Cliquez sur *OK*.

Cliquez sur *Suivant*. Une invite vous demande le CD d'installation Windows.

Cliquez sur *Terminer*.

Problèmes connus

1. Installation de Crystal Reports. Deux clés sont délivrées, une pour Crystal Reports Server et l'autre pour Crystal Reports Developer. Vérifiez que vous utilisez bien la clé de Crystal Reports Server, lors de l'installation de Crystal Reports Server.
2. Désinstallation de Crystal Reports : en cas de désinstallation de Crystal Reports Server, il existe une procédure de désinstallation manuelle qui nettoie les clés d'enregistrement, ce qui est particulièrement utile lorsque l'installation est endommagée. Allez sur le site Web de BusinessObjects suivant pour connaître les procédures de désinstallation manuelle de BusinessObjects Enterprise XI, http://support.businessobjects.com/library/kbase/articles/c2017905.asp.

   REMARQUE : l'URL ci-dessus était correct lors de la publication de ce document.
3. Pendant la configuration de .NET Administration Launchpad, lorsque le niveau d'accès est changé de *Droits hérités* vers *Affichage à la demande*, le processus de mise à jour est bloqué. Attendez environ 30 secondes. Le niveau d'accès est mis à jour.

Utilisation de Crystal Reports

Pour plus d'informations concernant l'utilisation de Crystal Reports pour la création de rapport Sentinel, voir la Documentation sur Crystal Reports et le guide d'utilisateur Sentinel.

Présentation de l'installation

Présentation de l'installation pour MS SQL 2000 Server avec l'authentification Windows

Pour installer correctement Crystal Reports, effectuez les tâches suivantes dansl'ordre indiqué ci-dessous.

1. Installez Crystal Reports Server 11: lors de l'installation de l'application Sentinel 5, si vous sélectionnez l'*authentification Windows* pour l'utilisateur des rapports

Sentinel, suivez le lien vers l'Installation de Crystal Server pour MS SQL 2000 Server avec l'authentification Windows.

2. Configurer ODBC (Open Database Connectivity)
3. Assigner Crystal Reports pour l'utilisation avec Sentinel
4. Correctifs Crystal Reports
5. Publier rapports
6. Configurer l'utilisateur comme compte d'utilisateur nommé
7. Importer les modèles Crystal Reports
8. Créer une page Web Crystal (Configurer .NET Administration Launchpad)
9. Configurer Sentinel pour Crystal Enterprise Server

Présentation de l'installation pour MS SQL 2000 Server avec l'authentification SQL Server

Pour installer correctement Crystal Reports, effectuez les tâches suivantes dans l'ordre indiqué ci-dessous.

1. Installez Crystal Reports Server 11 : lors de l'installation de l'application Sentinel 5, si vous sélectionnez l'*authentification SQL Server* pour l'utilisateur des rapports Sentinel, suivez le lien vers l'Installation de Crystal Server pour MS SQL 2000 Server avec l'authentification SQL ou pour Oracle.
2. Configurer ODBC (Open Database Connectivity)
3. Assigner Crystal Reports pour l'utilisation avec Sentinel
4. Importer les modèles Crystal Reports
5. Créer une page Web Crystal (Configurer .NET Administration Launchpad)
6. Configurer Sentinel pour Crystal Enterprise Server

Présentation de l'installation pour Oracle

Pour installer correctement Crystal Reports, effectuez les tâches suivantes dans l'ordre indiqué.

1. Installer Oracle 9i Client
2. Installer Crystal Reports Server 11 : suivez le lien vers l'Installation de Crystal Server pour MS SQL 2000 Server avec l'authentification SQL ou pour Oracle.
3. Configure Oracle native driver
4. Assigner Crystal Reports pour l'utilisation avec Sentinel
5. Importer les modèles Crystal Reports
6. Créer une page Web Crystal (Configurer .NET Administration Launchpad)
7. Configurer Sentinel pour Crystal Enterprise Server

Installation

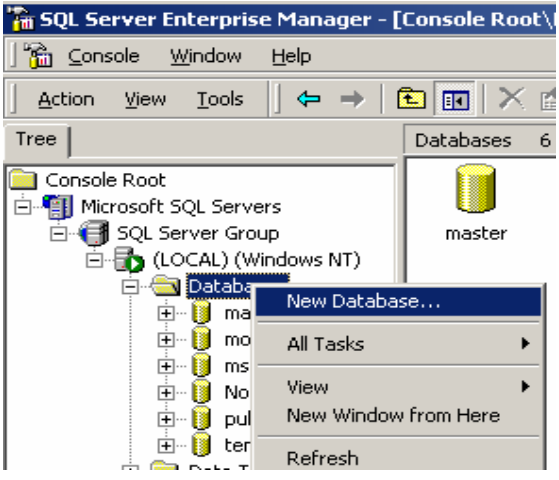
Cette section explique comment installer Crystal Server pour :

- base de données Sentinel pour MS SQL 2000 Server avec l'authentification Windows
- base de données Sentinel MS SQL 2000 Server avec l'authentification SQL Server
- base de données Sentinel Oracle

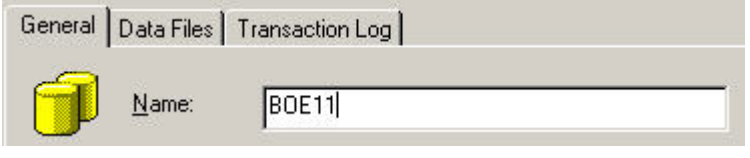
Installation de Crystal Server pour MS SQL 2000 Server avec l'authentification Windows

Installation de l'authentification Windows de Crystal Server BOE XI

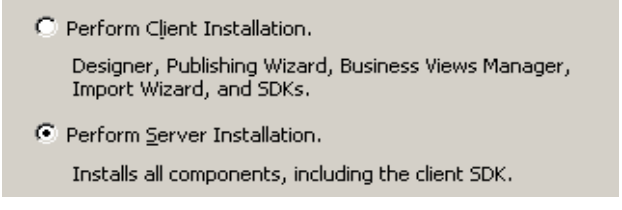
1. Installez MS SQL 2000 sp3a en mode mixte.
2. Lancez MS SQL Enterprise Manager.
3. Sur le panneau de navigation, agrandissez (local)(Windows NT).
4. Mettez en surbrillance et cliquez droit sur *Base de données* et sélectionnez *Nouvelle base de données*…



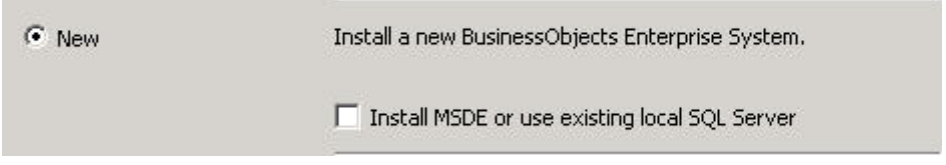
5. Sous l'onglet Général, dans le champ Nom entrez « BOE11 » et cliquez sur *OK*.



6. Quittez MS SQL Enterprise Manager.
7. Insérez le CD Crystal Server BOE XI dans l'unité de CD-ROM.
8. Si le lancement automatique est inactif sur la machine, exécutez *setup.exe*.
9. Dans la fenêtre Sélectionner l'installation de client ou de serveur, sélectionnez *Effectuer l'installation du serveur*.

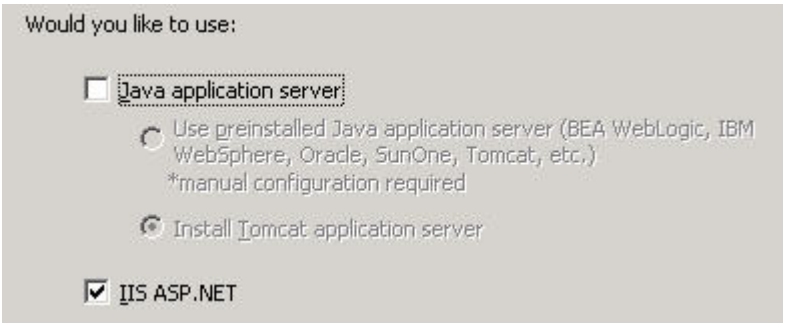


10. Pour le type d'installation, sélectionnez *Nouveau* et ne sélectionnez pas *Installer MSDE ou utiliser SQL Server local existant*.

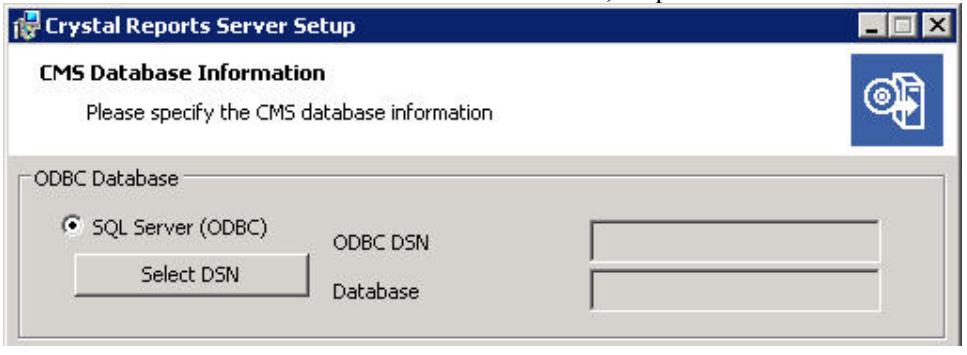


11. Dans la fenêtre Type d'adaptateur au composant Web, sélectionnez *IIS ASP.NET*.

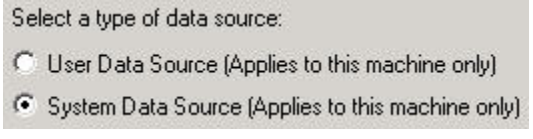
REMARQUE : si vous n'avez pas installé IIS et ASP.NET à partir du *Panneau de configuration* > *Ajouter/déplacer programmes* > *Ajouter/déplacer composants Windows*, IIS et ASP.NET sont affichés en gris.



12. Sur la fenêtre Informations de bases de données CMS, cliquez sur *Sélectionner DSN*.

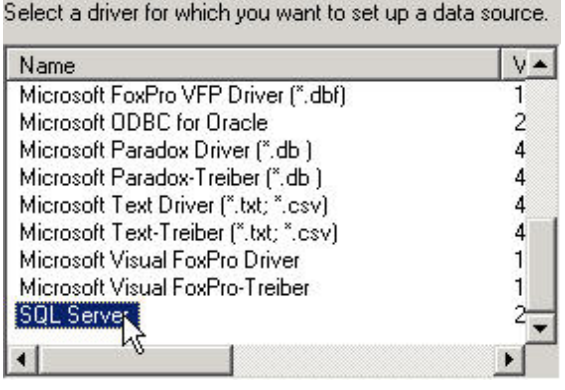


13. Cliquez sur l'onglet *Source de données de la machine*.
14. Cliquez sur *Nouveau…*.
15. Sélectionnez Source de données du système.

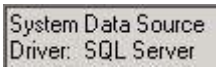


Cliquez sur Suivant.

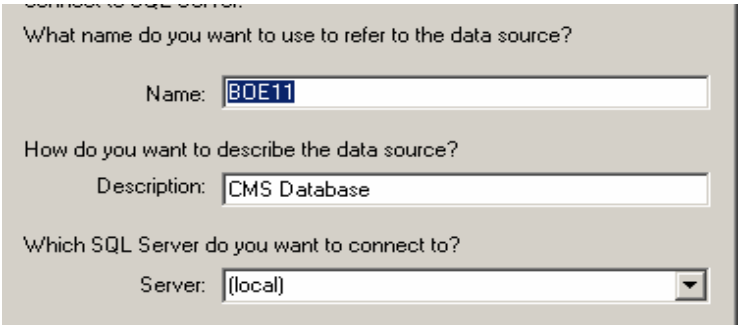
16. Défilez vers le bas pour sélectionner *SQL Server*, puis cliquez sur *Suivant*.



17. Une nouvelle source s'affiche, cliquez sur *Terminer*.

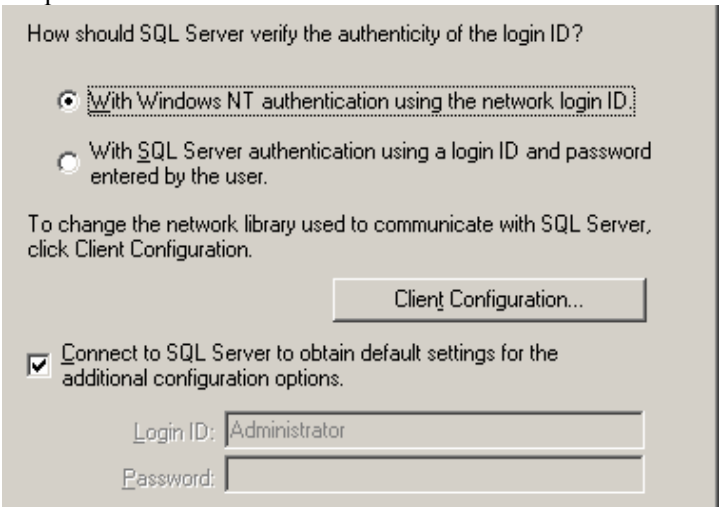


18. Dans la fenêtre *…nouvelle source de données pour SQL Server*, entrez :
    - nom de la source de données (par ex : BOE_XI)
    - description (facultative)
    - Pour le serveur, cliquez sur la flèche bas et sélectionnez (*local)*.



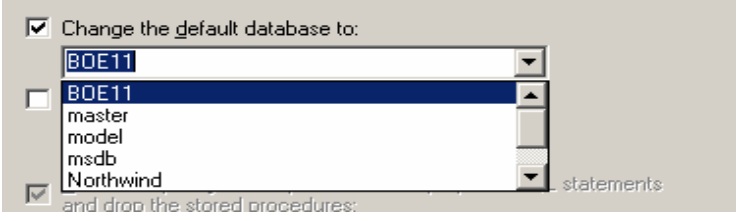
Cliquez sur *Suivant*.

19. Sélectionnez *Avec Windows NT…*, si ce n'est pas encore sélectionné. Cliquez sur *Suivant*.



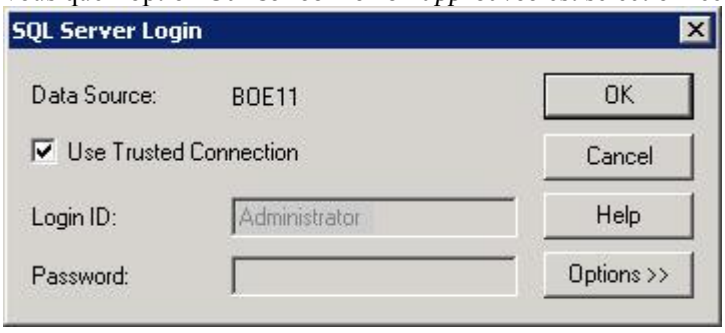
REMARQUE : l'ID de login (en gris) correspond à votre nom de login Windows.

20. Cochez la case *Remplacer la base de données par défaut par :* . Remplacer la base de données par défaut par *BOE11*. Cliquez sur *Suivant*.



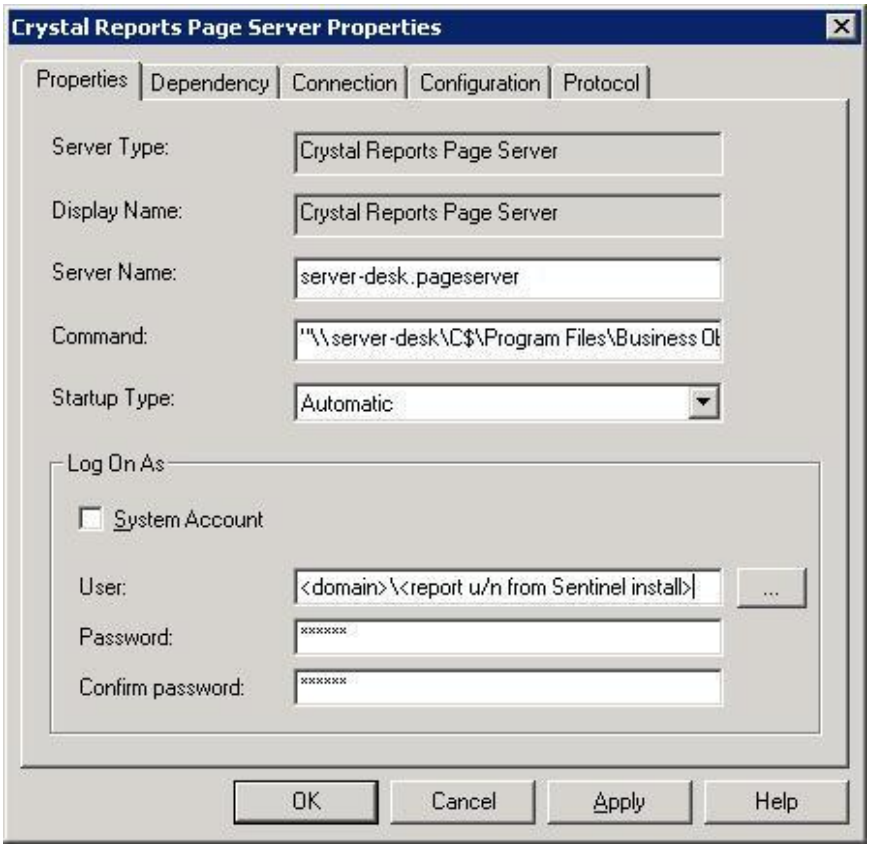
21. Dans la fenêtre *Créer une nouvelle source de données pour SQL Server*, cliquez sur *Terminer*.

22. Cliquez sur *Tester source de données*. Cela devrait réussir. Cliquez sur *OK*.
23. Dans la fenêtre Sélectionner une source de données, sélectionnez *BOE11* et cliquez sur *OK* successivement, jusqu'à ce que vous obteniez le *Login SQL Server*. Assurez-vous que l'option *Utiliser connexion approuvée* est sélectionnée. Cliquez sur *OK*.



REMARQUE : l'ID de login (en gris) correspond à votre nom de login Windows.

