Novell Sentinel

6.0

www.novell.com

VOLUME I - GUIDE D'INSTALLATION

Apr. 30, 2007

Novell®

Mentions légales

Novell, Inc. n'accorde aucune garantie, explicite ou implicite, quant au contenu de cette documentation, y compris toute garantie de bonne qualité marchande ou d'aptitude à un usage particulier. Novell se réserve en outre le droit de réviser cette publication à tout moment et sans préavis.

Par ailleurs, Novell exclut toute garantie relative à tout logiciel, notamment toute garantie, expresse ou implicite, que le logiciel présenterait des qualités spécifiques ou qu'il conviendrait à un usage particulier. Novell se réserve en outre le droit de modifier à tout moment tout ou partie des logiciels Novell, sans notification préalable de ces modifications à quiconque.

Tous les produits ou informations techniques fournis dans le cadre de ce contrat peuvent être soumis à des contrôles d'exportation aux États-Unis et à la législation commerciale d'autres pays. Vous vous engagez à respecter toutes les réglementations de contrôle des exportations et à vous procurer les licences et classifications nécessaires pour exporter, réexporter ou importer des éléments clés. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes d'exclusion d'exportation en vigueur aux États-Unis ou vers des pays terroristes ou soumis à un embargo par la législation américaine en matière d'exportations. Vous acceptez de ne pas utiliser les produits livrables pour le développement prohibé d'armes nucléaires, de missiles ou chimiques et biologiques. Reportez-vous à la page Web des services de commerce international de Novell (http://www.novell.com/info/exports/) pour plus d'informations sur l'exportation des logiciels Novell. Novell décline toute responsabilité dans le cas où vous n'obtiendriez pas les approbations d'exportation nécessaires.

Novell, Inc. dispose de droits de propriété intellectuelle sur la technologie intégrée dans le produit décrit dans ce document. En particulier, et sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains mentionnés sur le site Web de Novell relatif aux mentions légales (http://www.novell.com/company/legal/patents/) (en anglais) et un ou plusieurs brevets supplémentaires ou en cours d'homologation aux États-Unis et dans d'autres pays.

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

Documentation en Ligne : pour accéder à la toute dernière documentation en ligne de ce produit et des autres produits Novell, consultez la page Web de documentation Novell (http://www.novell.com/documentation).

Marques de Novell

Pour connaître les marques commerciales de Novell, reportez-vous à la liste des marques commerciales et des 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.

Tables des matières

Préface

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

La documentation technique de Sentinel se compose de cinq volumes. Il s'agit des champs suivants :

- Volume I – Guide d'installation de Sentinel™
- Volume II – Guide de l'utilisateur de Sentinel™
- Volume III – Guide de l'utilisateur de Sentinel™ Collector
- Volume IV : Guide des références utilisateur de Sentinel™5
- Volume V : Guide d'intégration de produits tiers de Sentinel™5

Volume I : Guide d'installation de Sentinel

Ce guide explique comment installer les composants suivants :

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

Volume II : Guide de l'utilisateur de Sentinel

Ce guide aborde les sujets suivants :

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

Volume III – Guide de l'utilisateur de Sentinel™ Collector

Ce guide aborde les sujets suivants :

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

Volume IV : Guide de référence utilisateur de Sentinel

Ce guide aborde les sujets suivants :

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

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

- Remedy
- HP OpenView Operations
- HP Service Desk

Introduction

1

Rubriques traitées dans ce chapitre :

Ce guide va vous accompagner lors de l'installation de base. Le guide de l'utilisateur de Sentinel 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.

1.1 Présentation de Sentinel

Solution de gestion des événements et des informations de sécurité, Sentinel™ reçoit des données de nombreuses sources réparties dans l'entreprise, les standardise, leur attribue une priorité et vous les présente pour que vous puissiez prendre des décisions en matière de stratégies, de risques et de menaces.

Sentinel automatise les processus de création de rapport, d'analyse et de collection de journaux pour garantir l'efficacité des contrôles informatiques dans le domaine des exigences d'audit et de la détection des menaces. Sentinel remplace ces processus manuels à forte intensité de main-d'œuvre par une surveillance automatisée permanente d'événements de sécurité et de conformité et des contrôles informatiques.

Sentinel collecte et corrèle les informations relatives ou non à la sécurité à partir de l'infrastructure en réseau d'une organisation, ainsi que d'applications, de périphériques et de systèmes tiers. Sentinel présente les données ainsi collectées dans une interface graphique plus sensible, identifie les problèmes de sécurité ou de conformité et assure le suivi des actions correctives, en rationalisant les processus précédemment enclins aux erreurs et en établissant un programme de gestion plus rigoureux et plus sûr.

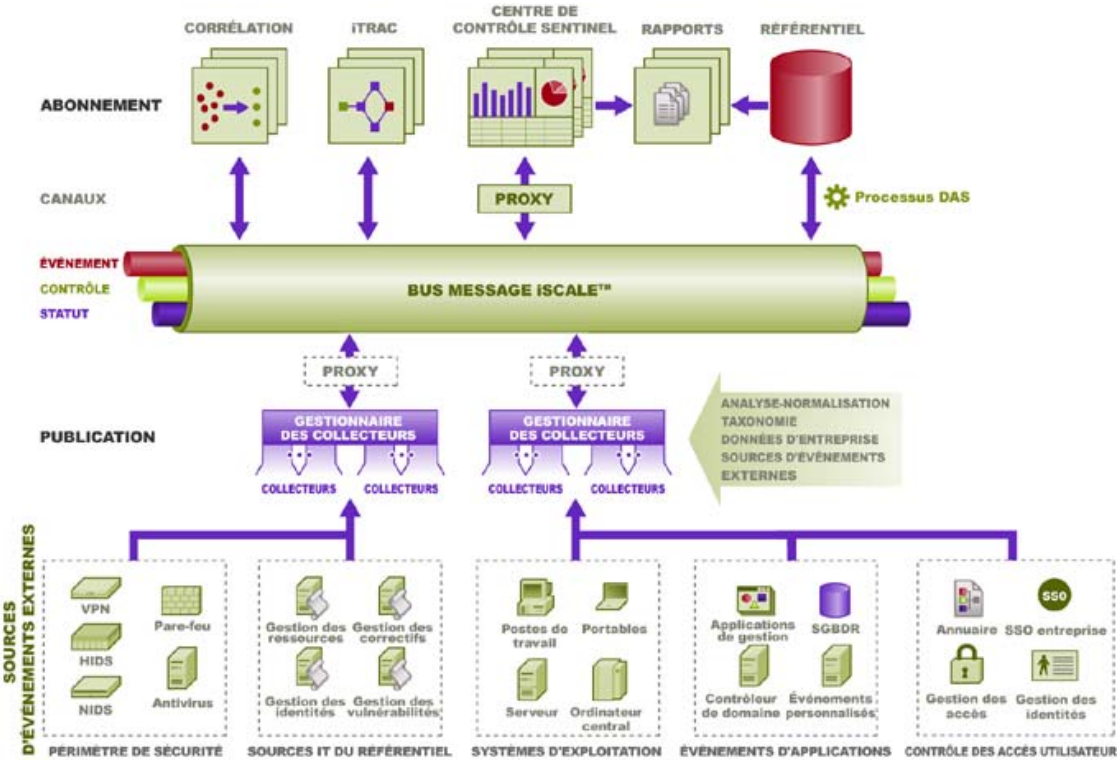
Une gestion automatisée des réponses en cas d'incidents vous permet de documenter et de formaliser le processus de suivi, de réaffectation et de réponse aux incidents et violations de stratégie et garantit

une intégration bilatérale avec des systèmes de tickets de dépannage. Sentinel permet de réagir rapidement et de résoudre les incidents efficacement.