24. Dans la fenêtre Avertissement, cliquez sur *OK*.
25. Dans la fenêtre *Informations de bases de données CMS*, cliquez sur *Suivant*.
26. Cliquez sur *Suivant* pour continuer l'installation.
27. Après l'installation, vous devez remplacer le compte de consignation Crystal Reports Page Server et de Crystal Reports Job Server par le compte de domaine d'utilisateur de Sentinel Report.
    a. Cliquez *Démarrer > Programmes > BusinessObjects 11 > Crystal Reports Server> Central Configuration Manager*.
    b. Cliquez avec le bouton droit sur *Crystal Reports Page Server* et sélectionnez *Arrêter*.
    c. Cliquez de nouveau avec le bouton droit sur C*rystal Reports Page Server* et sélectionnez *Propriétés*.
    d. Supprimez la coche *Se loguez comme compte du système* et entrez le nom et mot de passe du compte de domaine de l'utilisateur de Sentinel Report utilisés pour l'utilisateur de Sentinel Report, lors de l'installation Sentinel 5. Cliquez sur *OK*.



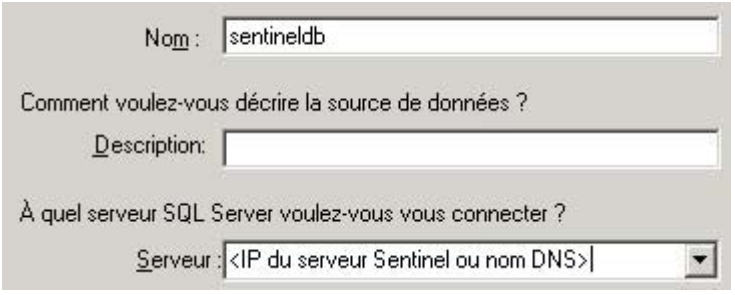
e. Sélectionnez Crystal Reports Page Server et cliquez avec le bouton droit pour démarrer Crystal Reports Page Server.

Configuration ODBC (Open Database Connectivity) pour l'authentification Windows

Cette procédure configure une source de données ODBC entre Crystal Reports sous Windows et SQL.Server Elle doit être effectuée sur la machine de Crystal.Server

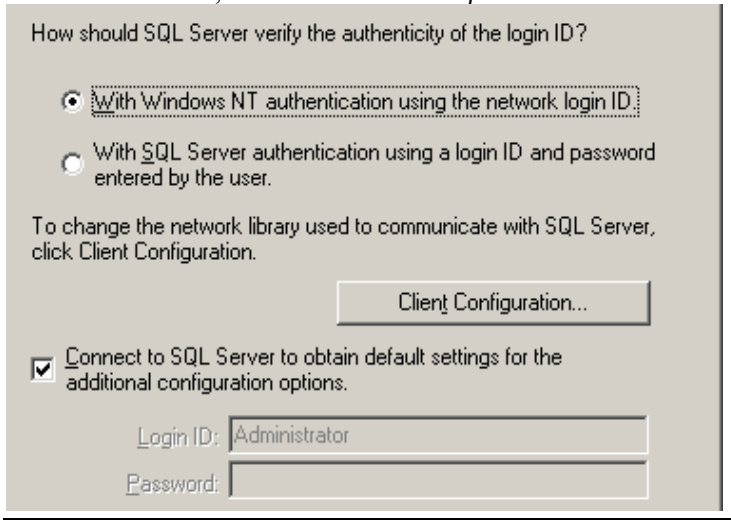
Configuration d'une source de données ODBC pour Windows

1. Sous Windows, allez au Panneau de configuration > Outils administratifs> Sources de données (ODBC)
2. Cliquez sur l'onglet *DSN du système* et cliquez sur *Ajouter*.
3. Sélectionnez *SQL Server*. Cliquez sur *Terminer*.
4. Un écran s'affiche demandant les informations de configuration de l'unité :
   - nom de source de données, entrez sentineldb
   - champ Description (facultatif), entrez une description
   - champ Serveur, entre le nom d'hôte ou l'adresse IP du serveur Sentinel



Cliquez sur *Suivant*.

5. Sur l'écran suivant, sélectionnez *Authentification Windows*.



REMARQUE : l'ID de login (en gris) correspond à votre nom de login Windows.

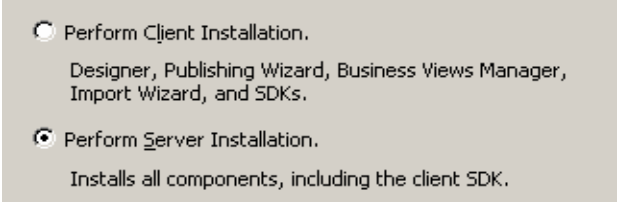
6. Sur l'écran suivant, sélectionnez :
   - Changer la base de données Sentinel (le nom par défaut est ESEC)
   - Laissez tous les paramètres par défaut

   Cliquez sur *Suivant*.
7. Cliquez sur *Terminer*.
8. Cliquez sur *Tester source de données…*. Vous devriez obtenir une connexion réussie. Cliquez sur *OK* jusqu'à la fermeture.

Installation de Crystal Server pour MS SQL 2000 Server avec l'authentification SQL

Installer Crystal Reports Server 11 avec les options suivantes sélectionnées.

- Effectuer l'installation du serveur

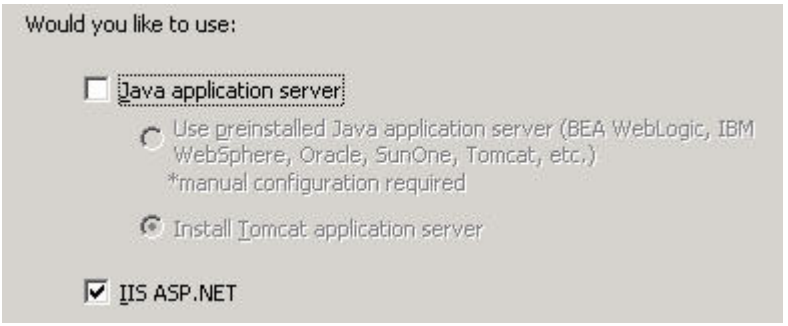


- Installer un nouveau système BusinessObjects Enterprise avec « Installer MSDE ou utiliser le serveur SQL Server local existant ».

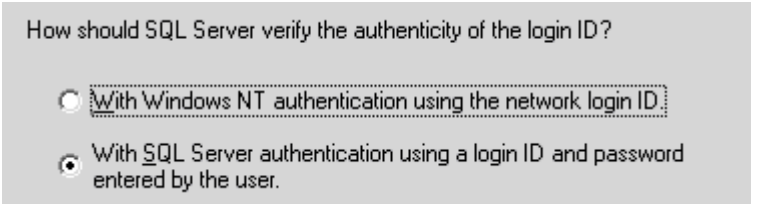
REMARQUE : les serveurs Crystal Server et MS SQL 2000 Server doivent se trouver sur la même machine.

- IIS ASP.NET

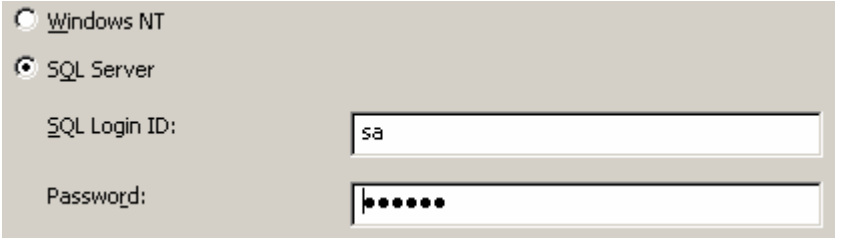
REMARQUE : si vous n'avez pas installé IIS et ASP.NET à partir du *Panneau de configuration > Ajouter/déplacer programmes > Ajouter/déplacer composants Windows*, IIS et ASP.NET sont affichés en gris.



- Une invite vous demande de spécifier le mode d'authentification. Sélectionnez *Authentification SQL Server.*



- Sélectionnez *Authentification SQL Server* Entrez un sa et un mot de passe sa.



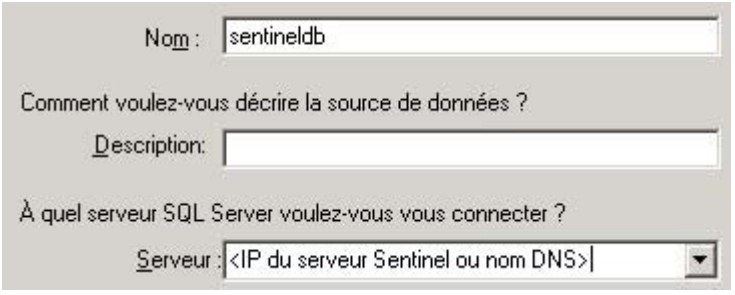
Configurer ODBC (Open Database Connectivity) pour l'authentification SQL

Cette procédure configure une source de données ODBC entre Crystal Reports sous Windows et SQL Server. This has to be performed on the Crystal Server machine.

Configuration d'une source de données ODBC pour Windows

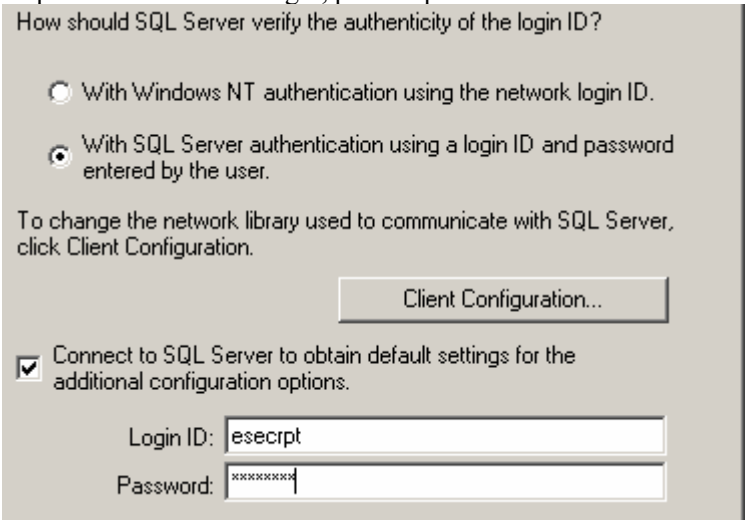
1. Sous Windows, allez au *Panneau de configuration > Outils administratifs> Sources de données (ODBC)*
2. Cliquez sur l'onglet *DSN du système* et cliquez sur *Ajouter*.
3. Sélectionnez *SQL Server*. Cliquez sur *Terminer*.

4. Un écran s'affiche demandant les informations de configuration de l'unité :
   - nom de source de données, entrez sentineldb
   - champ Description (facultatif), entrez une description
   - champ Serveur, entre le nom d'hôte ou l'adresse IP du serveur Sentinel



   Cliquez sur *Suivant*.

5. Sur l'écran suivant, sélectionnez *Authentification SQL*. Entrez esecrpt et le mot de passe comme ID de login, puis cliquez sur *Suivant*.



6. Sur l'écran suivant, sélectionnez :
   - Changer la base de données Sentinel (le nom par défaut est ESEC)
   - Laissez tous les paramètres par défaut

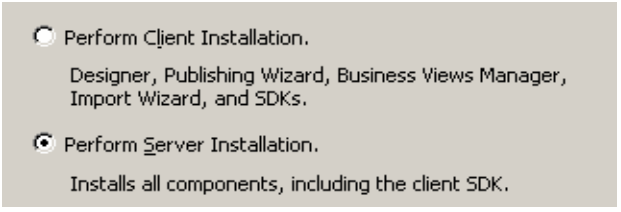
   Cliquez sur *Suivant*.

7. Cliquez sur *Terminer*.
8. Cliquez sur *Tester source de données…*. Vous devriez obtenir une connexion réussie. Cliquez sur *OK* jusqu'à la fermeture.

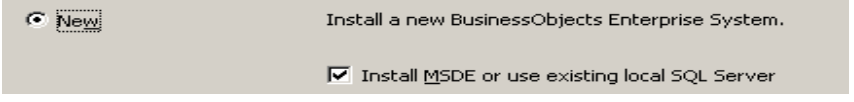
Installation de Crystal Server pour Oracle

Installer Crystal Reports Server 11 avec les options suivantes sélectionnées.

- Effectuer l'installation du serveur.



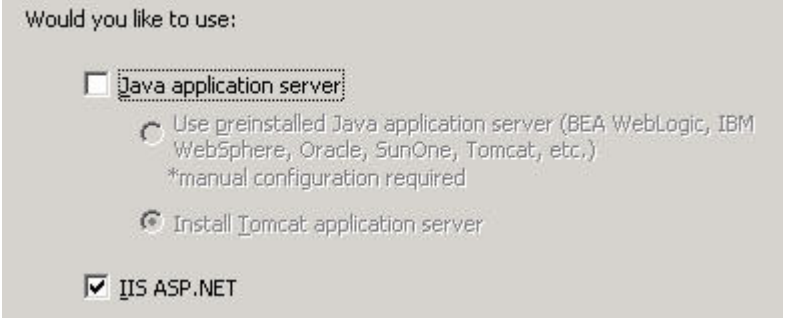
- Installer un nouveau système BusinessObjects Enterprise avec *Installer MSDE ou utiliser le serveur SQL Server local existant*.



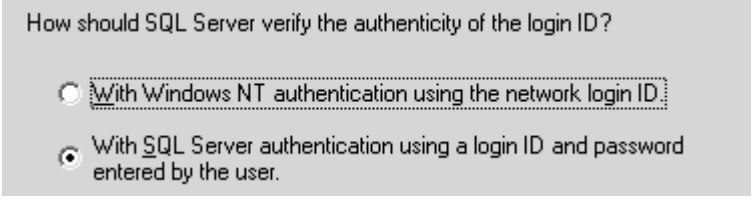
REMARQUE : les serveurs Crystal Server et MS SQL 2000 Server doivent se trouver sur la même machine.

- IIS ASP.NET

REMARQUE : si vous n'avez pas installé IIS et ASP.NET à partir du *Panneau de configuration > Ajouter/déplacer programmes > Ajouter/déplacer composants Windows*, IIS et ASP.NET sont affichés en gris.



- Une invite vous demande de spécifier le mode d'authentification. Sélectionnez *Authentification SQL Server.*



Crystal Reports ne prend pas en charge l'accès direct aux bases de données Oracle 9. Cette accessibilité est fournie par le fichier crdb_oracle.dll translation. Ce fichier communique avec l'unité de la base de données Oracle 9, qui travaille directement avec les bases de données et les clients Oracle et récupère les données nécessaires au rapport.

REMARQUE : afin que Crystal Reports puissent utiliser les bases de données Oracle 9, le logiciel client Oracle doit être installé sur le système et l'emplacement du client Oracle doit être inclus dans la variable d'environnement PATH.

Installation et configuration du logiciel Oracle 9i Client

Lors de l'installation d'Oracle 9i Client :

- acceptez l'emplacement d'installation par défaut
- non, pour effectuer des configurations types
- non – pour le service de répertoires
- Sélectionnez Local
- nom de service TNS : ESEC
- utilisateur (facultatif) : esecrpt

Après l'installation, créez une configuration du nom de service Net local.

Création de la configuration du nom de service Net (Configuration du pilote natif Oracle)

1. Sélectionnez *Oracle-OraHome92 >Outils de configuration et de migration > Net Manager*
2. Au panneau de navigation, agrandissez Local et sélectionnez Nommer services.
3. Cliquez sur le signe plus à gauche pour ajouter un Nom de service.
4. Dans la fenêtre Nom de service, entrez un nom de Net.Service.
   - Entrez SENTINELDB

   Cliquez sur *Suivant*.
5. Dans la fenêtre Sélectionner protocoles, sélectionnez par défaut :
   - TCP/IP (protocole Internet)

   Cliquez sur *Suivant*.
6. Pour le nom d'hôte et le numéro de port :
   - entrez le nom d'hôte ou l'adresse IP de la machine où se trouve la base de données.
   - sélectionnez le port Oracle (par défaut, 1521 lors de l'installation)

   Cliquez sur *Suivant*.
7. Pour identifier la base de données ou le service :
   - sélectionnez (*Oracle8i ou version ultérieure*), entrez votre nom de service (le nom de l'instance Oracle).
   - Pour le type de connexion, sélectionnez *Base de données par défaut*.

   Cliquez sur *Suivant*.
8. Dans la fenêtre *Test*, cliquez sur le bouton *Test…*. Cliquez sur *Suivant*. Le test peut échouer, s'il utilise un ID de base de données et un mot de passe.
9. Si le test échoue, effectuez les tâches suivantes :
   - Dans la fenêtre Connexion, cliquez sur *Changer Login*.
   - Entrez l'ID Sentinel Oracle (utilisateur esecrpt) et le mot de passe. Cliquez sur *OK*.

   Si le test échoue :

- Faites un ping du serveur Sentinel
- Vérifiez que le nom d'hôte du serveur Sentinel est inclus dans le fichier d'hôtes sur Crystal Reports Server. Le fichier d'hôtes est localisé sous %SystemRoot%\system32\drivers\etc\.

10. Cliquez sur *Terminer*.

Configuration pour toutes les authentifications et configurations

Assignation de Crystal Reports pour l'utilisation avec Sentinel

Les procédures suivantes sont requises pour que Crystal Server puisse travailler avec Sentinel Control Center.

Configuration inetmgr

inetmgr

1. Copier le fichier web.config à partir de :

   ```
   C:\Program Files\Business Objects\BusinessObjects
      Enterprise 11\Web Content
   ```

   pour c:\Inetpub\wwwroot.
2. Lancez le Internet Service Manager en cliquant sur *Démarrer* > *Exécuter*. Entrez *inetmgr* et cliquez sur *OK*.
3. *Agrandissez (ordinateur local)* > *Sites Web* > *Sites Web par défaut* > *businessobjects*.
4. Sur *businessobjects*, cliquez avec le bouton droit > *Propriétés*.
5. Sous l'onglet *Répertoire Virtuel*, cliquez sur le bouton *Configuration...*.
6. Vous devriez avoir les assignations suivantes : Sinon, ajoutez-lez. Si vous ajoutez une assignation, ne cliquez pas sur les nœuds *businessobjects* ou *crystalreportsviewer11*.

Extension	Exécutable
.csp	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cwr	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cri	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.wis	C:\Program Files\Business Objects\BusinessObjects Enterprise 11\win32_x86\cdzISAPI.dll

   Cliquez sur *OK* pour fermer la fenêtre.
7. Redémarrer IIS en agrandissant (ordinateur local) > *Sites Web* > *Sites Web par défaut*, sélectionnez *Sites Web par défaut* et cliquez avec le bouton droit >*Redémarrer*.

Correctifs de Crystal Reports pour l'utilisation avec Sentinel

Afin d'afficher Crystal Reports à partir de l'onglet Analyse de Sentinel Control Center, plusieurs fichiers Crystal Enterprise doivent être mis à jour pour les rendre compatibles avec le navigateur incorporé dans Sentinel.

Le tableau suivant énumère ces fichiers et décrit l'utilisation de chacun.

Nom du fichier	***Description***

`calendar.js`
 	
`calendar.html`
	Il affiche un calendrier contextuel lorsque vous sélectionnez une date comme paramètre d'un rapport.

`grouptree.html`	Il affiche le message Chargement… pendant le chargement des rapports.
`exportframe.html`	Il affiche la fenêtre qui vous permet d'exporter un rapport, afin de le sauvegarder ou de l'imprimer.
`exportIce.html`	Fichier utilisé par Sentinel lors de l'exportation d'un rapport, afin de le sauvegarder ou de l'imprimer.
`GetInfoStore.asp`	Fichier utilisé pour consulter Crystal Server.
`GetReports.asp`	Fichier utilisé par Sentinel Control Center pour établir une connexion avec Crystal Server et afficher la liste de rapports.
`GetReportURL.asp`	Fichier utilisé pour prendre en charge les liens hypertexte entre les rapports.
`helper_js.asp`	Un fichier d'appel utilisé par GetInfoStore.asp.

Correctifs de Crystal Reports

1. Sur le CD Sentinel Service Pack, allez à \content\reports\patch et copiez tous les fichiers *.html et *.js dans l'emplacement du fichier visualiseur, par défaut :

   ```
   C:\Program Files\Business Objects\BusinessObjects
      Enterprise 11\Web Content\Enterprise11\viewer\en
   ```

Sur le CD-ROM Sentinel Service Pack, allez à \content\reports\patch et copiez tous les fichiers *.asp et *.js pour :

```
C:\inetpub\wwwroot
```

REMARQUE : le dossier Web peut être placé sur une unité différente ou à un emplacement différent de celui mentionné ci-dessus.

Modèles Crystal Report

Les modèles Crystal Report sont publiés en utilisant Crystal Publishing Wizard.

Le dernier ensemble de modèles de rapports peut être téléchargé du portail client à http://esecurity.custhelp.com/.

REMARQUE : La liste d'attaques faite par le rapport CVE est une intersection de signatures d'attaques entre l'alimentation Advisor et les vulnérabilités analysées.

REMARQUE : pour exécuter un des rapports Top 10, certains résumés de regroupement doivent être activés et l'EventFileRedirectService (dans le processus DAS_Binary) doit également être actif. Pour obtenir des informations sur le mode d'activation des résumés de regroupement et l'EventFileRedirectService, consultez la section Activation de Sentinel Top 10 Reports.

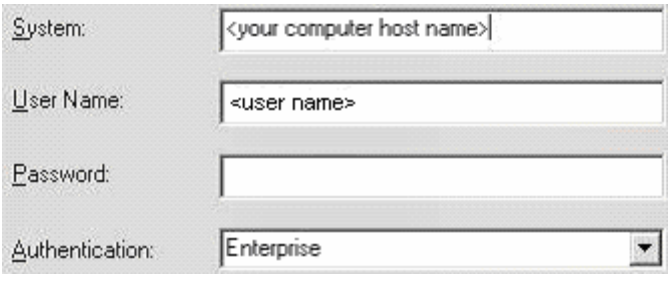
Publication des modèles de rapport à l'aide de Crystal Publishing Wizard

Publication des modèles Crystal Report

REMARQUE : si vous republiez les modèles de rapports, supprimez la dernière importation de modèles de rapports.

1. Cliquez Démarrer > Tous les programmes > BusinessObjects 11 > Crystal Reports Server > Publishing Wizard.
2. Cliquez sur *Suivant*.
3. Login. Système doit être le nom de l'ordinateur hôte et l'authentification doit être Entreprise. Le nom d'utilisateur peut être Administrateur. Pour des raisons de sécurité, il est vivement conseillé de créer un nouvel utilisateur au lieu d'utiliser Administrateur. Entrez votre mot de passe et cliquez sur *Suivant*.

REMARQUE : La publication des rapports sous l'administrateur d'utilisateurs permet à tous les utilisateurs d'avoir accès aux rapports.



4. Cliquez sur *Ajouter dossier*.
5. Sélectionnez *Inclure sous-dossier*. Sur le CD-ROM Sentinel Service Pack, naviguez vers :

   pour Crystal Reports (utilisateurs MS SQL) :

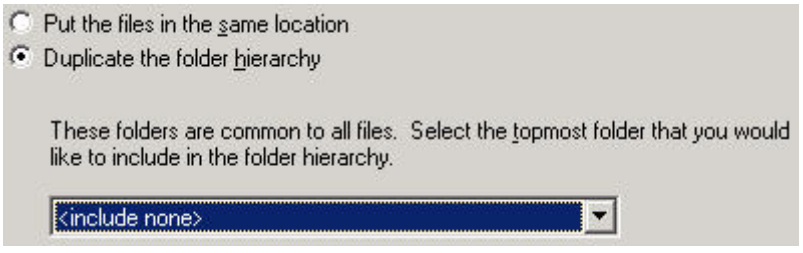
   ```
   \content\reports\Crystal_v11\SQL-Server
   ```

   Pour Crystal Reports (utilisateurs Oracle) :

   ```
   \content\reports\Crystal_v11\Oracle
   ```

   Cliquez sur *OK*.
6. Cliquez sur *Suivant*.
7. Sur la fenêtre Indiquer emplacement, cliquez sur *Nouveau dossier* (coin supérieur droit) et créez un dossier nommé *Rapports_Sentinel*. Cliquez sur *Suivant*.

8. Sélectionnez :
   - *Hiérarchie de dossiers dupliquée*.
   - Cliquez sur la flèche bas et sélectionnez <*inclure aucun*>.



   Cliquez sur *Suivant*.
9. Dans la fenêtre Confirmer emplacement, cliquez sur *Suivant*.
10. Dans la fenêtre Spécifiez Catégories :
    - un nom de catégorie au choix (comme sentinel)
    - sélectionner le nom, puis cliquez sur le bouton + (plus)

REMARQUE : seul le premier rapport apparaît sous la catégorie, après avoir cliqué sur Suivant.

    - cliquez sur *Suivant.*
11. Dans fenêtre Indiquer la planification, cliquez sur *Laisser les utilisateurs mettre à jour l'objet* (cette option doit être définie par défaut). Cliquez sur *Suivant*.
12. Dans la fenêtre Spécifier rafraîchissement de référentiel, cliquez *Activer* tout pour activer le rafraîchissement de référentiel. Cliquez sur *Suivant*.
13. Dans la fenêtre Spécifier sauvegarder données enregistrées, cliquez *Activer* tout pour sauvegarder les données enregistrées lors de la publication des rapports. Cliquez sur *Suivant*.
14. Dans la fenêtre Changer valeurs par défaut, cliquez sur *Publier rapports sans modifier les propriétés* (cette option doit être définie par défaut). Cliquez sur *Suivant*.
15. Cliquez sur *Suivant* pour ajouter les objets.
16. Cliquez sur *Suivant*.
17. Une liste publiée s'affiche, cliquez sur *Terminer*.

Quand les modèles Sentinel pour Crystal Reports sont publiés au Crystal Enterprise server, les modèles doivent se trouver dans le répertoire *Sentinel_Reports*.

Configurer un compte d'« utilisateur nommé »

La clé de licence fournie avec le serveur Crystal Server est une clé de compte d'« utilisateur nommé ». Le compte Guest doit être changé, « Utilisateur simultané » est remplacé par « Utilisateur nommé ».

Configuration du compte GUEST comme « Utilisateur nommé »

1. Cliquez *Démarrer* > *Tous les programmes* > *BusinessObjects 11* > *Crystal Reports Server*> *.NET Administration Launchpad.*
2. Cliquez sur *Central Management Console*.

Le nom du système devrait être le nom de l'ordinateur hôte. Le type d'authentification devrait être Enterprise. Dans le cas contraire, choisissez *Enterprise*.

Cliquez sur *Se loguer*.

3. Sur le panneau Organiser, cliquez sur *Utilisateurs*.
4. Cliquez sur *Guest*.
5. Changez le type de connexion en passant d'*Utilisateur simultané* à *Utilisateur nommé*.
6. Cliquez sur *Mettre à jour*.
7. Déloguez-vous et fermez la fenêtre ou avancez vers la section *Configuration de.NET Administration Launchpad*.

Configuration de .NET Administration Launchpad

Cette procédure traite du mode de configuration de .NET Administration Launchpad pour vous permettre de voir et de modifier les rapports.

Configureration de.NET Administration Launchpad

1. Démarrez .NET Administration Launchpad, si cela n'a pas encore été fait (Cliquez sur *Démarrer* > *Tous les programmes* > *BusinessObjects 11* > *Crystal Reports Server* > *.NET Administration Launchpad).*
2. Cliquez sur *Central Management Console*.

   Le nom du système devrait être le nom de l'ordinateur hôte. Le type d'authentification devrait être Enterprise. Dans le cas contraire, choisissez *Enterprise*.
3. Entrez votre nom d'utilisateur, votre mot de passe et cliquez sur *Se loguer*.
4. Sur le volet Organiser, cliquez sur *Dossiers*.
5. Cliquez une fois sur *Rapports_Sentinel*.
6. Sélectionnez *Tous*.
7. Cliquez sur l'onglet *Droits*.
8. Pour tout le monde, sur le menu déroulant à droite sous le Niveau d'accès sélectionnez *Affichage à la demande*. Cliquez sur *Mettre à jour*.

   REMARQUE : Pendant le changement du niveau d'accès où l'option *Droits hérités* est remplacée par *Affichage à la demande*, le processus de mise à jour est bloqué. Attendez environ 30 secondes. Le niveau d'accès est mis à jour.
9. Déloguez-vous et fermez la fenêtre.

Test de la connexion du serveur Web à la base de données

Test de la connexion du serveur Web à la base de données

1. Si cela n'a pas encore été fait, démarrez .NET Administration Launchpad, *(Démarrer > Tous les programmes > BusinessObjects 11 > Crystal Reports Server> .NET Administration Launchpad).*
2. Cliquez sur *Central Management Console*.
3. Entrez Administrateur comme nom d'utilisateur. Entrez votre mot de passe (par défaut, vide). Cliquez sur *Se loguer*.
4. Naviguer vers Dossiers publics > eSecurity_Reports > Évènements internes.
5. Sélectionnez Détails d'affichage de colonne.
6. Cliquez sur *Aperçu.*
7. En fonction du système, loguez-vous comme esecrpt ou comme utilisateur de Sentinel Report.
8. Sur le menu déroulant Trier les champs, sélectionnez *Balise*.
9. Cliquez sur *OK*. Un rapport devrait s'afficher.

Tester la connectivité serveur Web

Tester la connectivité serveur Web

1. Entrez sur une autre machine mais sur le même réseau que le serveur Web.
2. Entrez :

```
http://<nom DNS ou adresse IP de votre serveur Web >/
   businessobjects/enterprise11/WebTools/adminlaunch/
   default.aspx
```

Une page Web Crystal BusinessObjects devrait s'afficher.

Activation de Sentinel Top 10 des rapports

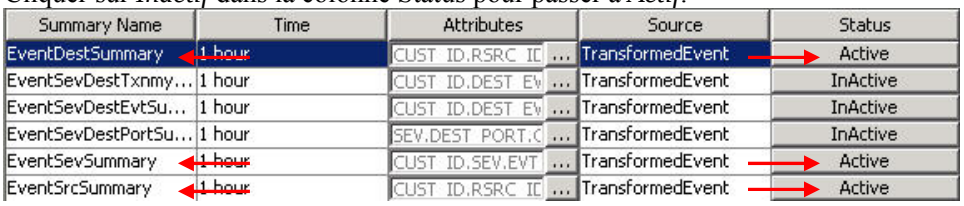
Pour activer Sentinel Top 10 Reports vous devez :

- activer Regroupement
- activer EventFileRedirectService

Activation de regroupement

1. Démarrer Sentinel Data Manager
2. Login.
3. Cliquez sur l'onglet Données de la création de rapport.
4. Activez les résumés suivants :
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

Cliquer sur *Inactif* dans la colonne Status pour passer à *Actif*.



Activation d'EventFileRedirestService

1. Sur la machine DAS, à l'aide de l'éditeur de texte, ouvrez :

   Pour UNIX :

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

   Pour Windows :

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

2. Pour EventFileRedirectService, transformez l'état en « actif ».

   ```
   <nom propriété="état">actif</propriété>
   ```

3. Redémarrez le composant DAS en suivant les instructions ci-dessous :

   Sous Windows :

   ```
   Utilisez le gestionnaire de services pour arrêter puis
      redémarrer le service « eSecurity ».
   ```

   Sur Solaris :

   ```
   $ESEC_HOME/sentinel/scripts/sentinel.sh stop

   Assurez-vous que tous les processus du serveur
      Sentinel sur cette machine se sont arrêtés à l'aide
      de la commande 'ps –ef | grep $ESEC_USER'.  S'il y
      a encore des processus du serveur Sentinel en
      exécution, détruisez-les à l'aide de la commande
      Détruire.

   $ESEC_HOME/sentinel/scripts/sentinel.sh start
   ```

Maximisation de la création de rapport d'évènements

En fonction du nombre d'évènements consultés par Crystal, vous pouvez obtenir un erreur sur la période maximale de traitement ou la limite maximale d'enregistrement. Pour configurer le serveur afin qu'il traite un nombre supérieur ou illimité de rapports, vous devez reconfigurer Crystal Page Server. Il y a deux méthodes pour le faire, à l'aide de Central Configuration Manager ou de la page Web Crystal.

Reconfiguration de Crystal Page Server à l'aide de Central Configuration Manager

1. Cliquez *Démarrer* > *Tous les programmes* > *BusinessObjects 11* > *Crystal Reports Server* > *Central Configuration Manager.*
2. Cliquez avec le bouton droit sur *Crystal Reports Page Server* et sélectionnez *Arrêter*.
3. Cliquez avec le bouton droit sur *Crystal Reports Page Server* et sélectionnez *Propriétés*.

4. Dans le champ Commande sous l'onglet Propriétés, à la fin de la ligne de commandes ajoutez -maxDBResultRecords <valeur supérieure à 20 000 ou 0 pour désactiver la limite par défaut>.
5. Redémarrez Crystal Page Server.

Reconfiguration de Crystal Page Server à l'aide de la page Web Crystal

1. Ouvrez un navigateur Web et entrez l'URL suivant :

```
http://<nom DNS ou adresse IP de votre serveur Web >
   /businessobjects/enterprise11/WebTools/adminlaunch/
   default.aspx
```

2. Cliquez sur *Central Management Console*.
3. Le nom du système devrait être le nom de l'ordinateur hôte. Le type d'authentification devrait être Enterprise. Dans le cas contraire, choisissez Enterprise.
4. Entrez votre nom d'utilisateur, votre mot de passe et cliquez sur *Se loguer*.
5. Cliquez sur *Serveurs*.
6. Cliquez sur <*nom_serveur*>.*pageserver*.
7. Sous *Enregistrements de la base de donnés à lire à l'aperçu ou au rafraîchissement d'un rapport*, cliquez sur *Enregistrements illimités*.
8. Cliquez sur *Appliquer*.
9. Une invite pour redémarrer le serveur de pages s'affiche, cliquez sur *OK*.
10. L'invite peut vous demander un nom de login et le mot de passe pour accéder au gestionnaire de services du système d'exploitation.

Configuration de Sentinel pour intégrer Crystal Enterprise Server

Après l'installation de Crystal Enterprise Server, Sentinel Control Center peut être configuré pour avoir un accès direct via Sentinel Control Center.

Configuration de Sentinel pour intégrer Crystal Enterprise Server

1. Loguez-vous sur Sentinel Control Center comme un utilisateur doté de privilèges pour l'onglet Admin.
2. Sur l'onglet Admin, sélectionnez *Configuration de la création de rapport*.
3. Dans le champ Analyse d'URL, entrez la commande suivante:

```
http://<nom_hôte_ou_IP_du_serveur_Web>/GetReports.asp?
   APS=<nom_hôte>&user=Guest&password=&tab=Analysis
```

REMARQUE : <nom_hôte_ou_IP_du_serveur_Web> doit être remplacé par l'adresse IP ou par le nom d'hôte de Crystal Enterprise Server.

REMARQUE : l'URL ci-dessus ne marche pas correctement si l'APS est configuré à l'adresse IP. Ce doit être le nom d'hôte de Crystal.Server.

4. Cliquez sur *Rafraîchir* à coté du champs Analyse d'URL.
5. Si l'Advisor est installé, entrez la commande suivante dans le champ URL Advisor :

```
http://<nom_hôte_ou_IP_du_serveur_Web>/GetReports.asp?
   APS=<nom_hôte>&user=Guest&password=&tab=Advisor
```

REMARQUE : <nom_hôte_ou_IP_du_serveur_Web> doit être remplacé par l'adresse IP ou par le nom d'hôte de Crystal Enterprise Server.

REMARQUE : l'URL ci-dessus ne marche pas correctement si l'APS est configuré à l'adresse IP. Ce doit être le nom d'hôte de Crystal.Server.

6. Cliquez sur *Rafraîchir* à coté du champs URL Advisor.
7. Cliquez sur *Enregistrer*.
8. Déloguez-vous et reloguez-vous sur Sentinel Control Center. Les arborescences Crystal Report dans les onglets Analyse et Advisor (si l'Advisor est installé) devraient alors apparaître dans la fenêtre Navigateur.

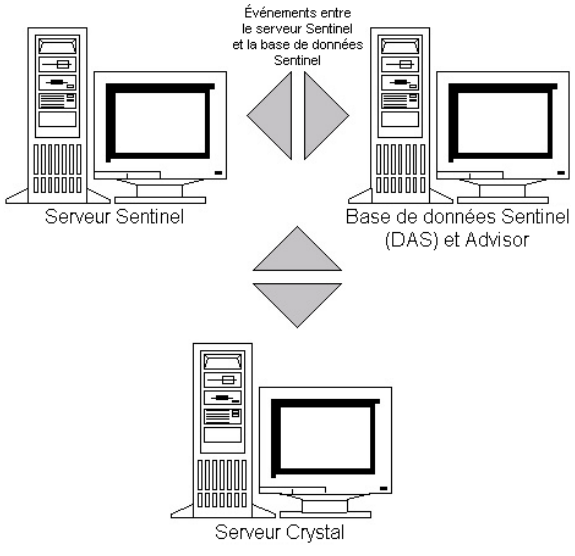
10 Crystal Reports pour Linux

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Crystal BusinessObjects Enterprise™ 11 est un des outils de création de rapport qui fait partie de Sentinel.