Sentinel vous propose les fonctionnalités suivantes :

- gestion de la sécurité et surveillance de la conformité en temps réel automatisées et intégrées sur tous les systèmes et tous les réseaux ;
- infrastructure permettant aux stratégies de l'entreprise d'orienter la stratégie et l'action informatiques ;
- création de rapport et documentation automatiques portant sur la sécurité, les systèmes et les accès dans l'entreprise ;
- gestion des incidents et correction intégrées ;
- capacité d'assurer et de surveiller la conformité avec les stratégies internes et les lois gouvernementales telles que Sarbanes-Oxley, HIPAA, GLBA, FISMA, etc.

Voici un aperçu de l'architecture de Sentinel qui illustre les différents composants impliqués dans la gestion de la sécurité.



Sentinel se compose de plusieurs éléments :

- Serveur Sentinel
- Serveur de communication Sentinel
- Moteur de corrélation
- iTRAC
- Base de données Sentinel
- Gestionnaire des collecteurs Sentinel

- Collecteurs Sentinel
- Centre de contrôle Sentinel
- Générateur de collecteurs Sentinel
- collecteur de données Sentinel
- Serveur Crystal Report
- Sentinel Advisor
- Intégration de tiers
  - HP OpenView Operations
  - HP Service Desk
  - Remedy

1.1.1 Serveur Sentinel

Le serveur Sentinel se compose de plusieurs éléments qui exécutent les services clés de traitement des événements. Il s'agit notamment de recevoir des événements envoyés par les Gestionnaires de collecteurs, de les stocker dans la base de données, de procéder au filtrage, de traiter les affichages ActiveView, d'exécuter des requêtes de base de données et d'en analyser les résultats, sans oublier la gestion de tâches administratives telles que l'authentification et l'autorisation des utilisateurs.

1.1.2 Serveur de communication Sentinel

Le bus de message iSCALE peut déplacer, en une seule seconde, des milliers de paquets de messages entre les différents composants de Sentinel. Cela garantit une évolutivité indépendante des composants et une intégration basée sur les standards avec les applications externes.

1.1.3 Moteur de corrélation

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

1.1.4 Processus de travail iTRAC

Sentinel propose un système de gestion des processus de travail iTRAC permettant de définir et d'automatiser les processus de réponse en cas d'incidents. Les incidents identifiés dans Sentinel, soit manuellement soit par une règle de corrélation, peuvent être associés avec un processus de travail iTRAC.

1.1.5 Base de données Sentinel

Le produit Sentinel s'articule autour d'une base de données principale qui stocke les événements de sécurité et toutes les métadonnées de Sentinel. Les événements sont stockés sous forme normalisée, avec les données de vulnérabilité et de ressource, les informations d'identité, l'état des incidents et des processus de travail, et bien d'autres données.

1.1.6 Gestionnaire des collecteurs Sentinel

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

Le Gestionnaire des collecteurs Sentinel peut se connecter au bus de message soit directement soit via un proxy SSL.

1.1.7 Sentinel Collectors

Sentinel collecte les données de périphériques source et fournit un flux d'événements plus riche en intégrant une taxinomie, une détection d'exploitation et des données d'entreprise au flux de données avant que les événements ne soient corrélés, analysés et envoyés à la base de données. Un flux d'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.

Les collecteurs Sentinel peuvent analyser les données émanant des types de périphériques énoncés ci-après :

systèmes de détection d'intrusion (hôte)	Antivirus
systèmes de détection d'intrusion (réseau)	Serveurs Web
Pare-feux	Bases de données
Systèmes d'exploitation	Ordinateur central
surveillance de stratégie	estimation de la vulnérabilité
Authentification	Services d'annuaire
routeurs & commutateurs	Gestion réseau
VPN	systèmes propriétaires

Vous pouvez télécharger des collecteurs existants propres au périphérique à partir du site de produits Novell (http://support.novell.com/products/sentinel/collectors.html). Il est possible de générer ou de modifier des collecteurs dans le Générateur de collecteurs, une application autonome fournie avec le système Sentinel.

1.1.8 Centre de contrôle Sentinel

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
- Gestion de la source d'événements : déploiement et contrôle des collecteurs

1.1.9 Générateur de collecteurs Sentinel

Le Générateur de collecteurs Sentinel permet de générer des collecteurs. Vous pouvez créer et personnaliser les modèles pour que le collecteur puisse analyser les données.

1.1.10 Gestionnaire de données Sentinel

Le Gestionnaire de données Sentinel (SDM) permet de gérer la base de données Sentinel. Vous pouvez exécuter les opérations suivantes dans SDM :

- contrôle de l'utilisation de l'espace de la base de données ;
- affichage et gestion des partitions de la base de données ;
- gestion des archives de la base de données ;
- importation de données dans la base de données ;
- configuration de l'assignation de données ;
- configuration des noms des étiquettes d'événements ;
- configuration des paramètres des rapports récapitulatifs.

1.1.11 Serveur de création de rapport Crystal

Les services complets de création de rapport inclus dans le Sentinel Control Center sont optimisés par Crystal Enterprise Server by Business Objects™. Sentinel est fourni avec des rapports prédéfinis axés sur les demandes de création de rapport les plus courantes des organisations qui contrôlent leur situation sur le plan de la sécurité et de la conformité. Le Crystal Report Developer permet aussi de développer de nouveaux rapports personnalisés répondant au schéma d'affichage des rapports publié par Sentinel.

1.1.12 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.

1.1.13 Intégration de tiers

Sentinel utilise des plug-ins API tiers à des fins de compatibilité avec les systèmes suivants :

- HP OpenView Operations
- HP Service Desk
- Remedy AR

1.2 Prise en charge linguistique

Les composants Sentinel ont été localisés pour les langues suivantes :

- Anglais
- Portugais (Brésil)
- Français
- Italien
- Allemand
- Espagnol
- Japonais
- Chinois (traditionnel)
- Chinois (simplifié)

Il existe plusieurs exceptions :

- L'interface et le langage de script du Générateur de collecteurs n'existent qu'en anglais, mais il peut toutefois être exécuté sur les systèmes d'exploitation non anglais mentionnés ci-dessus.
- Pour l'instant, les Gestionnaires de collecteurs ne peuvent traiter que des données ASCII étendu ou non (autrement dit, pas des données Unicode ni à double octet).
- Les collecteurs créés avec Novell sont conçus pour analyser des événements anglais.
- Les événements internes (pour auditer les opérations Sentinel) sont uniquement en anglais.