Ce chapitre traite de la configuration de l'installation de Crystal Reports Server pour Sentinel sous Linux. L'installation devrait être faite dans l'ordre indiqué ci-dessous :

- préinstallation et installation de Crystal BusinessObjects Enterprise™ 11
- correctif Crystal Reports
- publication (importation) de Crystal Reports
- configuration du compte « utilisateur nommé »
- test de la connectivité serveur Web
- activation du Top 10 des rapports (facultative)
- maximisation de la création de rapport d'évènements (recommandée)
- configuration de Sentinel pour Crystal Enterprise Server



Utilisation de Crystal Reports

Pour plus d'informations sur l'utilisation de Crystal Reports pour la création de rapport Sentinel, voir la documentation sur *Crystal Reports* et le *guide d'utilisateur Sentinel*.

Configuration

- Les versions Linux :
  - SuSE Linux Enterprise Server 9 (SLES 9)
  - Red Hat Enterprise Linux 3 Mise à jour 5 ES (x86)
- BusinessObjects Enterprise XI Server installé
- Pour Oracle - Oracle 9i Client Release 2 (9.2.0.1.0)

Installation

Préinstallation de Crystal BusinessObjects Enterprise™ 11

Préinstallation de Crystal BusinessObjects Enterprise

1. Si la base de données Sentinel n'est pas sur la même machine que Crystal Server, vous devez installer le logiciel Oracle Client sur la machine Crystal Server. Cette étape supplémentaire n'est pas nécessaire si la base de données Sentinel est sur la même machine que Crystal Server, puisque dans ce cas le logiciel Oracle est déjà installé avec le logiciel de la base de données Oracle comme requis par la base de données Sentinel.
2. Loguez-vous sur la machine Crystal Server comme utilisateur root.
3. Créez un groupe bobje

   ```
   groupadd bobje
   ```

4. Créez l'utilisateur crystal (le répertoire privé dans cet exemple est « /export/home/crystal », changez-le si nécessaire, la partie « /export/home » du chemin doit déjà exister).

   ```
   useradd –g bobje –s /bin/bash –d /export/home/crystal
      –m crystal
   ```

5. Créez un répertoire pour le logiciel Crystal :

   ```
   mkdir –p /opt/crystal_xi
   ```

6. Changez la propriété du répertoire du logiciel Crystal (de façon récurrente) en crystal/bobje:

   ```
   chown -R crystal:bobje /opt/crystal_xi
   ```

7. Passez à l'utilisateur crystal :

   ```
   su - crystal
   ```

8. La variable d'environnement ORACLE_HOME doit être configurée dans l'environnement de l'utilisateur crystal. À cet effet, modifiez le script du login de l'utilisateur crystal pour définir la variable d'environnement ORACLE_HOME pour la base du logiciel Oracle. Par exemple, si le shell de l'utilisateur crystal est bash et le logiciel Oracle est installé dans le répertoire /opt/oracle/product/9.2, ouvrez alors le fichier ~crystal/.bash_profile et ajoutez la ligne suivante à la fin du fichier :

   ```
   export ORACLE_HOME=/opt/oracle/product/9.2
   ```

9. La variable d'environnement LD_LIBRARY_PATH dans l'environnement de l'utilisateur crystal doit contenir le chemin vers les bibliothèques du logiciel Oracle. À cet effet, modifiez le script du login de l'utilisateur crystal pour définir la variable d'environnement LD_LIBRARY_PATH afin d'inclure les bibliothèques du logiciel Oracle. Par exemple, si le shell de l'utilisateur crystal est bash, ouvrez le fichier ~crystal/.bash_profile et ajoutez la ligne suivante à la fin du fichier (sous l'emplacement où la variable d'environnement ORACLE_HOME est définie :

```
export
   LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

10. Vous devez ajouter une entrée dans le fichier Oracle tnsnames.ora avec le nom de service « sentineldb » qui cible la base de données Sentinel. Pour le faire sur une machine Crystal Server.
    a. Loguez-vous comme utilisateur oracle.
    b. Changez les répertoires vers $ORACLE_HOME/network/admin
    c. Faites une sauvegarde du fichier tnsnames.ora.
    d. Ouvrez le fichier tnsnames.ora pour l'éditer.
    e. Si la base de données Sentinel est sur la machine Crystal Server, il doit déjà exister une entrée dans le fichier tnsnames.ora pour la base de données Sentinel. Par exemple, si la base de données Sentinel est nommée ESEC, il doit exister une entrée semblable à la suivante :

```
ESEC =
(DESCRIPTION =
 (LISTE_ADRESSES =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT
   = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

    f. Si la base de données Sentinel n'est pas sur la machine Crystal Server, ouvrez le fichier tnsnames.ora sur la machine de la base de données Sentinel, pour trouver l'entrée mentionnée ci-dessus.
    g. Faites une copie de toute l'entrée et collez-la à la fin du fichier tnsnames.ora dans la machine Crystal Server. La partie Nom de service de l'entrée doit être renommée « sentineldb ». Par exemple, lorsque l'entrée mentionnée ci-dessus est copiée et renommée correctement, elle correspond à :

```
sentineldb =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT
   = 1521))
```

```
    )
    (CONNECT_DATA =
    (SID = ESEC)
    )
  )
```

h. Vérifiez que la partie HÔTE de l'entrée est correcte (par ex. assurez-vous qu'elle n'est pas définie comme hôte local si Crystal Server et la base de données Sentinel sont dans des machines différentes).
i. Enregistrez les changements dans le fichier tnsnames.ora.
j. Exécutez la commande suivante pour vérifier que le nom de service sentineldb est configuré correctement :

```
tnsping sentineldb
```

k. Si la commande est exécutée avec succès, vous devrez obtenir un message déclarant que la connexion est OK.

Installation de Crystal BusinessObjects Enterprise™ 11

Installation de Crystal BusinessObjects Enterprise

1. Loguez-vous comme utilisateur crystal.
2. Changez les répertoires vers le DISK_1 du programme d'installation Crystal.
3. Exécutez :

```
./install
```

4. Sélectionnez la langue : *français*
5. Sélectionnez *Nouvelle Installation*
6. Acceptez l'accord de Licence
7. Entrez le code clé du produit
8. Entrez le répertoire d'installation :

```
/opt/crystal_xi
```

9. Sélectionnez : *Installation d'utilisateur*
10. Sélectionnez : *Nouvelle installation*
11. Sélectionnez : *Installer MySQL*
12. Entrez les informations de configuration pour MySQL :
    a. Utiliser le port par défaut 3306
    b. mot de passe Admin
13. Entrez plus d'informations de configuration pour MySQL :
    a. Nom base de données par défaut : BOE11
    b. ID utilisateur : mysqladm
    c. mot de passe
14. Entrez plus d'informations de configuration pour MySQL :
    a. Nom du serveur local : <nom_hôte_de_machine_locale>
    b. Numéro de port CMS par défaut : 6400

15. Sélectionnez : *Installer Tomcat*
16. Entrez les informations de configuration de Tomcat :
    a. port par défaut pour recevoir les requêtes HTTP : 8080
    b. port par défaut pour réorienter les requêtes jsp : 8443
    c. Numéro de port de raccordement d'arrêt : 8005
17. Appuyez sur *Enter* pour lancer l'installation

Correctifs de Crystal Reports pour l'utilisation avec Sentinel

Afin d'afficher Crystal Reports à partir de l'onglet Analyse de Sentinel Control Center, plusieurs fichiers Crystal Enterprise doivent être mis à jour pour les rendre compatibles avec le navigateur incorporé dans Sentinel.

Le tableau suivant liste ces fichiers et décrit l'utilisation de chacun.

Nom du fichier	***Description***

`calendar.js`
 	
`calendar.html`
	Il affiche un calendrier contextuel lorsque vous sélectionnez une date comme paramètre d'un rapport.

`grouptree.html`	Il affiche le message Chargement… pendant que les rapports sont chargés.
`exportframe.html`	Il affiche la fenêtre qui vous permet d'exporter un rapport afin de le sauvegarder ou de l'imprimer.
`exportIce.html`	Fichier utilisé par Sentinel lors de l'exportation d'un rapport, afin de le sauvegarder ou de l'imprimer.
`GetReports.asp`	Fichier utilisé par Sentinel Control Center pour établir une connexion avec Crystal Server et afficher la liste de rapports.

Correctifs Crystal Reports

1. ACTUELLEMENT DISPONIBLE SEULEMENT DEPUIS LE SERVICE PACK. Sur le CD Sentinel Service Pack, allez à \content\reports\patch et copiez tous les fichiers *.html et *.js dans l'emplacement du fichier visualiseur, par défaut :

   ```
   /opt/crystal_xi/bobje/webcontent/enterprise11/
      viewer/en/
   ```

2. Sur le CD Sentinel Service Pack, allez à \content\reports\patch et copiez tous les fichier *.jsp dans :

   `/opt/crystal_xi/bobje/tomcat/webapps/`**`esec-script/`**

REMARQUE : créez un dossier nommé **esec-script**

   `Copy all *.jar files`

   de :

   `/opt/crystal_xi/bobje/tomcat/webapps/jsfadmin/WEB-INF/lib/`

   vers :

   `/opt/crystal_xi/bobje/tomcat/webapps/esec-script/WEB-INF/lib`

REMARQUE : créez une structure de dossiers **WEB-INF/lib**

Publication de modèles Crystal Report

Ces modèles de rapport sont créés par Novell pour être utiliser dans l'analyse Sentinel Control Center et l'onglet Advisor.

Il y deux méthodes de publication de rapports.

- Crystal Publishing Wizard
- Crystal Reports Central Management Console

Des exemples de rapports sont également fournis en format pdf.

REMARQUE : La liste d'attaques faite par le rapport CVE est une intersection de signatures d'attaques entre l'alimentation Advisor et les vulnérabilités analysées.

REMARQUE : pour exécuter un des rapports Top 10, le regroupement doit être activé et l'EventFileRedirectService dans le DAS_Binary.xml doit être actif. Pour obtenir des informations sur le mode d'activation du regroupement, voir le *guide d'utilisateur Sentinel, chapitre 10, le gestionnaire de données Sentinel*, à la section *Onglet Données de création de rapport* ou allez à la section Activation des Top 10 rapports Sentinel.

Publication des modèles de Rapport - Crystal Publishing Wizard

REMARQUE : une plate-forme Windows est requise pour l'exécution de Crystal Publishing Wizard.

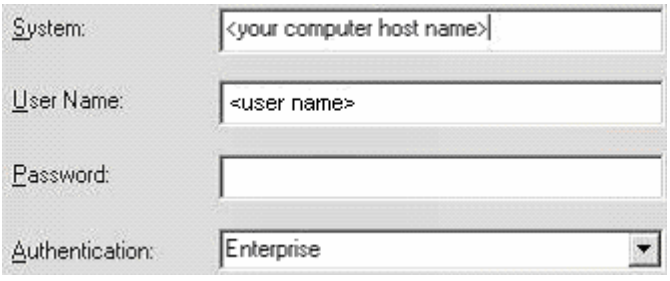
Importation de modèles Crystal Report

REMARQUE : si vous réimportez (republiez) les modèles de rapports, supprimez la dernière importation de modèles de rapports.

1. Cliquez sur Démarrer > Tous les Programmes > BusinessObjects 11 > Crystal Reports Server > Publishing Wizard.
2. Cliquez sur *Suivant.*

3. Login. Système doit être le nom de l'ordinateur hôte et l'authentification doit être Entreprise. Le nom d'utilisateur peut être Administrateur. Pour des raisons de sécurité, vous devriez utiliser un autre utilisateur différent d'Administrateur. Entrez votre mot de passe et cliquez sur *Suivant*.

REMARQUE : la publication des rapports sous l'Administrateur d'utilisateurs permet à tous les utilisateurs d'avoir accès aux rapports.

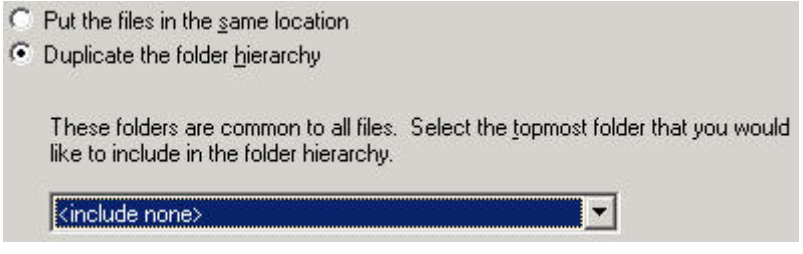


4. Cliquez sur *Ajouter dossier*.
5. Cliquez sur *Inclure sous-dossier*. Sur le CD-ROM Sentinel Service Pack, naviguez vers :

   ```
   content\reports\Crystal_v11\Oracle
   ```

   Cliquez sur *OK*.
6. Cliquez sur *Suivant.*
7. Sur la fenêtre Spécifier emplacement, cliquez sur *Nouveau dossier* (en haut à droite) et créez un dossier nommé *Rapports_Sentinel*. Cliquez sur *Suivant.*

8. Sélectionnez :
   - *Hiérarchie de dossiers dupliquée*.
   - Cliquez sur la flèche bas et sélectionnez *<n'inclure aucun>*



   Cliquez sur *Suivant.*
9. Sur la fenêtre Confirmer emplacement, cliquez sur *Suivant*.

10. Dans la fenêtre Spécifier Catégories :
    - un nom de catégorie au choix (comme sentinel)
    - sélectionnez le nom et cliquez sur le bouton + (plus)

REMARQUE : seul le premier rapport apparaît sous la catégorie, après avoir cliqué sur Suivant.

    - Cliquez sur *Suivant*.
11. Dans la fenêtre Spécifier la planification, cliquez sur *Laisser les utilisateurs mettre à jour l'objet* (cette option doit être définie par défaut). Cliquez sur *Suivant.*
12. Dans la fenêtre Spécifier rafraîchissement de référentiel, cliquez *Activer tout* pour activer le rafraîchissement de référentiel. Cliquez sur *Suivant.*
13. Dans la fenêtre Spécifier sauvegarder données enregistrées, cliquez *Activer tout* pour sauvegarder les données enregistrées lors de la publication des rapports. Cliquez sur *Suivant.*
14. Dans la fenêtre Changer valeurs par défaut, cliquez sur *Publier rapports sans modifier les propriétés* (cette option doit être définie par défaut). Cliquez sur *Suivant.*
15. Cliquez sur *Suivant* pour ajouter les objets.
16. Cliquez sur *Suivant.*
17. Cliquez sur *Terminer*.

Quand les modèles Sentinel pour Crystal Reports sont publiés dans Crystal Enterprise server, les modèles doivent se trouver dans le répertoire Sentinel_Reports.

Publication des modèles de Rapport - Console de gestion centralisée

Lors de la publication des rapports à l'aide de la centrale de gestion centralisée, le rapport ne peut pas être publié en lot, comme dans l'utilisation de Publishing Wizard actionné par Windows.

Importation de modèles Crystal Report

1. Ouvrez un navigateur Web et entrez l'URL suivant :

```
http://<nom_hôte_ou_IP_du_serveur_Web>:<port_default_de_serveur_Web_8080>/businessobjects/enterprise11/adminlaunch
```

2. Cliquez sur *Console de gestion centralisée*.
3. Loguez-vous sur Crystal Server.
4. Sur le volet Organiser, cliquez sur *Dossiers*.
5. En haut à droite, cliquez sur *Nouveau dossier…*.
6. Créez un dossier nommé *Rapports_Sentinel.* Cliquez sur *OK*.
7. Cliquez sur *Rapports_Sentinel*.

8. Cliquez sur l'onglet Sous-dossiers et créez les sous-dossiers suivants.
   - vulnérabilité_Advisor
   - gestion incidents
   - évènements internes
   - évènements de sécurité
   - Top 10
9. Cliquez sur *Accueil*.
10. Cliquez sur *Objets*.
11. Cliquez sur *Nouvel Objet*.
12. À gauche de la page, sélectionnez *Rapport*.
13. Cliquez *Parcourir* et parcourez le CD Sentinel Service Pack.

    ```
    content\reports\Crystal_v11\Oracle
    ```

    Choisissez un dossier et sélectionnez un rapport.
14. Sélectionnez *Rapports_Sentinel* et cliquez sur *Afficher sous-dossiers*.
15. Sélectionnez le dossier adéquat pour le rapport et cliquez sur *Afficher sous-dossiers*.
16. Cliquez sur *OK*.
17. Cliquez sur *Mettre à jour*.
18. Cliquez sur l'onglet *Rapports* et continuez l'ajout de *Rapports*.
19. Pour ajouter les rapports restants à un autre dossier, cliquez sur *Dossiers* (en haut à gauche) et répétez les étapes de 14 à 17.

Utilisation de Crystal XI Web Server

Crystal Server XI sous Linux installe un serveur Web par le biais duquel vous pouvez aussi bien effectuer des tâches administratives, que publier et afficher des rapports.

L'accès au portail administratif est effectué via le navigateur à l'URL suivant :

```
http://<nom_hôte_ou_IP_du_serveur_Web>:
   <port_default_de_serveur_Web_8080>/businessobjects/
   enterprise11/adminlaunch
```

L'accès au portail non administratif (utilisation générale) est effectué via le navigateur à l'URL suivant :

```
http://<nom_hôte_ou_IP_du_serveur_Web>:
   <port_default_de_serveur_Web_8080>/businessobjects/
   enterprise11
```

Test de la connectivité serveur Web

Tester la connectivité serveur Web

1. Entrez sur une autre machine mais dans le même réseau que votre serveur Web.
2. Entrez

```
http://<nom_hôte_ou_IP_du_serveur_Web>:<port_default_de_serveur_Web_8080>/businessobjects/enterprise11/adminlaunch
```

3. La page Web Crystal BusinessObjects devrait s'afficher.

Configuration d'un compte d'« utilisateur nommé »

La clé de licence fournie avec Crystal server est une clé de compte d'« utilisateur nommé ». Le compte Guest « Utilisateur simultané » doit être remplacé par « Utilisateur nommé ».

Configuration du compte GUEST comme « Utilisateur nommé »

1. Ouvrez un navigateur Web et entrez l'URL suivant :

```
http://<nom_hôte_ou_IP_du_serveur_Web>:<port_default_de_serveur_Web_8080>/businessobjects/enterprise11/adminlaunch
```

2. Cliquez sur *Console de gestion centralisée*.
3. Le nom du système devrait être le nom de l'ordinateur hôte. Le type d'authentification devrait être Entreprise. Dans le cas contraire, choisissez Enterprise.
4. Dans le volet Organiser, cliquez sur *Utilisateurs*.
5. Cliquez sur Guest.
6. Remplacez le type de connexion *Utilisateur simultané* par *Utilisateur nommé.*
7. Cliquez sur *Mettre à jour*.
8. Déloguez-vous et fermez la fenêtre.