1.3 Autres références Novell

Les manuels suivants sont disponibles sur le site de documentation Novell (http://www.novell.com/documentation/) :

- Guide d'installation Sentinel
- Sentinel User’s Guide (Guide de l'utilisateur de Sentinel)
- Sentinel Collector Builder User’s Guide (Guide de l'utilisateur du Générateur de collecteurs Sentinel)
- Sentinel User’s Reference Guide (Guide de référence utilisateur de Sentinel)
- Sentinel 3rd Party Integration Guide (Guide d'intégration de produits tiers de Sentinel)
- Notes de mise à jour

1.4 Contacter Novell

- Site Web : http://www.novell.com (http://www.novell.com)
- Support technique de Novell : http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- Autoassistance : http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)

- Site de téléchargement de correctifs : http://download.novell.com/index.jsp (http://download.novell.com/index.jsp)
- Support 24 h/24 et 7j/7 : http://www.novell.com/offices (http://www.novell.com/offices)

Meilleures pratiques

2

Rubriques traitées dans ce chapitre :

Ce chapitre traite des bonnes pratiques et recommandations pour mieux utiliser Sentinel.

2.1 Plates-formes prises en charge

Les composants Sentinel doivent toujours être installés sur une plate-forme prise en charge par Novell. Au moment de l'impression, Sentinel était pris en charge sur les plates-formes suivantes. Pour obtenir des informations actualisées, consultez la documentation en ligne à l'adresse http://www.novell.com/documentation (http://www.novell.com/documentation).

2.1.1 Systèmes d'exploitation

Les composants Sentinel (y compris la base de données) sont certifiés fonctionner sous les systèmes d'exploitation suivants :

- SuSE Linux Enterprise Server 9 SP2 et SP3
- SuSE Linux Enterprise Server 10 (correctif du 7/1/2006)
- Red Hat Enterprise Linux 3 Mise à jour 5 ES (x86)
- Sun Solaris 9 (groupe de correctifs recommandé DATE : 3 mai 2005)
- Sun Solaris 10
- Windows 2003 Standard ou Enterprise Edition SP1
- Windows XP SP1 (pour Sentinel Control Center, Collector Builder et Sentinel Data Manager uniquement)
- Windows 2000 SP4, Standard ou Enterprise Edition (pour Sentinel Control Center, Collector Builder et Sentinel Data Manager uniquement)

2.1.2 Bases de données

Sentinel est certifié fonctionner avec les bases de données suivantes :

- Oracle 10g Enterprise Edition (v 10.2.0.3 avec le correctif critique Oracle n° 5881721)

- Oracle 9i Enterprise Edition (v 9.2.0.7 p. 5490841)
- Microsoft SQL Server 2005 SP1 32 bits (v.9.00.2047), Standard ou Enterprise Edition
- Microsoft SQL Server 2005 64 bits (v.9.00.2047), Standard ou Enterprise Edition

---

Remarque : Toutes les bases de données doivent être installées sous un système d'exploitation dont le fonctionnement avec des composants Sentinel est certifié par le fournisseur de la base de données ainsi que par Novell. Oracle doit s'exécuter sous Linux ou Solaris (et non Windows).

2.1.3 Serveur de création de rapport

Le serveur de création de rapport pris en charge est Crystal Enterprise Server XI R2, qui peut s'exécuter sur l'une des plates-formes suivantes dans l'environnement Sentinel :

- Windows 2003 SP1 Server, Standard ou Enterprise Edition
  - Base de données Crystal sous Microsoft SQL 2005
- Red Hat Enterprise Linux 3 Mise à jour 5 ES (x86)
  - Base de données Crystal sous MySQL
- SuSE Linux Enterprise Server 9 SP2 (x86)
  - Base de données Crystal sous MySQL

2.1.4 Piles prises en charge

Novell prend en charge les composants Sentinel installés sur n'importe quel système d'exploitation pris en charge, et l'environnement peut être mixte (Linux, Solaris et Windows), avec les quelques exceptions et avertissements suivants :

- Générateur de collecteurs - ne s'exécute que sur des plates-formes Windows.
- Crystal Enterprise Server
  - Ne peut pas s'exécuter sous Solaris
  - Ne peut pas s'exécuter sous Windows 2000 dans un environnement Sentinel
  - Ne peut pas s'exécuter avec MSDE comme base de données dans un environnement Sentinel
- Base de données
  - Doit être SQL Server si Sentinel Server est sous Windows
  - Doit être Oracle si Sentinel Server est sous Linux ou Solaris (pas Windows)
  - Oracle sous Windows n'est pas pris en charge dans l'environnement Sentinel
- Data Access Service (DAS)
  - L'authentification Windows ne peut pas être utilisée si DAS est installé dans un environnement mixte dans lequel DAS est sous Windows et la base de données est de type Oracle ou dans lequel DAS est sous UNIX ou Linux et la base de données est de type SQL Server.

2.2 Recommandations matérielles

Lors de l'installation sous Linux ou Windows, les composants serveur et base de données Sentinel peuvent s'exécuter sur du matériel x86 (32 bits) ou x86-64 (64 bits), y compris les processeurs AMD Opteron et Intel Xeon. Les serveurs Itanium ne sont pas pris en charge.

Pour Solaris, l'architecture SPARC est prise en charge.

2.2.1 Architecture

L'architecture de Sentinel est hautement évolutive et, si des taux d'événements élevés sont prévus, les composants peuvent être répartis sur plusieurs machines pour obtenir les meilleures performances du système.