Configuration de rapports

Cette procédure traite du mode de configuration d'Administration Launchpad pour que vous puissiez voir et modifier les rapports.

Configuration d'Administration Launchpad

1. Ouvrez un navigateur Web et entrez l'URL suivant :

```
http://<nom_hôte_ou_IP_du_serveur_Web>:<port_default_de_serveur_Web_8080>/businessobjects/enterprise11/adminlaunch
```

2. Cliquez sur *Console de gestion centralisée*.
3. Le nom du système devrait être le nom de l'ordinateur hôte. Le type d'authentification devrait être Enterprise. Dans le cas contraire, choisissez *Enterprise*.
4. Entrez votre nom d'utilisateur, votre mot de passe et cliquez sur *Se loguer*.

5. Dans le volet Organiser, cliquez sur *Dossiers*.
6. Cliquez une fois sur *Rapports_Sentinel*.
7. Sélectionnez *Tous*.
8. Cliquez sur l'onglet Droits.
9. Pour Tout le monde, sur le menu déroulant vers la droite sélectionnez *Affichage à la demande*. Cliquez sur *Mettre à jour*.
10. Déloguez-vous et fermez la fenêtre.

Activer Top 10 des rapports Sentinel

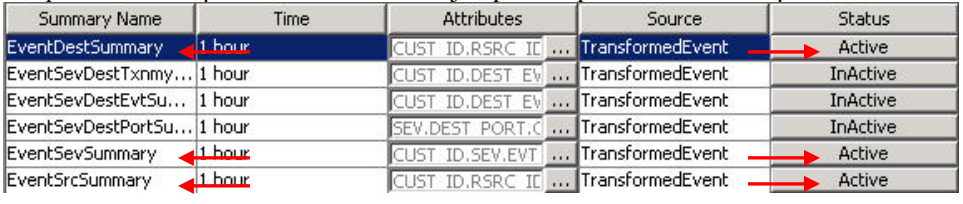
Pour activer le Top 10 des rapports Sentinel, vous devez :

- activer Regroupement
- activer EventFileRedirectService

Activation de regroupement

1. Démarrez le gestionnaire de données Sentinel.
2. Login.
3. Cliquez sur l'onglet *Données de la création de rapport*.
4. Activez les résumés suivants :
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   Cliquez sur *Inactif* dans la colonne État jusqu'à ce qu'il devienne *Actif*.



Activation d'EventFileRedirectService

1. Sur la machine DAS, à l'aide de l'éditeur de texte, ouvrez :

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

2. Pour EventFileRedirectService, changez l'état en « actif ».

   ```
   <nom propriété="état">actif</propriété>
   ```

3. Redémarrez le processus DAS_Binary. Ce qui peut être fait à l'aide de Sentinel Control Center ou en redémarrant la machine.

   Utilisation de Sentinel Control Center :

   - Loguez-vous dans Sentinel Control Center comme un utilisateur doté de droits d'administrateur. Cet utilisateur doit avoir les autorisations de « Vues de serveur » suivantes :
     - Afficher serveurs
     - Contrôler serveurs

- Depuis l'onglet Admin, ouvrez une vue de serveur pour afficher tous les processus du serveur Sentinel.
- Cliquez avec le bouton droit sur le processus *DAS_Binary* et sélectionnez *Redémarrer*.
- Le décompte de « démarrages » pour ce processus augmente d'un si le processus est redémarré avec succès.

Maximisation de la création de rapport d'évènements

En fonction du nombre d'évènements consultés par Crystal, vous pouvez obtenir une erreur sur la durée maximale de traitement ou sur la limite maximale d'enregistrements. Pour configurer le serveur afin qu'il traite un nombre supérieur ou illimité de rapports, vous devez reconfigurer Crystal Page Server.

Reconfiguration de Crystal Page Server

1. Ouvrez un navigateur Web et entrez l'URL suivant :

   ```
   http://<nom_hôte_ou_IP_du_serveur_Web>:<port_default_de_serveur_Web_8080>/businessobjects/enterprise11/adminlaunch
   ```

2. Cliquez sur *Console de gestion centralisée*.
3. Le nom du système devrait être le nom de l'ordinateur hôte. Le type d'authentification devrait être Enterprise. Dans le cas contraire, choisissez Enterprise.
4. Entrez votre nom d'utilisateur, votre mot de passe et cliquez sur *Se loguer*.
5. Cliquez sur *Serveurs*.
6. Cliquez sur *<nom_serveur>.pageserver*
7. Sous *Enregistrements de la base de données à lire à l'aperçu ou au rafraîchissement d'un rapport*, cliquez sur *Enregistrements illimités*.
8. Cliquez sur *Appliquer*.
9. Une invite pour redémarrer le serveur de pages apparaît, cliquez sur *OK*.
10. L'invite peut vous demander un nom de login et le mot de passe pour accéder au gestionnaire de services du système d'exploitation.

Configuration de Sentinel pour Crystal Enterprise Server

Après l'installation de Crystal Enterprise, Sentinel Control Center a besoin des URLs pour les rapports Analyses.

Configuration de Sentinel pour Crystal Enterprise Server

1. Loguez-vous sur Sentinel Control Center comme un utilisateur dotés de privilèges à l'onglet Admin.
2. Sur l'onglet Admin, sélectionnez *Configuration de la création de rapport*.

3. Dans le champ Analyse d'URL, entrez la commande suivante :

```
http://<nom_hôte_ou_IP_du_serveur_Web>:<port_default_de_serveur_Web_8080>/esec-script/GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

REMARQUE : <nom_hôte_ou_IP_du_serveur_Web> doit être remplacé par l'adresse IP ou par le nom d'hôte de Crystal Enterprise Server.

REMARQUE : l'URL ci-dessus ne fonctionne pas correctement si l'APS est configuré à l'adresse IP. C'est obligatoirement le nom d'hôte.

REMARQUE : <port_par_défaut_du_serveur_Web_8080> doit être remplacé par le port sur lequel le serveur Web Crystal écoute.

4. Cliquez sur *Rafraîchir* à coté du champ Analyse d'URL.
5. Si l'Advisor est installé, entrez la commande suivante dans le champ URL Advisor :

```
http://<nom_hôte_ou_IP_du_serveur_Web>:<port_par_defaut_de_serveur_Web_8080>/esec-script/GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

REMARQUE : <nom_hôte_ou_IP_du_serveur_Web> doit être remplacé par l'adresse IP ou par le nom d'hôte de Crystal Enterprise Server.

REMARQUE : l'URL ci-dessus ne fonctionne pas correctement si l'APS est configuré à l'adresse IP. C'est obligatoirement le nom d'hôte.

REMARQUE : <port_par_défaut_du_serveur_Web_8080> doit être remplacé par le port sur lequel le serveur Web Crystal écoute.

6. Cliquez sur *Rafraîchir* à coté du champ URL Advisor.
7. Cliquez sur *Enregistrer*.
8. Déloguez-vous et reloguez dans Sentinel Control Center. Les arborescences Crystal Report dans les onglets Analyse et Advisor (si l'Advisor est installé) devraient alors s'afficher sur la fenêtre Navigateur.

Utilitaires et dépannage

Démarrage de MySQL

Pour vous assurer que MySQL est en cours exécution :

1. Loguez-vous comme utilisateur crystal.
2. cd /opt/crystal_xi/bobje
3. ./mysqlstartup.sh

Démarrage de Tomcat

Pour vous assurer que Tomcat est en cours d'exécution :

1. Loguez-vous comme utilisateur crystal
2. cd /opt/crystal_xi/bobje
3. ./tomcatstartup.sh

Démarrage de serveurs Crystal Server

Pour vous assurer que les serveurs Crystal Server sont en cours d'exécution :

1. Loguez-vous comme utilisateur crystal
2. cd /opt/crystal_xi/bobje
3. ./startservers

Erreur de nom d'hôte Crystal

Erreur de nom d’hôte

1. Si l’erreur suivante s’affiche :

```
Avertissement : ORB::BOA_init: recherche de noms
   d’hôte affiche « hôte local » (127.0.0.1)

Utilisez l’option -OAhost pour sélectionner d’autres
   noms d’hôte
```

   Assurez-vous que votre IP et votre nom d’hôte sont dans le fichier /etc/hosts. Exemple :

```
192.0.2.46  linuxCE02
```

Impossible de se connecter à CMS

Si le système indique qu'il ne peut pas se connecter à CMS, essayez d'exécuter les commandes suivantes.

Dépannage de l’échec de la connexion CMS

1. Si la commande « netstat –an | grep 6400 » ne renvoie pas de résultats, essayez les opérations suivantes :
   - entrez à nouveau les informations de connexion MySQL :

   a. Loguez-vous comme utilisateur crystal
   b. cd /opt/crystal_xi/bobje
   c. ./cmsdbsetup.sh
   d. Appuyez sur Enter lorsque « [<nom_hôte>.cms] » s’affiche
   e. Choisissez *Sélectionner* et entrez à nouveau toutes les infos de la base de données MySQL qui ont été entrées pendant l’installation (consultez les instructions d’installation).
   f. Après avoir fait cela, quittez cmsdbsetup.sh
   g. ./stopservers
   h. ./startservers

   - réinitialisez la base de données MySQL :

   a. Loguez-vous comme utilisateur crystal
   b. cd /opt/crystal_xi/bobje
   c. ./cmsdbsetup.sh
   d. Appuyez sur Enter lorsque « [<nom_hôte>.cms] » s’affiche
   e. Choisissez « réinitialiser » et suivez les instructions.
   f. Après avoir fait cela, quittez cmsdbsetup.sh
   g. ./stopservers
   h. ./startservers

2. Assurez-vous que tous les serveurs CCM sont activés :
    a. Loguez-vous comme utilisateur crystal
    b. cd /opt/crystal_xi/bobje
    c. ./ccm.sh -enable all

11 Configuration de l’Advisor

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Sentinel Advisor, optimisé par SecurityNexus, fournit des renseignements en temps réel pour les vulnérabilités d’entreprise, des conseils d’expertise et des étapes recommandées pour la résolution. L'Advisor fournit une référence croisée entre les signatures d’attaque IDS en temps réel et la base de connaissances de l'Advisor sur les vulnérabilités. Visitez http://www.esecurity.net/Software/Products/Advisor.asp pour obtenir plus d’informations.

L’installation d’Advisor est facultative. Cependant, c'est un composant nécessaire si vous voulez utiliser la détection d’exploits Sentinel ou les fonctionnalités de création de rapport Advisor.

Crystal BusinessObjects Enterprise™ 11 est un des outils de création de rapport qui fait partie de Sentinel. Pour plus d’informations sur l’installation de Crystal BusinessObjects Enterprise™ 11, voir le chapitre *Crystal Reports* adéquat pour la plate-forme sur laquelle vous voulez exécutez le Crystal Enterprise Server (Windows ou Linux). Si vous n’allez utiliser l'Advisor que pour la détection d'exploits, il n'est pas nécessaire d'installer Crystal Server. Crystal Server n’est nécessaire que si vous avez l'intention d'exécuter des rapports.

Ce chapitre explique comment configurer Sentinel pour exécuter Advisor Reports directement depuis Sentinel Control Center. Advisor Reports est conçu par Novell pour la création de rapport et l’analyse et, si l’intégration de Sentinel Control Center est configurée de façon adéquate, il apparaît sous l’onglet Advisor de Sentinel Control Center.

Installation de l’Advisor

Advisor peut seulement être installé sur la même machine où le DAS (Database Access Service) est installé.

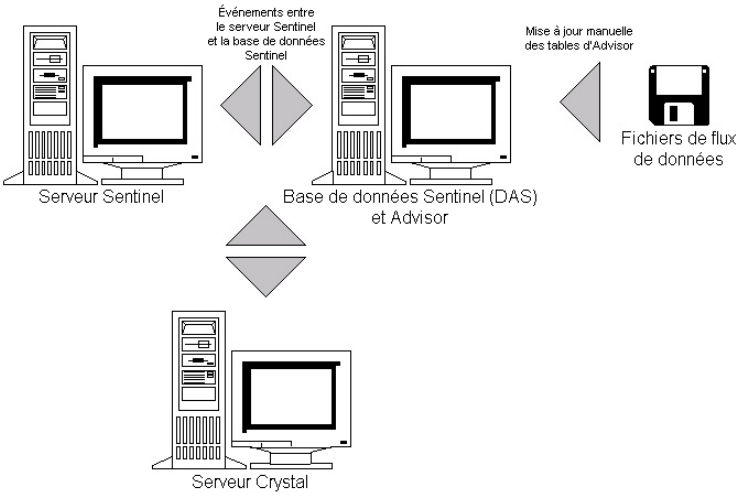
Deux options d’installation différentes sont disponibles. À savoir :

- indépendante
- téléchargement direct d’Internet

Si vous voulez exécuter Advisor Crystal Reports, consultez d’abord le chapitre *Crystal Reports* sur l’installation et la configuration de Crystal Server. Publiez ensuite Advisor Crystal Report dans Crystal Server. Voir Importation de modèles de rapport pour obtenir des instructions sur la publication des rapports.

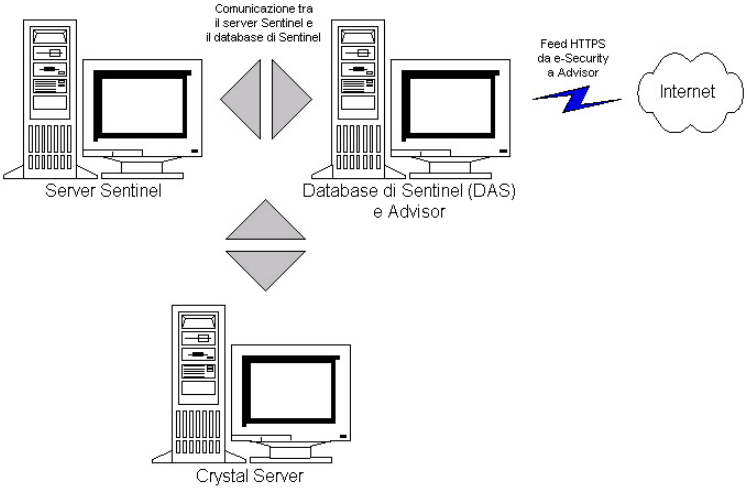
Configuration indépendante

L’installation indépendante est l'option où l’Advisor est un système isolé requérant une intervention manuelle pour recevoir des mises à jour de Novell.



Configuration de téléchargement direct d’Internet

Le téléchargement direct d’Internet est l'option où la machine Advisor est directement connectée à l’Internet. Dans cette configuration, les mises à jour de Novell sont automatiquement téléchargées de Novell sur Internet, à un rythme régulier.



Installation de l’Advisor

REMARQUE : avant d’installer l'Advisor, vérifiez que vous avez l’ID Advisor et le mot de passe de qui vous ont été donnés par Novell. Pendant l’installation, une invite vous demande le nom d’utilisateur et le mot de passe.

Si vous voulez exécuter Advisor Reports (Crystal Reports), effectuez les tâches suivantes dans l'ordre indiqué. Vous n’avez pas besoin d’effectuer les tâches suivantes, si vous comptez utiliser Advisor seulement pour la détection d’exploits.

- Si cela n'a pas encore été fait, réalisez les opérations suivantes (voir le chapitre *Crystal Reports*) :
  - Installez Microsoft Internet Information Server (IIS)
  - **Pour la base de données Sentinel sur Oracle (Linux) -** Préinstallez Crystal BusinessObjects Enterprise
  - Installez Crystal BusinessObjects Enterprise™ 11
  - **Pour la base de données Sentinel sur Oracle (Solaris) -** configurez le pilote natif Oracle (pour des installations Oracle)
  - **Pour la base de données Sentinel sur MS SQL (Windows) -** Configurer ODBC (Open Database Connectivity)
  - Correctif Crystal Reports - voir le chapitre *Crystal Reports*.
- Installez l'Advisor – s'il n'est pas encore installé, voir le chapitre *Ajout des composants sur une installation existante*.
- Importez les modèles Crystal Report
- Créez une page Web Crystal
- Configurez Sentinel Control Center pour intégrer Crystal Enterprise Server

Importation des modèles de rapports

En fonction du système d'exploitation, consultez :

- *le chapitre 9 – Crystal Reports pour Windows et Solaris*
- *le chapitre 10 – Crystal Reports pour Linux*

Configuration d' Administration Launchpad

En fonction du système d'exploitation, consultez :

- *le chapitre 9 – Crystal Reports pour Windows et Solaris*
- *le chapitre 10 – Crystal Reports pour Linux*

Configuration de l'intégration de Sentinel Control Center avec Advisor Reports

Sentinel Control Center a la capacité via l'onglet Advisor de s'intégrer avec Advisor Reports. À l'aide de cette capacité vous pouvez afficher un rapport Advisor directement depuis Sentinel Control Center.

Pour activer cette capacité, premièrement installez Crystal Server, puis importez les modèles d'Advisor Reports dans Crystal Reports et installez l'Advisor. Une fois ces conditions préalables remplies, suivez les instructions de la section « Configuration de Sentinel pour l'intégration avec Crystal Enterprise Server » dans :

- *le chapitre 9 – Crystal Reports pour Windows et Solaris*
- *le chapitre 10 – Crystal Reports pour Linux*

Mise à jour de données sur les tables Advisor

Sauf si vous avez une configuration indépendante, les données sur les tables Advisor sont automatiquement mises à jour pendant le prochain téléchargement d'alimentation Advisor programmé. Toutefois, les données peuvent être mises à jour manuellement. Pour la mise à jour manuelle, voir le *guide de l'utilisateur Sentinel*.

Réinitialiser le mot de passe Advisor (seulement téléchargement direct)

Si vous exécutez l'Advisor sous le mode de téléchargement direct et que vous venez d'obtenir un nouveau mot de passe Advisor, ou encore si le mot de passe Advisor défini pendant l'installation était incorrect, vous devez réinitialiser le mot de passe Advisor codifié stocké dans le fichier de configuration de l'Advisor.

La mise à jour du mot de passe Advisor codifié n'est pas applicable, si vous exécutez l'Advisor dans une configuration indépendante, parce que, sous ce mode-là, le mot de passe n'est pas stocké dans le fichier de configuration Advisor.