De nombreux facteurs doivent être pris en considération lors de la conception d'un système Sentinel. Voici une liste partielle de facteurs à prendre en considération lors de la conception d'un système :

- Taux d'événements (événements par seconde ou EPS)
- Emplacement géographique/réseau des sources d'événements et largeur de bande entre les réseaux
- Matériel disponible
- Systèmes d'exploitation de prédilection
- Projets d'évolutivité
- Niveau prévu de filtrage d'événements
- Stratégies locales de rétention des données
- Exigences en matière de nombre et de complexité des règles de corrélation
- Nombre prévu d'incidents par jour
- Nombre prévu de processus de travail qui seront gérés par jour
- Nombre d'utilisateurs se loguant au système
- Vulnérabilité et organisation des ressources

Le principal facteur dans la conception d'un système Sentinel est le taux d'événements – en effet, une augmentation des taux d'événements affecterait pratiquement tous les composants de l'architecture Sentinel. Dans un environnement où le taux d'événements est élevé, le composant le plus sollicité est la base de données qui est très dépendante des E/S et peut tout aussi bien gérer simultanément des insertions de centaines voire de milliers d'événements par seconde, des objets créés par plusieurs utilisateurs, des mises à jour des processus de travail, des requêtes historiques simples émanant de Sentinel Control Center et des rapports à long terme provenant de Crystal Enterprise Server. Novell formule donc les recommandations suivantes :

- La base de données doit être installée sans aucun autre composant Sentinel.
- Le serveur de la base de données doit être dédié aux activités Sentinel. D'autres applications (ou processus ETL) peuvent affecter les performances de la base de données.
- Le serveur de base de données requiert une pile de disques haute vitesse répondant aux exigences d'E/S basées sur les taux d'insertion d'événements.

- Un administrateur de base de données spécialisé doit évaluer régulièrement les aspects suivants de la base de données :
  - Taille
  - Activités E/S
  - Espace disque
  - Mémoire
  - Indexer

Dans les environnements à faible taux d'événements (par exemple, EPS < 25), les recommandations ci-dessus peuvent être moins strictes, car la base de données et les autres composants utiliseront moins de ressources.

Cette section inclut des recommandations matérielles générales destinées à vous aider à concevoir un système Sentinel. En général, les recommandations en termes de conception sont basées sur des plages de taux d'événements. Elles sont toutefois basées sur les suppositions suivantes :

- Le taux d'événements tend vers la limite supérieure de la plage EPS.
- La taille moyenne des événements est de 600 octets.
- Tous les événements sont stockés dans la base de données (autrement dit, il n'existe aucun filtre permettant d'éliminer certains événements).
- L'équivalent de trente jours de données est stocké en ligne dans la base de données.
- L'espace de stockage pour les données Advisor n'est pas repris dans les spécifications ci-dessous.
- Sentinel Server dispose d'un espace disque par défaut de 5 Go pour le caching temporaire des données d'événements dont l'insertion dans la base de données n'a pas abouti.
- Sentinel Server dispose également d'un espace disque par défaut de 5 Go pour les événements qui ne peuvent pas être écrits dans les fichiers d'événements de regroupement.

Les recommandations matérielles pour une mise en œuvre Sentinel étant susceptibles de varier d'un déploiement à l'autre, il est recommandé de consulter Novell Consulting Services avant de finaliser l'architecture Sentinel. Les recommandations suivantes peuvent servir de lignes directrices.

Remarque : en raison des charges d'événements élevées et du caching local, la machine Sentinel Server avec DAS doit être pourvue d'une pile de disques à bande locale ou partagée (RAID) avec un minimum de 4 broches.

Les hôtes distribués doivent être connectés aux autres hôtes du serveur Sentinel via un seul commutateur de haute vitesse (GIGE) afin d’éviter des goulot d’étranglement de trafique des réseaux.

Novell recommande d'installer Crystal Enterprise Server sur une machine qui lui est spécifique, surtout si la base de données est volumineuse ou si l'on prévoit de créer de nombreux rapports. Crystal peut être installé sur la même machine que la base de données si cette dernière est peu volumineuse, si la création de rapport est peu intense et si la base de données est installée sous Windows ou Linux.

Remarque : Sentinel 6.0 était toujours en phase de développement au moment de la rédaction du présent document, les valeurs suivantes sont donc basées sur un test de Sentinel 5.1.3. Pour obtenir

des informations actualisées, consultez le site de documentation Novell à l'adresse http://www.novell.com/documentation (http://www.novell.com/documentation).

EPS 1-500 : configuration 2 machines (Sentinel 5.1.3)			
Composants	**RAM**	**Espace**	**UC**
Machine 1 : Sentinel Server / Collector Manager ◆ Moteur de corrélation ◆ DAS ◆ Serveur de communication ◆ Advisor ◆ Collector Manager / Collectors ◆ Base de données ◆ Crystal Server (facultatif pour Windows/Linux)	6 Go	250 Go	Windows ou Linux - 2 x Intel® Xeon® 5150 double cœur (2,66 GHz) ou Sun Solaris - 4 x UltraSPARC IIIi (1,5 GHz)
Machine 2 : Report Server ◆ Crystal Server	2 Go	20 Go	Windows ou Linux - 1 x Intel® Xeon® 5150 double cœur (2,66 GHz)

EPS 500 – 1500 : configuration 3 machines (Sentinel 5.1.3)			
Composants	**RAM**	**Espace**	**UC**
Machine 1 : Sentinel Server / Collector Manager ◆ Moteur de corrélation ◆ DAS ◆ Serveur de communication ◆ Advisor ◆ Collector Manager / Collectors	4 Go	40 Go	Windows ou Linux - 2 x Intel® Xeon® 5160 double cœur (3,0 GHz) ou Sun Solaris - 2 x UltraSPARC IV+ de 1,8 GHz
Machine 2 : Base de données ◆ Base de données ◆ Crystal Server (facultatif pour Windows/Linux)	4 Go+	1 To+	Windows ou Linux - 2 x Intel® Xeon® 5160 double cœur (3,0 GHz) ou Sun Solaris - 2 x UltraSPARC IV+ de 1,8 GHz
Machine 3 : Report Server (uniquement nécessaire si Sentinel/la base de données sont sous Solaris) ◆ Crystal Server	2 Go	20 Go	Windows ou Linux - 1 x Intel® Xeon® 5150 double cœur (2,66 GHz)

EPS 1500 - 3000 : configuration 4-5 machines (Sentinel 5.1.3)			
Composants	**RAM**	**Espace**	**UC**
Machine 1 : Sentinel Server ◆ Moteur de corrélation ◆ DAS ◆ Serveur de communication ◆ Advisor	4 Go	40 Go	Windows ou Linux - 2 x Intel® Xeon® 5160 double cœur (3,0 GHz) ou Sun Solaris - 2 x UltraSPARC IV+ de 1,8 GHz
Machine 2 : Base de données ◆ Base de données ◆ Crystal Server (facultatif pour Windows/Linux)	8 Go+	3 To+	Windows ou Linux - 2 x Intel® Xeon® 5160 double cœur (3,0 GHz) ou Sun Solaris - 2 x UltraSPARC IV+ de 1,8 GHz
Machine 3 : Collector Manager ◆ Collector Manager / Collectors	2 Go	20 Go	Windows ou Linux - 2 x Intel® Xeon® 5160 double cœur (3,0 GHz) ou Sun Solaris - 2 x UltraSPARC IV+ de 1,8 GHz
Machine 4 : Report Server ◆ Crystal Server	4 Go	20 Go	Windows ou Linux - 1 x Intel® Xeon® 5150 double cœur (2,66 GHz)
Machine 5 : Composant DAS (nécessaire si EPS > 2000)	2 Go	40 Go	Windows ou Linux - 2 x Intel® Xeon® 5160 double cœur (3,0 GHz) Sun Solaris - 2 x UltraSPARC IV+ de 1,8 GHz

2.3 Évaluation des performances

Les tableaux suivants décrivent plusieurs configurations représentatives et résultats de test.