Pour réinitialiser le mot de passe Advisor codifié stocké dans le fichier de configuration Advisor, effectuez les étapes suivantes :

1. Pour UNIX, loguez-vous comme esecadm ou pour Windows, loguez-vous comme utilisateur doté de droits administratifs. Loguez-vous sur la machine où l'Advisor est installé.
2. Changez les répertoires vers :

   Pour UNIX :

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

   Pour Windows :

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

3. Exécutez la commande suivante, où <nouveau_mot_de_passe> correspond au mot de passe Advisor que vous voulez définir :

   Pour UNIX :

   ```
   ./adv_change_passwd.sh <nouveau_mot_de_passe>
   ```

   Pour Windows :

   ```
   adv_change_passwd.bat <nouveau_mot_de_passe>
   ```

12 Test de l’installation

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Les collecteurs de test suivants sont installés avec le composant service de collecteur (gestionnaire de collecteurs) pour vous aider à tester votre installation. Le nom et la description de chacun de ces collecteurs sont les suivants :

Pour tester le flux d’évènements de base :

- SendOneEvent – il envoie un évènement par Sentinel, puis il s’arrête.
- SendMultipleEvents – il envoie 20 évènements par Sentinel, puis il s’arrête.

Pour tester l’assignation des actifs d'évènements et la détection d’exploits :

- DemoEvents – il envoie 13 évènements par Sentinel, puis il s’arrête.
- DemoAssetUpload – il charge les données d’un actif démo dans Sentinel. Lorsque le collecteur DemoEvents est exécuté après l'exécution de ce collecteur, les données d'actifs provenant de ce collecteur apparaissent dans les évènements provenant du collecteur DemoEvents, suite à l’assignation d’évènements. Ce collecteur ne génère pas d’évènements externes.
- DemoVulnerabilityUpload – il charge les données démo de vulnérabilité dans Sentinel. Lorsque le collecteur DemoEvents est exécuté après l’exécution de ce collecteur et du téléchargement d’alimentation de l'Advisor, certains évènements du collecteur DemoEvents déclenchent une détection d'exploits (c.-à-d., le champ Vulnérabilité de l’évènement est défini sur « 1 ». Ce collecteur ne génère pas d’évènements externes.

Pour plus d'informations (y compris la configuration) sur d’autres collecteurs, veuillez consulter :

```
%ESEC_HOME%\wizard\Elements\<Nom collecteur>\docs\
```

Test de l’installation avec les collecteurs de test

Dans Sentinel v5.1.2 et les versions ultérieures, les collecteurs de test sont installés préconfigurés sur tous les gestionnaires de collecteurs. Par conséquent, si vous utilisez cette version de Sentinel, vous pouvez exécuter directement les collecteurs de test pour tester votre installation.

Dans Sentinel v5.1.1 et les versions antérieures, vous devez configurer manuellement les collecteurs sur un gestionnaire de collecteurs avant de les utiliser. Pour configurer les collecteurs de test, suivez les instructions dans la section Configuration des collecteurs de test. Ensuite, retournez à cette section pour tester votre installation à l'aide des collecteurs de test.

Exécuter les collecteurs de test pour tester votre installation

1. Ouvrez l'application Sentinel Control Center.
2. Cliquez sur l'onglet *Collecteurs*.
3. Sur le dialogue gestionnaire de vues de collecteurs, double-cliquez sur la vue *TOUS LES AGENTS* pour ouvrir la vue de tous les ports de collecteur.
4. Cette vue de collecteurs affiche tous les ports de collecteurs qui sont actuellement configurés, groupés selon le nom du gestionnaire de collecteur. Si vous ne voyez aucun port de collecteur, cela signifie qu'aucun de vos gestionnaires de collecteurs n'est actuellement connecté à Sentinel. Si vous voulez qu'un ou plusieurs gestionnaires de collecteurs soient connectés à Sentinel, vérifiez que vos gestionnaires de collecteurs sont en cours d'exécution et s'il y a des erreurs dans les fichiers journaux du gestionnaire de collecteurs ou du serveur Sentinel.
5. Avant d'exécuter un collecteur, ouvrez Active View pour pouvoir afficher les évènements générés par les collecteurs de test. À cet effet, :
   - cliquez sur l'onglet *Active Views*.
   - sélectionnez *Active Views* > *Create Active View* sur la barre de menu.
   - sélectionnez le filtre *PUBLIC::External_Events*.
   - Cliquez sur *Terminer*.
6. Pour exécuter un collecteur afin de tester le flux d'évènements de base :
   - Allez à l'onglet *Collecteurs*.
   - cliquez avec le bouton droit sur le port du collecteur *SendMultipleEvents* dans la vue Collecteur et sélectionnez l'opération Démarrer. Comme les collecteurs de test sont exécutés pendant peu de temps et qu'ils s'arrêtent rapidement, l'état du port du collecteur devient brièvement « actif », puis il redevient « inactif ».
   - Pour vérifier que les évènements passent par le système, retournez à l'onglet Active Views et surveillez l' Active View que vous venez de créer. Veuillez noter que l'affichage de l'évènement sur l' Active View peut durer une minute après l'exécution du collecteur.
7. Pour exécuter un collecteur afin de tester l'assignation d'actifs d'évènement :
   - Allez à l'onglet Collecteurs
   - Cliquez avec le bouton droit sur le port du collecteur *DemoAssetUpload* dans la vue Collecteur et sélectionnez l'opération Démarrer. Comme les collecteurs de test sont exécutés pendant peu de temps et qu'ils s'arrêtent rapidement, l'état du port du collecteur devient brièvement « actif », puis il redevient « inactif ».
   - Attendez une ou deux minutes jusqu'à ce que les données d'actifs soient chargées dans Sentinel, générées dans une assignation par le service d'assignation et distribuées aux gestionnaires de collecteurs. Vous saurez que cela est terminé, en cherchant un évènement interne RefreshingMapFromServer avec « Actif » dans le message d'évènement. Pour voir cet évènement interne, vous devez utiliser Active View avec un filtre permettant le passage d'évènements internes (par ex, PUBLIC::Internal_Events). Le filtre PUBLIC::External_Events ne permet pas le passage d'évènements internes.
   - Cliquez avec le bouton droit sur le port du collecteur *DemoEvents* dans la vue Collecteur et sélectionnez l'opération Démarrer. Comme les collecteurs de test sont exécutés pendant peu de temps et qu'ils s'arrêtent rapidement, l'état du port du collecteur devient brièvement « actif », puis il redevient « inactif ».

- Pour vérifier la réalisation des assignations d'actifs d'évènement, double-cliquez sur un évènement (sur la table d'évènements en bas de l'Active View) qui vient d'être généré par le collecteur DemoEvents pour afficher les détails de l'évènement. Dans les détails de l'évènement affichés, à gauche de la table d'évènements, agrandissez le groupe Actif pour afficher les données de l'assignation d'actifs de l'évènement. Veuillez noter que l'affichage de l'évènement sur l' Active View peut durer une minute après l'exécution du collecteur.

8. Pour exécuter un collecteur afin de tester la détection d'exploits (il faut que vous ayez installé le composant Advisor) :
   - Exécutez le téléchargement d'alimentation de l'Advisor (qui peut durer un certain temps) :

   Sous Windows :

   - Loguez-vous sur la machine où l'Advisor est installé. Exécutez la tâche planifiée Advisor (*Démarrer > Panneau de Configuration > Tâches Planifiées > {e-Security_Advisor | at1}*)

   Sur UNIX :

   - Loguez-vous sur la machine où l'Advisor est installé comme utilisateur esecadm et exécutez :

     ```
     $ESEC_HOME/sentinel/bin/advisor.sh
     ```

   - Dans Sentinel Control Center, allez sur l'onglet Collecteurs.
   - Cliquez avec le bouton droit sur le port du collecteur *DemoVulnerabilityUpload* dans la vue Collecteur et sélectionnez l'opération Démarrer. Comme les collecteurs de test sont exécutés pendant peu de temps et qu'ils s'arrêtent rapidement, l'état du port du collecteur devient brièvement « actif », puis il redevient « inactif ».
   - Attendez jusqu'à ce que les données de détection d'exploits mises à jour soient téléchargées dans le gestionnaire de collecteurs. Vous saurez que cela est terminé en cherchant un évènement interne RefreshingMapFromServer avec « IsExploitWatchlist » dans le message d'évènement. Pour afficher cet évènement interne, vous devez utiliser Active View avec un filtre permettant le passage d'évènements internes (par ex, PUBLIC::Internal_Events). Le filtre PUBLIC::External_Events ne permet pas le passage d'évènements internes. L'envoi au gestionnaire de collecteurs des données de détection d'exploits mis à jour peut durer plus d'une demi-heure, du fait que le DAS, par défaut, ne fait au maximum qu'une mise à jour des données de détection d'exploits toutes les 30 minutes.
   - Cliquez avec le bouton droit sur le port du collecteur *DemoEvents* dans la vue Collecteur et sélectionnez l'opération Démarrer. Comme les collecteurs de test sont exécutés pendant peu de temps et qu'ils s'arrêtent rapidement, l'état du port du collecteur devient brièvement « actif », puis il redevient « inactif ».
   - Pour vérifier que la détection d'exploits a bien eu lieu, double-cliquez sur un évènement (dans la table d'évènements, en bas de l'Active View) qui vient d'être généré par le collecteur DemoEvents pour afficher les détails de l'évènement. Dans les détails de l'évènement affichés à gauche de la table d'évènements, agrandissez le groupe Exploit pour afficher les données de la détection d'exploits. Certains évènements devraient s'afficher avec le champ

Vulnérabilité défini sur « 1 ». Veuillez noter que l'affichage de l'évènement sur l'Active View peut durer une minute après l'exécution du collecteur.

Configuration des collecteurs de test

Dans Sentinel v5.1.1 et les versions antérieures, les collecteurs de test ne sont pas pré-configurés lors de l'installation. Par conséquent, vous devez utilisez le générateur de collecteurs (sur une machine Windows) pour configurer les collecteurs avant qu'ils puissent être exécutés.

Dans Sentinel v5.1.2 et les versions ultérieures, ces étapes de configuration ne sont pas nécessaires, sauf si les ports du collecteur de test ont été supprimés.

Configuration du collecteur SendOneEvent

Configurer, télécharger et exécuter le collecteur Send One Event

1. Ouvrez l'application du générateur de collecteurs.
2. Cliquez sur l'onglet *Hôtes Wizard*.
3. Sélectionnez le nom d'hôte de l'ordinateur. Le nom d'hôte apparaît dans le champ en dessous du menu, en haut de l'application.
4. Double-cliquez sur *nouveau…* sous l'en-tête du nom de port.
5. Entrez un nom de port Wizard (par ex. SendOneEvent).
6. Pour le type Rx/Tx, sélectionnez *Aucun*.
7. Laissez la valeur Rx/Tx vide.
8. Sur la même ligne, cliquez sur le menu déroulant de la colonne Collecteur et sélectionnez SendOneEvent.
9. Cliquez sur *Enregistrer*.
10. Cliquez sur l'onglet *Collecteurs*.
11. Agrandissez le collecteur SendOneEvent.
12. Cliquez avec le bouton droit sur le fichier modèle SendOneEvent et cliquez sur *Générer Scripts*.
13. Cliquez avec le bouton droit sur le collecteur SendOneEvent et cliquez sur *Télécharger collecteur*.
14. Sous l'onglet Collecteurs, votre ordinateur devrait être sélectionné. Cliquez sur *Télécharger*.
15. À l'invite, entrez le mot de passe du gestionnaire de collecteurs.
16. Cliquez sur *OK*.

Configuration du collecteur SendMultipleEvents

Configurer, télécharger et exécuter le collecteur Send Multiple Events

1. Ouvrez l'application du générateur de collecteurs.
2. Cliquez sur l'onglet *Hôtes Wizard*.
3. Sélectionnez le nom d'hôte de l'ordinateur. Le nom d'hôte apparaît dans le champ en dessous du menu, en haut de l'application.

4. Double-cliquez sur nouveau… sous l'en-tête du nom de port et insérez un nom de port Wizard (par ex. SendMultipleEvents).
5. Sur la même ligne, cliquez sur le menu déroulant de la colonne Type Rx/Tx et sélectionnez Archiver tout.
6. Sur la même ligne, cliquez sur la zone de texte de la colonne Valeur Rx/Tx et entrez le chemin vers le fichier d'entrées :

   ```
   Elements\SendMultipleEvents\config\test_events.csv
   ```

7. Sur la même ligne, cliquez sur le menu déroulant de la colonne Collecteur et sélectionnez SendMultipleEvents.
8. Cliquez sur *Enregistrer*.
9. Cliquez sur l'onglet *Collecteurs*.
10. Agrandissez le collecteur SendMultipleEvent.
11. Cliquez avec le bouton droit sur le fichier modèle SendMultipleEvents et cliquez sur *Générer Scripts*.
12. Cliquez avec le bouton droit sur le collecteur SendMultipleEvents et cliquez sur *Télécharger collecteur*.
13. Sous l'onglet Collecteurs, votre ordinateur devrait être sélectionné. Cliquez sur *Télécharger*.
14. À l'invite, entrez le mot de passe du gestionnaire de collecteurs.
15. Cliquez sur *OK*.

Configuration du collecteur DemoEvents

Configurer, télécharger et exécuter le collecteur DemoEvents

1. Ouvrez l'application du générateur de collecteurs.
2. Cliquez sur l'onglet Hôtes Wizard.
3. Sélectionnez le nom d'hôte de l'ordinateur. Le nom d'hôte apparaît dans le champ en dessous du menu, en haut de l'application.
4. Double-cliquez sur nouveau… sous l'en-tête du nom de port et entrez un nom de port Wizard (par ex. DemoEvents).
5. Sur la même ligne, cliquez sur le menu déroulant de la colonne Type Rx/Tx et sélectionnez Archiver tout.
6. Sur la même ligne, cliquez sur la zone de texte de la colonne Valeur Rx/Tx et entrez le chemin vers le fichier d'entrées :

   ```
   Elements\DemoEvents\data\Generic_Events.csv
   ```

7. Sur la même ligne, cliquez sur le menu déroulant de la colonne Collecteur et sélectionnez DemoEvents.
8. Cliquez sur *Enregistrer*.
9. Cliquez sur *Télécharger*.
10. Sélectionnez l'onglet Collecteurs.
11. Cliquez sur la flèche bas et sélectionnez le collecteur DemoEvents.
12. Cliquez sur *Télécharger*.

13. À l'invite, entrez le mot de passe du gestionnaire de collecteurs.
14. Cliquez sur *OK*.

Configuration du collecteur DemoAssetUpload

Configurer, télécharger et exécuter le collecteur DemoAssetUpload

1. Ouvrez l'application du générateur de collecteurs.
2. Cliquez sur l'onglet Hôtes Wizard.
3. Sélectionnez le nom d'hôte de l'ordinateur. Le nom d'hôte apparaît dans le champ en dessous du menu, en haut de l'application.
4. Double-cliquez sur *nouveau…* sous l'en-tête du Nom de port et entrez un Nom de port Wizard (par ex. DemoAssetUpload).
5. Sur la même ligne, cliquez sur le menu déroulant de la colonne Type Rx/Tx et sélectionnez Archiver tout.
6. Sur la même ligne, cliquez sur la zone de texte de la colonne Valeur Rx/Tx et entrez le chemin vers le fichier d'entrées :

   ```
   Elements\DemoAssetUpload\data\asset_info.csv
   ```

7. Sur la même ligne, cliquez sur le menu déroulant de la colonne Collecteur et sélectionnez DemoAssetUpload.
8. Cliquez sur *Enregistrer*.
9. Cliquez sur *Télécharger*.
10. Sélectionnez l'onglet Collecteurs.
11. Cliquez sur la flèche bas et sélectionnez DemoAssetUpload.
12. Cliquez sur *Télécharger*.
13. À l'invite, entrez le mot de passe du gestionnaire de collecteurs.
14. Cliquez sur *OK*.

Configuration du collecteur DemoVulnerabiltyUpload

Configurer, télécharger et exécuter le collecteur DemoVulnerabiltyUpload

1. Ouvrez l'application du générateur de collecteurs.
2. Cliquez sur l'onglet Hôtes Wizard.
3. Sélectionnez le nom d'hôte de l'ordinateur. Le nom d'hôte apparaît dans le champ en dessous du menu, en haut de l'application.
4. Double-cliquez sur *nouveau…* sous l'en-tête du nom de port et entrez un nom de port Wizard (par ex. DemoVulnerabiltyUpload).
5. Sur la même ligne, cliquez sur le menu déroulant de la colonne Type Rx/Tx et sélectionnez Archiver tout.
6. Sur la même ligne, cliquez sur la zone de texte de la colonne Valeur Rx/Tx et entrez le chemin vers le fichier d'entrées :

   ```
   Elements\DemoVulnerabiltyUpload\data\vuln_info.csv
   ```

7. Sur la même ligne, cliquez sur le menu déroulant de la colonne Collecteur et sélectionnez DemoVulnerabiltyUpload.

8. Cliquez sur *Enregistrer*.
9. Cliquez sur *Télécharger*.
10. Sélectionnez l'onglet Collecteurs.
11. Cliquez sur la flèche bas et sélectionnez DemoVulnerabiltyUpload.
12. Cliquez sur *Télécharger*.
13. Entrez le mot de passe du gestionnaire de collecteurs.
14. Cliquez sur *OK*.

13 Modifications de la couche de communication (iSCALE)

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

La couche de communication (iSCALE) qui connecte tous les composants de l'architecture est une connexion basée sur TCP/IP codé. Par défaut, cette communication est codée à l'aide de AES à 256 bits. ARC4 est disponible pour l'utilisation.

Le programme keymgr vous permet de choisir la méthode de codage à utiliser et de modifier la clé. Ce programme génère un fichier dans le répertoire lib de l'installation Sentinel ($ESEC_HOME/lib ou %ESEC_HOME%\lib) nommé .keystore. Ce fichier doit être copié dans chaque machine où un composant Sentinel est installé.

Sentinel recommande, à titre de bonne pratique, que la clé de sécurité par défaut soit modifiée afin d'obtenir des paramètres de codage et d'authentification uniques.

REMARQUE : Si vous utilisez Advisor, DBConnector ou un connecteur RDEP Collector, vous devez mettre à jour les mots de passe stockés dans chaque fichier de configuration de ces composants. Ce processus est nécessaire parce que la clé de codage utilisée pour codifier le mot de passe, avant qu'il ne soit stocké dans ces fichiers de configuration, est basée sur la clé dans le fichier .keystore qui a été mis à jour.

Modifications de la clé de codage

Modifications de la clé ou activation d'autres méthodes de codage

1. Pour UNIX, loguez-vous comme utilisateur esecadm. Pour Windows, loguez-vous comme utilisateur doté de droits administratifs.
2. cd vers :

   Pour Windows :

   ```
   %ESEC_HOME%\lib
   ```

   Pour UNIX :

   ```
   $ESEC_HOME/lib
   ```

3. Exécutez la commande suivante :

   Sous Windows :

   ```
   "%ESEC_JAVA_HOME%\java" -jar keymgr.jar --keyalgo
      <encryption [AES ou ARC4]> --keysize 256
   ```

Sur UNIX :

```
$ESEC_JAVA_HOME/java -jar keymgr.jar --keyalgo
   <encryption [AES or ARC4]> --keysize 256
```

Cette procédure vous permet de configurer la méthode de codage. Un fichier nommé .keystore va être créé dans le répertoire lib.

4. Copiez .keystore dans chaque machine où un composant Sentinel est installé. Le fichier doit être copié dans :

   Pour Windows :

   ```
   %ESEC_HOME%
   ```

   Pour UNIX :

   ```
   $ESEC_HOME
   ```

5. Si vous avez le connecteur DBConnector ou le connecteur RDEP Collector configuré sur une des machines du gestionnaire de collecteurs, vous devez mettre à jour les mots de passe dans toutes les instances du fichier de configuration du connecteur. Ce processus est nécessaire parce que la clé de codage utilisée pour codifer le mot de passe. avant qu'il ne soit stocké dans le fichier de configuration du connecteur, est basée sur la clé dans le fichier .keystore qui vient d'être mis à jour. Pour lire les instructions sur la configuration des mots de passe dans les fichiers de configuration de connecteurs, voir la documentation concernant le connecteur DBConnector et le connecteur RDEP.
6. Si vous exécutez Advisor en mode de téléchargement direct sur le système, vous devez mettre à jour le mot de passe codé Advisor stocké dans le fichier de configuration de l'Advisor. Ce processus est nécessaire parce que la clé de codage utilisée pour codifier le mot de passe, avant qu'il ne soit stocké dans le fichier de configuration de l'Advisor, est basée sur la clé dans le fichier .keystore qui vient d'être mis à jour. La mise à jour du mot de passe Advisor codifié n'est pas applicable si vous exécutez l'Advisor dans une configuration indépendante, parce que, dans ce mode-là, le mot de passe n'est pas stocké dans le fichier de configuration Advisor. Pour mettre à jour votre mot de passe Advisor codifié et stocké dans le fichier de configuration Advisor, effectuez les étapes suivantes dans l'ordre indiqué ci-dessous :

   - Pour UNIX, loguez-vous comme utilisateur esecadm ou pour Windows, loguez-vous comme utilisateur doté de droits administratifs. Loguez-vous sur la machine où l'Advisor est installé.
   - Changez les répertoires en :

   Pour UNIX :

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

   Pour Windows :

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

   - Entrez les commandes suivantes :

   Pour UNIX :

   ```
   ./adv_change_passwd.sh <nouveau_mot_de_passe>
   ```

   Pour Windows :

   ```
   adv_change_passwd.bat <nouveau_mot_de_passe>
   ```

14 Ajout de composants sur une installation existante

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Le programme d'installation Sentinel 5 Enterprise Security Management prend en charge l'ajout de composants Sentinel sur une installation existante. L'ajout d'un composant est utile, par exemple, si sur une machine vous avez seulement installé le gestionnaire de collecteurs Wizard et que, plus tard, vous aimeriez aussi installer Sentinel Control Center sur cette machine. Dans ce cas, vous voudriez ajouter le composant Sentinel Control Center sur l'installation du gestionnaire de collecteurs Wizard.

REMARQUE : Avant d'ajouter un composant, vérifiez que vous avez bien l'ensemble correct des variables Sentinel .

```
ESEC_HOME
ESEC_JAVA_HOME
WORKBENCH_HOME
ESEC_CONF_FILE
ESEC_VERSION
ESEC_USER
LD_LIBRARY_PATH
```

Ajout de composants sous Solaris ou Linux

Ajout de composants sous Solaris

1. Loguez-vous comme utilisateur root.
2. Insérez et montez le CD d'installation de Sentinel.
3. Démarrez le programme d'installation en accédant au répertoire d'installation sur le CD-ROM et entrez :

   ```
   ./setup.sh
   ```

   ou

   ```
   ./setup.sh –console (si X Windows n'est pas
      disponible)
   ```

4. Un message s'affiche indiquant l'emplacement de l'installation précédente et les composants déjà installés. Cliquez sur *Suivant.*
5. Choisissez les composants à ajouter, puis cliquez sur *Suivant*.
6. Suivez les invites et entrez les informations adéquates. Pour plus d'informations sur une invite spécifique, consultez le chapitre d'installation correspondant.

Ajout de composants sous Windows

Ajout de composants sous Windows

1. Insérez le CD d'installation Sentinel dans l'unité de CD-ROM.
2. Parcourez le CD et double-cliquez sur setup.bat.

   REMARQUE : l'installation en mode de console n'est pas prise en charge sous Windows.
3. Cliquez *Suivant* sur l'écran d'accueil.
4. Acceptez l'accord de licence utilisateur final et cliquez sur *Suivant*.
5. Un message s'affiche indiquant l'emplacement de l'installation précédente et les composants déjà installés. Cliquez sur *Suivant*.
6. Choisissez les composants à ajouter, puis cliquez sur *Suivant*.
7. Suivez les invites et entrez les informations adéquates. Pour plus d'informations sur une invite spécifique, consultez le chapitre 3 (pour Solaris), le chapitre 4 (pour Linux) ou le chapitre 5 (pour Windows).

15 Désinstallation de logiciel

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Désinstallation de Sentinel, du gestionnaire de collecteur et de l'Advisor

Désinstallation pour Solaris sous Linux

Démarrage du programme de désinstallation Sentinel pour Solaris

1. Loguez-vous comme utilisateur root.
2. Arrêtez le serveur Sentinel
3. cd vers :

   ```
   $ESEC_HOME/_uninst
   ```

4. Entrez :

   ```
   ./uninstall.bin
   ```

REMARQUE : sous Solaris et Linux, après avoir désinstallé le serveur Sentinel, vous devez déplacer manuellement l'utilisateur esecadm du SE, si vous le souhaitez.

Désinstallation sous Windows

Utilisation du programme de désinstallation Sentinel Windows

1. Loguez-vous comme Administrateur.
2. Arrêtez le serveur Sentinel
3. Sélectionnez Démarrer > Fichiers de programme > Sentinel > Désinstaller Sentinel 5.x.

Suivez les invites d'écran. Sélectionnez les applications à désinstaller :

- base de données
- serveur de communication (bus de message)
- Advisor
- services Sentinel de base
- corrélation
- DAS
- service de collecteur (gestionnaire de collecteurs)
- Sentinel Control Center
- gestionnaire de données Sentinel (SDM)

- HP OpenView Service Desk
- Remedy Integration

Désinstallation à l'aide du panneau de configuration

Pour désinstaller les applications Sentinel Windows

1. Cliquez sur *Démarrer* > *Programmes* > *Paramètres* > *Panneau de configuration* > *Ajouter/déplacer programmes*
2. Cliquez sur *Sentinel 5.x.*
3. Suivez les invites Une invite s'affiche demandant l'application à désinstaller. Sélectionnez les applications que vous voulez désinstaller.

Post-désinstallation

La désinstallation laisse quelques fichiers sur la machine, vous devez les supprimer manuellement après la désinstallation de Sentinel 5. Vous devez, éventuellement, supprimer le répertoire $ESEC_HOME ou %ESEC_HOME% et tous les sous-répertoires. Pour l'Advisor, vous devez éliminer les dossiers d'attaque et d'alerte utilisés pour les fichiers de données de l'Advisor.

Certains fichiers subsistent, à savoir :

- fichiers journaux Sentinel
- fichiers journaux Wizard
- fichiers journaux DAS
- fichiers journaux du gestionnaire de collecteurs

Parfois, après la désinstallation, les paramètres du système subsistent. Consultez l'*Annexe E* pour voir les procédures d'élimination manuelle des paramètres du système qui subsistent.

A Questionnaire de préinstallation

REMARQUE : pour les utilisateurs MS SQL 2000, la taille de l'évènement ne peut pas dépasser 8 Ko.

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Questions sur la préinstallation

1. Après avoir déterminer la machine qui est votre machine DAS, vérifiez qu'elle correspond aux configurations SE et matérielles requises :
   a. Procurez-vous le numéro ID hôte de la machine DAS.
   b. Contactez Novell pour vous procurer la clé de licence.
2. Quel est votre but ou objectif en utilisant Novell Sentinel ?
   a. Conformité
   b. SEM
   c. Autre_____
3. Quelle est l'architecture de réseau pour les périphériques source, en ce qui concerne le segment sécurité où le matériel Sentinel/Wizard doit être localisé ?

   REMARQUE : ceci est important pour comprendre la hiérarchie de collecte de données de l'assistant et pour identifier des pare-feux qui doivent être pénétrés pour permettre la communication entre Wizard et Sentinel, ou Sentinel et la BD ou encore Crystal Server et la BD.

   Entrez les informations ci-dessous (texte e/ou figure) ou un lien vers l'information.

4. Quels rapports voulez-vous que le système vous donne ? Ceci est important pour vérifier que les collecteurs collectent les données correctes à transmettre à la base de données Sentinel.
   a. _____
   b. _____
   c. _____
   d. _____
   e. _____
   f. _____
5. De quels périphériques source voulez-vous collecter des données (IDS, HIDS, routeurs, pare-feux, etc.), des taux d'évènements (EPS – évènements par seconde), des versions, des méthodes de connexion, des plates-formes et des correctifs ?

Périphérique (mfr/modèle)	**Taux d'évènements (EPS)**	**Version**	**Méthode de connexion**	**Plate-forme**	**Correctifs**

   Pouvez-vous fournir des données d'exemple concernant ce que les collecteurs Sentinel doivent collecter et analyser pour vous ? Cela est important pour que Sentinel puisse vous fournir ce que vous voulez ?
6. Quels modèles/standards de sécurité existent sur votre site ?
   - Quelle est votre position sur les comptes locaux versus l'authentification de domaine ?
     - Pour Windows avec authentification de domaine, des paramètres spécifiques de compte de domaine doivent être créés afin de garantir que Sentinel peut bien être installé.
     - Cela ne s'applique pas aux installations Solaris. Toutefois, Sentinel 5 ne prend pas en charge NIS.
7. Quel matériel a été alloué pour installer Sentinel ? Est-il conforme aux spécifications matérielles mentionnées aux chapitres 1 et 2 du Guide d'installation ?
8. Quelle est la rétention de données requise en terme de jours ? Normalement, 30 jours est un nombre adéquat. MS SQL a des difficultés avec plus de 60 jours. Oracle est OK.

9. Selon les informations concernant la rétention de données et les EPS, quelle est la taille du disque que vous allez utiliser ? Comptez 500 à 800 octets/évènement pour les prévisions de taille.
10. Avez-vous validé les configurations Sentinel requises pour l'opération par rapport à votre configuration, comme mentionné aux chapitres 1 et 2 du Guide d'installation ?
    - niveaux de correctif SE
    - correctifs de service
    - Hot Fix, etc.

B Maintenance préinstallation et post-installation pour la base de données Oracle sous Solaris

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Liste de contrôle de préinstallation

La liste de contrôle de préinstallation concerne en priorité les installations distribuées. Elle peut toutefois être utilisée pour des installations indépendantes. Si le nombre d'instances du gestionnaire de collecteurs et du moteur de corrélation est supérieur à trois, veuillez les noter. Cette liste de contrôle n'autorise qu'un maximum de trois instances de gestionnaire de collecteurs et de moteur de corrélation.

Pour plus d'informations, voir le *Chapitre 3, Installation de Sentinel 5 pour Oracle*.

	Variable de configuration			
1.	*Version Sentinel :*			*Date du jour :*
	Système d'exploitation			
	▪ SE correct pour BD	□ :Oui |□ : Non	▪ correctif adéquat	□ :Oui |□ : Non
	▪ BD Oracle correcte avec partitionnement	□ :Oui |□ : Non	▪ correctif adéquat	□ :Oui |□ : Non
	▫ Version		▫ niveau de correctif	
	▪ Copie de la remarque Oracle 148673.1	□ :Oui |□ : Non		
	▪ ensemble de variables d'environnement correct pour utilisateur du SE Oracle	□ :Oui |□ : Non		
	▪ SE correct pour composants Sentinel	□ :Oui |□ : Non	▪ correctif adéquat	□ :Oui |□ : Non
2.	*Machine DAS*			
	▪ ID hôte			
	▪ numéro de série			
	▪ clé de licence			
3.	*Installation DAS*			
	▪ nom d'hôte BD ou IP			par défaut : ESEC
	▪ nom base de données			par défaut : 1521
	▪ port de base de données			
	▪ emplacement fichier JDBC			

	Variable de configuration			
4.	*Valeurs Kernel UNIX pour Oracle. Ci-dessous valeurs min.*			
	▪ shminfo_shmmax	4294967295	□ :Oui |□ : Non	valeur si sup. :
	▪ shminfo_shmmin	1	□ :Oui |□ : Non	valeur si sup. :
	▪ shminfo_shmseg	50	□ :Oui |□ : Non	valeur si sup. :
	▪ shminfo_shmmni	400	□ :Oui |□ : Non	valeur si sup. :
	▪ seminfo_semmns	14000	□ :Oui |□ : Non	valeur si sup. :
	▪ seminfo_semmni	1024	□ :Oui |□ : Non	valeur si sup. :
	▪ seminfo_semmsl	1024	□ :Oui |□ : Non	valeur si sup. :
	▪ seminfo_shmopm	100	□ :Oui |□ : Non	valeur si sup. :
	▪ seminfo_shmvmx	32767	□ :Oui |□ : Non	valeur si sup. :
5.	*Instance base de données (SID)*			
6.	*Nom base de données*			
7.	*Composants Sentinel :*			
	▪ base de données Sentinel (IP ou DNS)			SE : correctif :
	▫ journal d'installation BD			
	▫ mémoire (RAM) Oracle			
	▫ nom d'instance			
	▫ port d'écoute		par défaut : 1521	
	▫ mot de passe SYS			
	▫ mot de passe SYSTÈME			
	▪ serveur de communication (iSCALE) (IP ou DNS)			SE : correctif :
	▪ services Sentinel de base (IP ou DNS)			SE : correctif :
	▪ DAS/Advisor (IP ou DNS) (l'Advisor est facultatif)			SE : correctif :
	▫ DAS RAM			
	▪ moteur de corrélation (IP et SE)			
		IP :		SE :
		IP :		SE :
		IP :		SE :

	Variable de configuration		
	▪ Crystal Server (IP ou DNS)		
	▫ MS SQL (facultatif mais recommandé)	version MS SQL : correctif MS SQL : mot de passe administrateur système ou titulaire du mot de passe :	
	▪ générateur de collecteurs (IP ou DNS) (une seule installation recommandée)		
	▪ gestionnaire de collecteurs (services de collecteur)	**REMARQUE** : le gestionnaire de collecteurs peut être défini sans mot de passe.	
	▫ IP : ▫ IP : ▫ IP :	MP : MP : MP :	SE : SE : SE :
8.	*Advisor (facultatif)*		
	▪ emplacement fichier alimentation données		
	▪ Advisor adresse expéditeur		
	▪ Advisor adresse destinataire		
	▪ nom d'utilisateur et mot de passe	n/u :	MP :
9.	*Emplacements fichier de base de données :*		
	▪ fichiers de données		
	▪ fichiers d'index		
	▪ fichiers de données récapitulatifs		
	▪ fichiers d'index récapitulatifs		
	▪ Création temporaire et annulation de fichiers d'espace de table		
	▪ journal des répétitions du répertoire du membre A		
	▪ journal des répétitions du répertoire du membre A		
10.	*Taille de la base de données :*		
	▪ standard (20 Go)		
	▪ grande (400 Go)		
	▪ personnalisée (taille)		
11.	*Serveur SMTP (DNS ou IP)*		

	Variable de configuration		
12.	*Mots de passe utilisateur*		
	▪ esecadm	MP :	
	▫ répertoire privé		par défaut : /export/home
	▪ esecapp	MP :	
	▪ esecdba	MP :	
	▪ esecrpt	MP :	

Maintenance post-installation

Des utilitaires vous permettent de réaliser périodiquement la maintenance de la base de données. Ces utilitaires comprennent les éléments suivants :

- l'analyse de partitions, qui regroupe les statistiques de partition des partitions récemment remplies.
- l'analyse de tables, qui regroupe les statistiques globales de table pour les évènements et les tables d'évènements associés.
- la vérification de l'état de santé de la base de données, qui regroupe des informations de la base de données. Elle peut :
  - vérifier que l'instance de la base de données est bien active.
  - vérifier que le processus d'écoute Oracle est bien actif.
  - afficher l'utilisation de l'espace.
  - chercher des index inutilisables.
  - chercher des objets de base de données invalides.
  - chercher des analyses de base de données.

Pour plus d'informations, lire la section *Bonnes pratiques de maintenance* au *chapitre 2*, intitulé *Bonnes pratiques*.

Une application dénommée Sentinel Data Manager est fournie avec Sentinel. Utilisez cette application pour effectuer la gestion de bases de données. Pour plus d'informations, voir *le guide de l'utilisateur Sentinel, chapitre 10* intitulé *Sentinel Data Manager.*

C Maintenance préinstallation et post-installation pour la base de données Oracle sous Linux

REMARQUE : le terme « agent » est échangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Liste de contrôle de préinstallation

La liste de contrôle de préinstallation concerne en priorité les installations distribuées. Elle peut toutefois être utilisée pour des installations indépendantes. Si le nombre d'instances du gestionnaire de collecteurs et du moteur de corrélation est supérieur à trois, veuillez les noter. Cette liste de contrôle n'autorise qu'un maximum de trois instances de gestionnaire de collecteurs et de moteur de corrélation.

Pour plus d'informations, voir le *Chapitre 3 – Installation de Sentinel 5 pour Oracle*.