Ces valeurs doivent être considérées comme des points de référence pour déterminer la conception architecturale et ne représentent nullement des limites figées. Dans ces tests, les charges système ne dépassaient pas le pourcentage d'utilisation de 75 % et les taux d'événements représentent les performances à l'état stable.

Remarque : Les tests d'évaluation étaient essentiellement axés sur les insertions d'événements Sentinel, la corrélation et le service d'assignation. Les autres activités, telles que la création de rapport ou les requêtes de données historiques, n'ont pas été reprises dans le test.

Tous les tests ci-dessous ont été exécutés sur un système avec RAID 5 avec segmentation et configuration 4+1.

2.3.1 Configuration test ou démonstration de faisabilité

Cette configuration mono-machine convient pour les démonstrations ou les tests limités et peut être installée à l'aide de l'option « simple » du programme d'installation de Sentinel. L'utilisation de cette configuration est fortement déconseillée dans un système de production.

Remarque : Sentinel 6.0 était toujours en phase de développement au moment de la rédaction du présent document, les valeurs suivantes sont donc basées sur un test de Sentinel 5.1.3. Pour obtenir des informations actualisées, consultez le site de documentation Novell à l'adresse http://www.novell.com/documentation (http://www.novell.com/documentation/index.html).

Fonction	RAM	MODEL
Sentinel Server + base de données + Collector Manager	5 Go, RAID 5 x 36 Go	SLES9 - 2 x Intel® Xeon® 5150 double cœur (2,66 GHz)

Les mesures de performances suivantes ont été observées sur ce système.

Attribut	Coefficient	Commentaires
Événements traités et stockés par jour (dans la base de données)	86 millions	
Événements par seconde (Collector Manager)	1000	Un processeur simple (double cœur) Xeon a été utilisé pour Collector Manager
Événements par seconde (Correlation Engine)	300	Des périphériques PIX, Snort et autres ont été utilisés dans ce test
Événements par seconde (Syslog)	300	1 serveur Syslog a été exécuté sur l'hôte Collector Manager avec 1 moteur
Collecteurs déployés pour chaque gestionnaire des collecteurs	3	1 collecteur a utilisé Syslog ; d'autres ont employé un connecteur de fichier
Nombre de gestionnaires des collecteurs	1	20 est le nombre maximal de gestionnaires des collecteurs pris en charge pour chaque serveur Sentinel
Nombre de moteurs de corrélation déployés	1	S'exécute sur la machine Sentinel Server
Règles déployées par moteur de corrélation	10	
Nombre d'instances Active Views™	10	
Nombre d'utilisateurs simultanés	3	
Nombre de vues par instance Active View	2	
Nombre d'assignations déployées	2	
Taille maximale d'assignation du service d'assignation	1.5 Mo	
Nombre de lignes dans la plus grande assignation	1.5 millions	

2.3.2 Configuration d'un système de production – Option 1

Cette configuration comprend trois machines et traite environ 2 000 événements par seconde.

Remarque : Sentinel 6.0 était toujours en phase de développement au moment de la rédaction du présent document, les valeurs suivantes sont donc basées sur un test de Sentinel 5.1.3. Pour obtenir des informations actualisées, consultez le site de documentation Novell à l'adresse http://www.novell.com/documentation (http://www.novell.com/documentation/index.html).

Fonction	RAM	MODEL
Serveur Sentinel	4 Go, RAID 5 x 36 Go	SLES9 - 2 x Intel® Xeon® 5150 double cœur (2,66 GHz)
Base de données	4 Go, RAID 5 x 250 Go	SLES9 - 2 x Intel® Xeon® 5150 double cœur (2,66 GHz)
Gestionnaire des collecteurs	2 GIG, 72 GIG	SLES9 - 1 x Intel® Xeon® 5150 double cœur (2,66 GHz)

Les mesures de performances suivantes ont été observées sur ce système :

Attribut	Coefficient	Commentaires
Événements traités et stockés par jour (dans la base de données)	173 millions	
Événements par seconde (Collector Manager)	2000	Un processeur simple (double cœur) Xeon a été utilisé pour Collector Manager
Événements par seconde (Correlation Engine)	1200	Des périphériques PIX, Snort et autres ont été utilisés dans ce test
Événements par seconde (Syslog)	1200	1 serveur Syslog a été exécuté sur l'hôte Collector Manager avec 1 moteur
Collecteurs déployés pour chaque gestionnaire des collecteurs	10	1 collecteur a utilisé Syslog ; d'autres ont employé un connecteur de fichier
Nombre de gestionnaires des collecteurs	1	20 est le nombre maximal de gestionnaires des collecteurs pris en charge pour chaque serveur Sentinel
Moteurs de corrélation déployés	1	S'exécute sur la machine Sentinel Server
Règles déployées par moteur de corrélation	20	
Nombre d'instances Active Views™	20	
Nombre d'utilisateurs simultanés	5	
Nombre de vues par instance Active View	4	
Nombre d'assignations déployées	4	
Taille maximale d'assignation	1.5 Mo	

Attribut	Coefficient	Commentaires
Nombre de lignes dans la plus grande assignation	1.5 millions	

2.3.3 Configuration d'un système de production – Option 2

Cette configuration exige quatre machines et traite environ 3 000 événements par seconde.

Remarque : Sentinel 6.0 était toujours en phase de développement au moment de la rédaction du présent document, les valeurs suivantes sont donc basées sur un test de Sentinel 5.1.3. Pour obtenir des informations actualisées, consultez le site de documentation Novell à l'adresse http://www.novell.com/documentation (http://www.novell.com/documentation/index.html).

Fonction	RAM	MODEL
Serveur Sentinel	4 Go, RAID 5 x 36 Go	SLES9 - 2 x Intel® Xeon® 5160 double cœur (2,66 GHz)
Base de données	8 Go, RAID 5 x 250 Go	SLES9 - 2 x Intel® Xeon® 5160 double cœur (2,66 GHz)
Gestionnaire des collecteurs	2 GB, 72 GB	SLES9 - 2 x Intel® Xeon® 5160 double cœur (2,66 GHz)
Sentinel Server (DAS - nœud 2)	2 Go, RAID 5 x 36 Go	SLES9 - 2 x Intel® Xeon® 5160 double cœur (2,66 GHz)

Les mesures de performances suivantes ont été observées sur ce système :

Attribut	Coefficient	Commentaires
Événements traités et stockés par jour (dans la base de données)	260 millions	
Événements par seconde (Collector Manager)	3000	Un processeur double (double cœur) Xeon a été utilisé pour Collector Manager
Événements par seconde (Correlation Engine)	1200	Des périphériques PIX, Snort et autres ont été utilisés dans ce test
Événements par seconde (Syslog)	2500	1 serveur Syslog a été exécuté sur l'hôte Collector Manager
Collecteurs déployés pour chaque gestionnaire des collecteurs	10	3 collecteurs ont utilisé Syslog ; d'autres ont utilisé un connecteur de fichier
Nombre de gestionnaires des collecteurs	1	
Moteurs de corrélation déployés	1	S'exécute sur la machine Sentinel Server
Règles déployées par moteur de corrélation	20	
Nombre d'instances Active Views™	20	
Nombre d'utilisateurs simultanés	5	

Attribut	Coefficient	Commentaires
Nombre de vues par instance Active View	4	
Nombre d'assignations déployées	4	
Taille maximale d'assignation	1.5 Mo	
Nombre de lignes dans la plus grande assignation	1.5 millions	

2.4 Configuration de pile de disques

Le serveur Novell Sentinel sous une configuration de production requiert une pile de disques haute vitesse pour la base de données et les hôtes Sentinel. Cette section fournit des recommandations pour la configuration de disques classiques (RAID). Les fonctionnalités suivantes sont affectées par les performances du matériel disque :

- Composant base de données (Microsoft SQL/Oracle) : les fonctionnalités de taux d'événements (événements par seconde) et de requête sont affectées (y compris la requête d'événements historiques, la requête hors ligne et la création de rapport Crystal).
- Composant DAS-RT (Data Access Service Real Time) : la fonctionnalité Active Views est affectée.
- Regroupement DAS : le nombre de résumés pouvant être activés est affecté.

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

La configuration minimum recommandée est l'utilisation de RAID 5. RAID 5 peut être le plus rentable. Cette configuration ne sacrifie pas quelque performance et redondance pour la rentabilité. Veuillez notez que tout cela n'est 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, débit et redondance.

- RAID Groupe 1 – BD (données, indexes, journaux des transactions, etc.)
- RAID Groupe 2 – DAS du serveur Sentinel (Data dir, Temp DIR*)
- Nombre minimal de disques : 13 par groupe RAID
- Type de disque : 12k+ 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

2.4.2 Configuration optimale

Pour une configuration optimale au niveau de la performance et de la redondance, un RAID 1+0 peut être utilisé avec les mêmes paramètres. Il se peut toutefois que des groupes RAID et des LUN supplémentaires respectant les mêmes directives que ci-dessus soient nécessaires pour davantage de parallélisme et d'E/S pour certaines bases de données.

Remarque : pour plus d'informations sur la façon de faire pointer DAS TEMP DIR vers un autre emplacement, reportez-vous à la Section 2.7, « Installation et configuration de Sentinel », page 34

2.4.3 Exemple de configuration de stockage pour une installation Microsoft SQL

Cet exemple utilise le sous-système EMC2 CLARiiON avec :

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

Groupes RAID

Pile	LUN	Type de RAID	Groupe RAID	Taille (Go)
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

Affectations 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

2.4.4 Exemple de configuration de stockage pour une installation 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	espace de table annulations et modèles
volume 5	RAID 0+1 ou RAID 5	espace de table de données Sentinel
volume 6	RAID 0+1 ou RAID 5	espace de table d’index Sentinel
volume 7	RAID 0+1 ou RAID 5	espace de table de données récapitulatifs Sentinel
volume 8	RAID 0+1 ou RAID 5	espace de table d’index récapitulatifs Sentinel
volume 9	RAID 1	fichiers journaux de stockage

2.5 Configuration du réseau

Composants côté Sentinel Server : ils doivent être connectés les uns aux autres via un seul commutateur de 1 Go. Ils incluent base de données, serveur de communication, Advisor, services de base Sentinel, moteur de corrélations et DAS.

Sentinel Control Center, Collector Builder et Collector Service (Collector Manager) : ils doivent être connectés à Sentinel Server via des commutateurs FULL DUPLEX d'au moins 100 Mbits.

2.6 Meilleures pratiques - Installation/ configuration d'une base de données

Remarque : la plupart des paramètres d'installation d'une base de données peuvent être modifiés après l'installation de la base de données via les outils de gestion de la base de données ou la ligne de commande.

1. Sentinel utilise une stratégie d'archivage prédéfinie pour gérer les tables à croissance rapide (la table des événements, par exemple). Ces tables sont partitionnées, les parties plus anciennes pouvant être archivées et supprimées sans affecter les données plus récentes. D'autres tables ne bénéficient toutefois pas de cette stratégie de partitionnement et d'archivage et devront être gérées séparément.
2. Pour des raisons de performances, 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 des modifications (Oracle)
   - Journal des transactions (Microsoft SQL)
3. Pour déterminer plus précisément la taille de la base de données, vous pouvez commencer au début par une base de données petite et accroître sa taille quand le système est déjà prêt et en exécution pour une brève période. Ainsi, vous pouvez voir l'accroissement de la base de donnés en fonction du taux d'insertion d'évènements pour déterminer les conditions requises à l'espace de la base de données du système.
4. À des fins de récupération, un administrateur de base de données doit régulièrement effectuer des sauvegardes planifiées des tables non partitionnées de la base de données.
5. Pour les installations Oracle, le programme d'installation Sentinel désactive par défaut 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 de stockage cible, sinon la base de données ne va plus accepter d'évènements lorsque le journal de stockage cible atteint sa capacité maximale.
6. À des fins de performances dans les environnements à taux d'événements élevé, les emplacements de stockage doivent pointer vers des emplacements différents (par ex. plusieurs contrôleurs de disque) pour éviter des conflits d'E/S.
   - répertoire de données
   - répertoire d'index
   - répertoire de données récapitulatif
   - répertoire d'index récapitulatif
   - répertoire du journal (Microsoft SQL uniquement)
   - répertoire d'espace de table temporaire et d'annulation d'espace de table (Oracle uniquement)
   - répertoire du membre A du journal des modifications (Oracle uniquement)
   - répertoire du membre B du journal des modifications (Oracle uniquement)

2.6.1 Correctifs de la base de données Sentinel

Pour Microsoft SQL uniquement, quand les correctifs de la base de données Sentinel sont appliqués, le programme d'installation n'ajoute de nouveaux index qu'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 les performances des requêtes exécutées sur les partitions existantes.

2.6.2 Paramètres kernel UNIX recommandés pour Oracle

Vous trouverez ci-dessous des suggestions de valeurs minimums. Pour plus d'informations, consultez la documentation Oracle et celle du système.

Valeurs minimums des paramètres Kernel pour Linux

Pour plus d'informations sur l'affichage et la définition des paramètres kernel sous Linux, reportez-vous au Chapitre 3, « Installation de Sentinel 6 », page 45 du guide d'installation.