	Variable de configuration			
1.	*Version Sentinel :*			*Date du jour :*
	Système d'exploitation			
	▪ SE correct pour BD	Î: Oui | Î: Non	▪ correctif adéquat	Î: Oui | Î: Non
	▫ Version		▫ Niveau de correctif	
	▪ BD Oracle correcte avec partitionnement	Î: Oui | Î: Non	▪ correctif adéquat	Î: Oui | Î: Non
	▫ Version		▫ niveau de correctif	
	▪ ensemble de variables d'environnement correct pour utilisateur du SE Oracle	Î: Oui | Î: Non		
	▪ script de démarrage (machine BD)	Î: Oui | Î: Non		
	▪ processus (machine BD)	Î: Oui | Î: Non		
	▪ sockets	Î: Oui | Î: Non		
	▪ SE correct pour composants Sentinel	Î: Oui | Î: Non	▪ correctif adéquat	Î: Oui | Î: Non
2.	*Machine DAS*			
	▪ ID hôte			
	▪ numéro de série			
	▪ clé de licence			
3.	*Installation DAS*			
	▪ nom d'hôte BD ou IP			

	Variable de configuration			
	▪ nom base de données			par défaut : ESEC
	▪ port de base de données			par défaut : 1521
	▪ emplacement fichier JDBC			
4.	*Valeurs Kernel UNIX pour Oracle. Ci-dessous valeurs min.*			
	▪ shmmax	2147483648	☐: Oui | ☐: Non	valeur si sup. :
	▪ shmmin	1	☐: Oui | ☐: Non	valeur si sup. :
	▪ shmseg	4096	☐: Oui | ☐: Non	valeur si sup. :
	▪ shmmni	400	☐: Oui | ☐: Non	valeur si sup. :
	▪ semmns	500	☐: Oui | ☐: Non	valeur si sup. :
	▪ semmni	1024	☐: Oui | ☐: Non	valeur si sup. :
	▪ semmsl	1024	☐: Oui | ☐: Non	valeur si sup. :
	▪ shmopm	100	☐: Oui | ☐: Non	valeur si sup. :
	▪ shmvmx	32767	☐: Oui | ☐: Non	valeur si sup. :
5.	*Instance base de données (SID)*			
6.	*Nom base de données*			
7.	*Composants Sentinel :*			
	▪ base de données Sentinel (IP ou DNS)			SE : correctif :
	▫ journal d'installation BD			
	▫ mémoire (RAM) Oracle			
	▫ nom d'instance			
	▫ port d'écoute		par défaut : 1521	
	▫ mot de passe SYS			
	▫ mot de passe SYSTÈME			
	▪ serveur de communication (iSCALE) (IP ou DNS)			SE : correctif :
	▪ services Sentinel de base (IP ou DNS)			SE : correctif :
	▪ DAS/Advisor (IP ou DNS) (l'Advisor est facultatif)			SE : correctif :
	▫ DAS RAM			

	▪ moteur de corrélation (IP et SE)			
		▫ IP :		SE :
		▫ IP :		SE :
		▫ IP :		SE :
	▪ Crystal Server (IP ou DNS) ▫ MS SQL (facultatif mais recommandé)	version MS SQL : correctif MS SQL : mot de passe admin.système ou titulaire ou mot de passe :		
	▪ générateur de collecteurs (IP ou DNS) (une seule installation recommandée)			
	▪ gestionnaire de collecteurs (services de collecteur)	**REMARQUE :** Le gestionnaire de collecteurs peut être défini sans mot de passe.		
	▫ IP : ▫ IP : ▫ IP :	n/u : n/u : n/u :	MP : MP : MP :	SE : SE : SE :
8.	*Advisor (facultatif)*			
	▪ emplacement fichier alimentation données			
	▪ Advisor adresse expéditeur			
	▪ Advisor adresse destinataire			
	▪ nom d'utilisateur et mot de passe	n/u :		MP :
9.	*Emplacements fichier de base de données :*			
	▪ fichiers de données			
	▪ fichiers d'index			
	▪ fichiers de données récapitulatifs			
	▪ fichiers d'index récapitulatifs			
	▪ Création temporaire et annulation de fichiers d'espace de table			
	▪ journal des répétitions du répertoire du membre A			
	▪ journal des répétitions du répertoire du membre A			

10.	*Taille de la base de données :*		
	▪ standard (20 Go)		
	▪ grande (400 Go)		
	▪ personnalisée (taille)		
11.	*Serveur SMTP (DNS ou IP)*		
12.	*Mots de passe utilisateur*		
	▪ esecadm	MP :	
	▫ répertoire privé		par défaut : /export/home
	▪ esecapp	MP :	
	▪ esecdba	MP :	
	▪ esecrpt	MP :	

Maintenance post-installation

Des utilitaires vous permettent de réaliser périodiquement la maintenance de la base de données. Ces utilitaires comprennent les éléments suivants :

- l'analyse de partitions, qui regroupe les statistiques de partition des partitions récemment remplies.
- l'analyse de tables, qui regroupe les statistiques globales de table pour les évènements et les tables d'évènements associés.
- la vérification de l'état de santé de la base de données, qui regroupe des informations de la base de données. Elle peut :
  - vérifier que l'instance de la base de données est bien active
  - vérifier qu'Oracle Listener est bien actif
  - afficher l'utilisation de l'espace
  - chercher des index inutilisables
  - chercher des objets de base de données invalides
  - chercher des analyses de base de données

Pour plus d'informations, lire la section *Bonnes pratiques de maintenance* au *chapitre 2* sur les bonnes pratiques.

Une application dénommée Gestionnaire de données Sentinel (Sentinel Data Manager) est fournie avec Sentinel. Utilisez cette application pour effectuer la gestion de bases de données. Pour plus d'informations, voir *le guide de l'utilisateur Sentinel, chapitre 10* intitulé *Gestionnaire de données Sentinel.*

D Maintenance préinstallation et post-installation pour la base de données MS SQL sous Windows

REMARQUE : le terme « agent » est échangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

REMARQUE : Pour les utilisateurs MS SQL 2000, la taille de l'évènement ne peut pas dépasser 8 Ko.

Liste de contrôle de préinstallation

Cette liste de contrôle de préinstallation concerne en priorité les installations distribuées. Elle peut toutefois être utilisée pour des installations indépendantes. Si le nombre d'instances du gestionnaire de collecteurs et du moteur de corrélation est supérieur à trois, veuillez les noter. Cette liste de contrôle n'autorise qu'un maximum de trois instances de gestionnaire de collecteurs et de moteur de corrélation.

Pour plus d'informations, voir le *chapitre 4*, *Installation de Sentinel 5 pour MS SQL*.

	Variable de configuration			
1.	*Version Sentinel :*			*Date du jour :*
	Système d'exploitation			
	▪ SE correct pour BD	☐: Oui | ☐: Non	▪ correctif adéquat	☐: Oui | ☐: Non
	▪ BD de SQL correcte	☐: Oui | ☐: Non	▪ correctif adéquat	☐: Oui | ☐: Non
	▫ Version		▫ niveau de correctif	
	▪ SE correct pour composants Sentinel	☐: Oui | ☐: Non	▪ correctif adéquat	☐: Oui | ☐: Non
2.	*Pour l'installation DAS sous un compte de domaine Windows, assigner « se loguer comme service »*	☐: Oui | ☐: Non		
3.	*Machine DAS*			
	▪ ID hôte			
	▪ numéro de série			
	▪ clé de licence			
4.	*nom d'hôte de la base de données ou IP*	*<nom_hôte>[\<nom_instance >]*		
5.	*Nom base de données*			par défaut : ESEC
6.	*port :*		par défaut : 1433	

	Variable de configuration		
7.	*Installation SQL*	Î: mixte Î: non mixte	
8.	*mot de passe administrateur de SQL Server ou titulaire du mot de passe :*	MP :	
9.	*Composants Sentinel :*		
	▪ base de données Sentinel (IP ou DNS)		SE : correctif :
	▪ serveur de communication (iSCALE) (IP ou DNS)		SE : correctif :
	▪ services Sentinel de base (IP ou DNS)		SE : correctif :
	▪ DAS/Advisor (IP ou DNS) (l'Advisor est facultatif)		SE : correctif :
	▪ moteur de corrélation (IP et SE)		
		IP :	SE :
		IP :	SE :
		IP :	SE :
	▪ Crystal Server (IP ou DNS)		SE : correctif :
	▫ MS SQL (facultatif mais recommandé)	version MS SQL : correctif MS SQL : mot de passe administrateur système ou titulaire du mot de passe :	
	▪ générateur de collecteurs (IP ou DNS) (une seule installation recommandée)		
	▪ gestionnaire de collecteurs (mot de passe des services de collecteur avec IP ou DNS ou SE)	REMARQUE : Le gestionnaire de collecteurs peut être défini sans mot de passe.	
	▫ IP : ▫ IP : ▫ IP :	MP : MP : MP :	SE : SE : SE :
10.	*Advisor (facultatif)*		
	▪ emplacement fichier alimentation données		
	▪ Advisor adresse expéditeur		
	▪ Advisor adresse destinataire		
	▪ nom d'utilisateur et mot de passe	n/u :	MP :

	Variable de configuration		
11.	*Emplacements fichier de base de données :*		
	▪ fichiers de données		
	▪ fichiers d'index		
	▪ fichiers de données récapitulatifs		
	▪ fichiers d'index récapitulatifs		
	▪ fichiers journaux		
12.	*Taille de la base de données :*		
	▪ standard (20 Go)		
	▪ grande (400 Go)		
	▪ personnalisée (taille)		
13.	*Serveur SMTP (DNS ou IP)*		
14.	*pour authentification SQL (mots de passe)*		
	▪ esecadm	MP :	
	▪ esecapp	MP :	
	▪ esecdba	MP :	
	▪ esecrpt	MP :	
15.	*pour authentification Windows (mots de passe)*		
	▪ DBA (login)	n/u :	
	▪ utilisateur d'application (login et mot de passe)	n/u :	MP :
	▪ administrateur Sentinel (login)	n/u :	
	▪ utilisateur de rapports Sentinel (login)	n/u :	

Maintenance post-installation

Le système d'exploitation Windows permet l'archivage automatique des données et l'ajout de partitions. Pour plus d'informations, lire la section *Archivage automatique des données et ajout de partitions*, au chapitre 2 intitulé *Bonnes pratiques*.

E Nettoyage manuel des installations précédentes

REMARQUE : le terme « agent » est interchangeable avec « collecteur ». Désormais, les agents sont dénommés collecteurs.

Si vous effectuez une nouvelle installation de Sentinel, il est VIVEMENT conseillé d'effectuer toutes les étapes suivantes pour vérifier qu'il ne reste plus de fichiers ni de paramètres système de l'installation précédente de Sentinel, qui pourraient aboutir faire échouer la toute nouvelle installation. Effectuez les étapes suivantes sur chaque machine où vous réalisez une nouvelle installation, AVANT d'exécuter le programme d'installation.

ATTENTION : ces instructions impliquent la modification des paramètres du système d'exploitation et des fichiers. Si vous n'êtes pas familiarisé avec la modification de ces paramètres de système et/ou ces fichiers, veuillez contacter l'administrateur du système.

Solaris

Nettoyage manuel de Sentinel sous Solaris

1. Loguez-vous comme utilisateur root.
2. Assurez-vous qu'il n'y a pas de processus Sentinel en cours d'exécution.
3. Supprimez le contenu de /opt/sentinelXX (ou l'emplacement où le logiciel Sentinel avait été installé et nommé).
4. Déplacez les fichiers suivants dans le répertoire /etc/rc3.d :
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (si le connecteur SDEE est installé)
5. Déplacez les fichiers suivants dans le répertoire /etc/rc0.d :
   - K01wizard
   - K02sentinel
   - K01esdee (si le connecteur SDEE est installé)
   - K01esyslogserver (v5.1.1.1)
6. Déplacez les fichiers suivants dans le répertoire /etc/init.d :
   - sentinel
   - wizard
   - esdee (si le connecteur SDEE est installé)
   - esyslogserver (v5.1.1.1)

7. Supprimez les fichiers suivants de /usr/local/bin :
   - restart_wizard.sh
   - stop_wizard.sh
   - start_wizard.sh
8. Nettoyez les références installshield dans /var/sadm/pkg. Supprimez les fichiers suivants du répertoire /var/sadm/pkg :
   - tous les fichiers qui commencent par IS (IS* sur la ligne de commande)
   - tous les fichiers qui commencent par ES (ES* sur la ligne de commande)
   - tous les fichiers qui commencent par MISCwp (MISCwp* sur la ligne de commande)
9. Supprimez l'utilisateur esecadm (et rép. privé) et le groupe esec (assurez-vous que personne n'est logué comme utilisateur esecadm avant de réaliser cette étape.
   - Exécutez : userdel -r esecadm
   - Exécutez : groupdel esec
10. Supprimez la section Installshield de /etc/profile, /etc/.login
11. Supprimez le répertoire /InstallShield, s'il en existe un.
12. Supprimez la base de données Sentinel Oracle en suivant les instructions de la section « Nettoyage manuel d'une base de données Sentinel Oracle sous Solaris ».
13. Redémarrez le système d'exploitation.

Nettoyage manuel d'une base de données Sentinel Oracle sous Solaris

1. Comme utilisateur oracle, arrêtez le processus d'écoute Oracle :
   - Exécutez : lsnrctl stop
2. Arrêtez la base de données Sentinel :
   - Passez à l'utilisateur oracle
   - Configurez la variable d'environnement ORACLE_SID pour le nom de l'instance de la base de données Sentinel (normalement, ESEC).
   - Exécutez : sqlplus '/as sysdba'
   - À l'invite sqlplus, exécutez : shutdown immediate
3. Déplacez l'entrée de la base de données Sentinel dans le fichier /var/opt/oracle/oratab.
4. Supprimez le fichier init<nom_votre_instance>.ora (normalement initESEC.ora) du répertoire $ORACLE_HOME/dbs.
5. Déplacez les entrées de la base de données Sentinel des fichiers suivants vers le répertoire $ORACLE_HOME/network/admin :
   - tnsnames.ora
   - listener.ora
6. Supprimez les fichiers de données de la base de données de l'emplacement où vous avez choisi de les installer.

Linux

Nettoyage manuel de Sentinel sous Linux

1. Loguez-vous comme utilisateur root.
2. Assurez-vous qu'il n'y a pas de processus Sentinel en cours d'exécution.
3. Supprimez le contenu de /opt/sentinelXX (ou l'emplacement où le logiciel Sentinel avait été installé et nommé).
4. Déplacez les fichiers suivants dans le répertoire /etc/rc5.d :
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (si le connecteur SDEE est installé)
5. Déplacez les fichiers suivants dans le répertoire /etc/rc3.d :
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (si le connecteur SDEE est installé)
6. Déplacez les fichiers suivants dans le répertoire /etc/rc0.d :
   - K01esyslogserver (v5.1.1.1)
   - K01wizard
   - K02sentinel
   - K01esdee (si le connecteur SDEE est installé)
7. Déplacez les fichiers suivants dans le répertoire /etc/init.d :
   - sentinel
   - wizard
   - esyslogserver (v5.1.1.1)
   - esdee (si le connecteur SDEE est installé)
8. Supprimez les fichiers suivants de /usr/local/bin :
   - restart_wizard.sh
   - stop_wizard.sh
   - start_wizard.sh
9. Supprimez le répertoire /InstallShield
10. Supprimez le fichier /root/vpd.properties
11. Supprimez l'utilisateur esecadm (et rép. privé) et le groupe esec (assurez-vous que personne n'est logué comme utilisateur esecadm avant de réaliser cette étape.
    - Exécutez : userdel -r esecadm
    - Exécutez : groupdel esec
12. Supprimez la section Installshield de /etc/profile, /etc/.login
13. Supprimez la base de données Sentinel Oracle en suivant les instructions de la section « Nettoyage manuel d'une base de données Sentinel Oracle sous Linux ».
14. Redémarrez le système d'exploitation.

Nettoyage manuel d'une base de données Sentinel Oracle sous Linux

1. Comme utilisateur oracle, arrêtez le processus d'écoute Oracle :
   - Exécutez : lsnrctl stop
2. Arrêtez la base de données Sentinel :
   - Passez à l'utilisateur oracle
   - Configurez la variable d'environnement ORACLE_SID pour le nom de l'instance de la base de données Sentinel (normalement, ESEC).
   - Exécutez : sqlplus '/as sysdba'
   - À l'invite sqlplus, exécutez : shutdown immediate
3. Éliminez l'entrée de la base de données Sentinel dans le fichier /etc/oratab
4. Supprimez le fichier init<nom_votre_instance>.ora (normalement initESEC.ora) du répertoire $ORACLE_HOME/dbs.
5. Déplacez les entrées de la base de données Sentinel des fichiers suivants vers le répertoire $ORACLE_HOME/network/admin :
   - tnsnames.ora
   - listener.ora
6. Supprimez les fichiers de données de la base de données de l'emplacement où vous avez choisi de les installer.

Windows

Nettoyage manuel de Sentinel sous Windows

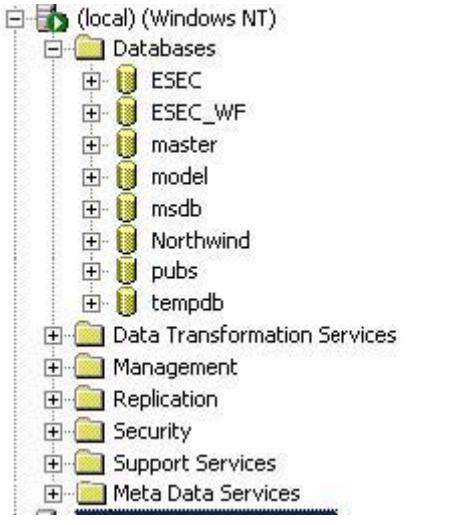
1. Supprimez le dossier C:\Program Files\Common Files\InstallShield\Universal et tout son contenu.
2. Supprimez l'ancien dossier d'installation Sentinel (par ex. C:\Program Files\sentinel [%ESEC_HOME%]).
3. Supprimez les variables d'environnement suivantes (si elles existent) en cliquant avec le bouton droit sur Poste de travail et sélectionnant Propriétés, puis en cliquant sur l'onglet Avancées et ensuite sur le bouton Variables de l'environnement.
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
4. Supprimer toutes les entrées dans la variable d'environnement PATH qui ciblent une installation précédente.

   ATTENTION : prenez soin de n'éliminer que les chemins vers les anciennes installations de Sentinel. La suppression d'autres entrées dans PATH peut provoquer un mauvais fonctionnement du système.
5. Supprimez les raccourcis Sentinel du Bureau.
6. Supprimez le dossier raccourci *Démarrer > Programmes >Sentinel* depuis le menu de démarrage.

7. Supprimez la base de données Sentinel Microsoft SQL Server en suivant les instructions dans la section *Nettoyage manuel d'une base de données Sentinel Microsoft SQL Server sous Windows*.
8. Redémarrez le système d'exploitation.

Nettoyage manuel d'une base de données Sentinel Microsoft SQL Server sous Windows

1. Ouvrez Microsoft SQL Server Enterprise Manager et connectez-vous à l'instance SQL Server où vous avez installé la base de données Sentinel.
2. Agrandissez l'arborescence Base de données et localisez la base de données Sentinel.



3. Pour chaque base de données ESEC et ESEC_WF (ou tout autre nom éventuel donné à la base de données lors de son installation), cliquez avec le bouton droit sur la base de données et sélectionnez *Supprimer*.
4. À l'invite, sélectionnez *OUI* pour supprimer la base de données.