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

Valeurs minimums des paramètres Kernel pour Solaris

Vérifiez les paramètres Kernel pour Oracle sur /etc/system et configurez les éléments suivant :

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

2.6.3 Configuration de paramètres lors de la création de votre propre instance de base de données

Si vous le souhaitez, vous pouvez créer manuellement la structure de la base de données (au niveau des espaces de table) plutôt que via le programme d'installation de Sentinel. Ensuite, pendant l'installation, vous pouvez choisir l'option « Ajouter les objets de la base de données à une base de données vide existante ». Vous trouverez ci-dessous les paramètres recommandés lors de la création de votre propre instance de base de données. Les valeurs peuvent varier en fonction de la configuration et des conditions requises du système.

Sur l'instance Oracle, vous devez créer :

- les paramètres d'initialisation Oracle (ces valeurs changent en fonction de la taille et de la configuration du système)

- Paramètres de configuration d’espaces de tables requis par Sentinel sur 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	TRUE
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 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

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

2.7 Installation et configuration de Sentinel

Pour des raisons de performance et sauvegarde, lors de l'installation de Sentinel vous devez 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 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 supprimer, reportez-vous au Chapitre 11, « Désinstallation de Sentinel », page 153 du guide d'installation.
2. Les performances d'Active Views et de la fonction d'assignation peuvent être améliorées de manière spectaculaire en faisant pointer le répertoire temporaire des processus DAS_RT et DAS_Query vers un disque rapide (par ex., une pile de disques). Pour cibler le répertoire de modèles de ces processus vers un disque plus rapide, effectuez le suivant sur la machine où le DAS est installé. :
   - **2a** Créez un repertoire sur le disque rapide pour placer les fichiers modèles. Sous UNIX, ce répertoire doit être la propriété de l'administrateur Sentinel et du groupe esec et être accessible en écriture par ces derniers.
   - **2b** Effectuez une copie de sauvegarde du fichier %ESEC_HOME%\config\configuration.xml.
   - **2c** Ouvrez le fichier %ESEC_HOME%\config\configuration.xml dans un éditeur de texte.
   - **2d** Pour les procesuss DAS_RT et DAS_Query, ajouter l'argument JVM java.io.tmpdir, le configurant vers le répertoire que vous venez de créer.

2e Pour effectuer cette modification au processus DAS_RT, cherchez la ligne contenant le text

```
-Dsrv_name=DAS_RT
```

et, en regard de celle-ci, ajoutez l'argument mentionné ci-dessous.

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

Vous trouverez ci-dessous un exemple à quoi la ligne semblera (vos arguments –Xmx, -Xms et –XX peuvent être differents) :

```
<process component="DAS" image="&amp;quot;$(ESEC_JAVA_HOME)/
java&amp;quot; -server -Dsrv_name=DAS_RT -Djava.io.tmpdir=D:\Temp2
-Xmx310m -Xms103m -XX:+UseParallelGC -Xss128k -Xrs -
Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml -
Djava.util.logging.config.file=../config/das_rt_log.prop -
Dcom.esecurity.configurationfile=../../configuration.xml -
Djava.security.auth.login.config=../config/auth.login -
Djava.security.krb5.conf=../../lib/krb5.conf -jar ../../lib/
ccsbase.jar ..//config//das_rt.xml" min_instances="1"
post_startup_delay="5" shutdown_command="cmd //C
&amp;quot;$(ESEC_HOME)/bin/stop_container.bat&amp;quot; localhost
DAS_RT" working_directory="$(ESEC_HOME)/bin"/>
```

2f Pour effectuer cette modification au processus DAS_Query, cherchez la ligne contenant le text

```
-Dsrv_name=DAS_Query
```

et, en regard de celle-ci, ajoutez l'argument mentionné ci-dessous.

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

Vous trouverez ci-dessous un exemple à quoi la ligne semblera (vos arguments –Xmx, -Xms et –XX peuvent être differents) :

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

2.8 Définition de mots de passe – Meilleures pratiques

Pour répondre aux exigences strictes de sécurité requises par la certification des critères communs :

1. Choisissez des mots de passe comportant un minimum de 8 caractères et incluant au moins un caractère en MAJUSCULE, un caractère en minuscule, un caractère spécial (!@#$%^&*()_+) et un chiffre (0-9).
2. Votre mot de passe ne peut contenir ni votre adresse de messagerie ni une partie de votre nom.
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 mots d'une langue, quelle qu'elle soit, car de nombreux programmes de reconnaissance de mots de passe sont capables de rechercher parmi des millions de combinaisons de mots possibles en quelques secondes.
5. Choisissez un mot de passe facile à mémoriser et complexe à la fois. Par exemple, Mfa5!As (mon fils a 5 ans) OU J!hb1tE75 (j'habite à Paris).

2.9 Configuration de rapport

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 d'enregistrements, vous devez reconfigurer Crystal Page Server. Pour ce faire, vous pouvez utiliser Central Configuration Manager ou la page Web Crystal.

Pour reconfigurer Crystal Page Server via Central Configuration Manager :

1. Cliquez sur 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 <value greater than 20000 or 0 to disable the default limit>`
5. Redémarrez Crystal Page Server.

Pour reconfigurer Crystal Page Server via la page Web Crystal :

1. Cliquez sur Démarrer > Tous les programmes > BusinessObjects 11 > Crystal Reports Server> .NET Administration Launchpad.
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 Database Records to Read When previewing or Refreshing a report (Enregistrements de base de données à lire lors de l'aperçu avant impression ou du rafraîchissement d'un rapport), cliquez sur Unlimited records (Enregistrements illimités).
8. Cliquez sur Appliquer.
9. Une invite pour redémarrer le serveur de pages s'affiche, cliquez sur OK.

L'invite peut vous demander un nom de login et le mot de passe pour accéder au gestionnaire de services du système d'exploitation.

Pour reconfigurer Crystal Page Server (serveurs Linux ou Windows Crystal) :

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

   Pour serveurs Linux Crystal :

   ```
   http://<DNS or IP of Crystal Server>:8080/businessobjects/
   enterprise11/adminlaunch
   ```

   Pour serveurs Windows Crystal :

   ```
   http://<DNS name or IP address of your web server>/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.

2.9.1 Rapports fournis par Sentinel

Pour accroître les performances, les 10 principaux rapports interrogent les tables récapitulatives plutôt que la table des événements. Les tables récapitulatives contiennent des comptages temporels de combinaisons de champs dans les données d'événements. L'ensemble de données est ainsi bien moins volumineux pour certains types de requêtes, donnant lieu à une bien plus grande rapidité d'exécution des requêtes et des rapports.

Le service de regroupement est chargé de compléter les tables récapitulatives avec des récapitulations de tous les événements de la table des événements. Il ne générera des données résumées que pour les récapitulatifs actifs. Les récapitulatifs suivants sont requis par les 10 principaux rapports et activés par défaut :

- EventDestSummary

- EventSevSummary
- EventSrcSummary

La fenêtre Configuration des données de rapport sous l'onglet Admin de Sentinel Control Center permet d'activer ou de désactiver les récapitulatifs.

Le service de regroupement dépend également du composant EventFileRedirectService du processus DAS Binary qui lui fournit les données d'événements à résumer. Par conséquent, ce composant doit être activé pour que le service de regroupement fonctionne correctement. Pour activer ou désactiver ce composant, définissez l'attribut « Status » du composant EventFileRedirectService dans le fichier das_binary.xml sur « on » (activé) ou « off » (désactivé). Par défaut, ce composant est activé.

Remarque : pour plus d'informations sur le service EventFileRedirectService et les trois récapitulatifs de regroupement, consultez « Sentinel Data Manager » dans le guide d'utilisation de Sentinel Control Center ou de Crystal Reports pour Windows ainsi que le Chapitre 10, « Crystal Reports pour Linux », page 137 du guide d'installation de Sentinel.

Remarque : les rapports dont l'interrogation porte sur une vaste plage de dates peuvent nécessiter un temps d'exécution assez long. Ils peuvent être planifiés plutôt qu'exécutés de manière interactive. Pour plus d'informations sur la programmation de Crystal Reports, consultez la documentation de Crystal BusinessObjects Enterprise™ 11.

2.9.2 Conseils pour le développement de Crystal Reports personnalisés

Les recommandations suivantes s'imposent pour le développement de rapports personnalisés :

1. Si les rapports peuvent utiliser des tables de regroupement prédéfinies, sélectionnez la table de regroupement résultant du traitement de la quantité la plus petite de données.
2. Essayez de pousser la plupart du traitement de données vers le moteur de la base de données.
3. Afin de réduire la surcharge du traitement sur Crystal server, minimiser la quantité de données à récupérer vers lui.
4. Rédigez toujours les rapports en vous basant sur les vues de base de données fournies par Novell plutôt que sur les tables de base.

2.10 Maintenance de la base de données

Sentinel utilise sa base de données principale pour stocker tous les événements ainsi que les données de configuration. Cette base de données devra être administrée attentivement pour garantir son fonctionnement efficace.

2.10.1 Informations d'événements dans la base de données

La base de données est en grande partie constituée de données d'événements normalisées et résumées. Pour faciliter l'administration de cet ensemble de données sans cesse croissant, Novell partitionne ces tables et propose un outil de gestion, Sentinel Data Manager, pour archiver et supprimer des partitions plus anciennes. Vous pouvez développer un plan d'archivage pouvant être automatisé pour minimiser l'intervention de l'utilisateur.

Remarque : pour plus d'informations sur Sentinel Data Manager, consultez “Sentinel Data Manager” dans le guide d'utilisation de Sentinel Control Center.

2.10.2 Autres informations dans la base de données

La base de données Sentinel inclut de nombreuses autres informations, comme les comptes utilisateur, les informations de configuration, les incidents, les processus de travail, des données sur les ressources, sur la vulnérabilité, etc. Toutes ces données doivent être sauvegardées à l'aide d'outils de base de données normaux à des fins de reprise après sinistre. Novell recommande le développement d'une stratégie de sauvegarde détaillée pour l'intégralité de la base de données Sentinel (ainsi que les serveurs), à l'exception des tables partitionnées ci-dessus.

Pour SQL Server, les bases de données Sentinel sont créées par défaut d'après un modèle de récupération complète. Dans ce type de modèle, l'espace utilisé du journal des transactions n'est pas libéré tant que le journal des transactions n'est pas sauvegardé. Pour éviter que le journal des transactions ne soit rempli, des sauvegardes doivent être programmées dans SQL Server tout au long de la journée (3 à 4 fois par jour selon votre taux d'événements). Si votre organisation n'exige pas une reprise à partir du point de défaillance, vous pouvez configurer le modèle de récupération de la base de données sur Simple. Dans ce modèle simple, l'espace du journal des transactions sera libéré automatiquement par SQL Server sans aucune sauvegarde du journal.

2.10.3 Maintenance supplémentaire de la base de données

Outre les sauvegardes, la base de données devrait être régulièrement contrôlée à des fins de cohérence interne. Novell propose à cette fin des outils automatisés. Pour plus d'informations, reportez-vous au guide d'utilisation de Sentinel.

Ces utilitaires comprennent les éléments suivants :

- l'analyse de partitions, qui regroupe les statistiques des partitions récemment remplies.
- la vérification de l'état de santé de la base de données, qui regroupe des informations de la base de données. Elle peut :
  - 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
  - chercher des index inutilisables
  - il cherche des objets de base de données invalides
  - il cherche des analyses de base de données

Remarque : ces utilitaires ne remplacent nullement une maintenance régulière de la base de données effectuée par un administrateur.

Analyse de base de données pour Oracle

En raison de l'insertion permanente d'événements dans la base de données Sentinel, les statistiques doivent être régulièrement mises à jour pour garantir la bonne performance des requêtes. L’utilitaire d’analyse de la base de données met à jour les statistiques de la base de données pour les données

d’évènements sur Oracle. Pour une performance optimale, cet utilitaire devra être planifié pour une exécution régulière.

Remarque : cet utilitaire inclut le script SQL requis qui peut être mis à jour à un rythme régulier. Il est recommandé de consulter régulièrement lesite du support technique de Novell (http://support.novell.com/techselect/index.html) pour obtenir d'éventuelles mises à jour.

Analyse de partitions

Le script AnalyzePartitions.sh analyse les partitions complétées récemment. Ce script doit être programmé quotidiennement via cron ou tout autre planificateur pour mettre à jour les statistiques de la base de données au niveau des partitions complétées la veille. Il est recommandé d'exécuter ce script à un moment de la journée où la base de données est peu utilisée.

Ce script se trouve dans le répertoire $ESEC_HOME/bin. Il doit être exécuté localement sur le serveur où la base de données Sentinel est installé. 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.

Pour installer sp_esec_dba_utl.sql :

1. Loguez-vous comme propriétaire du logiciel Oracle.
2. À l'aide de SQL*Plus, connectez-vous à la base de données comme Utilisateur de la base de données Sentinel.
3. Installez le package ESEC_DBA_UTL. À l’invite SQL (SQL>), entrez :
   ```
   @sp_esec_dba_utl.sql
   ```
4. Quittez SQL*Plus.

Pour exécuter AnalyzePartitions.sh :

1. Sur la machine du serveur de base de données Oracle, accédez à :
   ```
   $ESEC_HOME/bin/
   ```
   ou à 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 écrites.

   Si le script réussi, il quitte affichant un code de renvoi de 0. S’il échoue, il quitte affichant un code de renvoi de 1. Planifiez dûment les travaux pour vérifier le code de renvoi. Si le travail d’analyse échoue, vérifiez le fichier journal pour voir des messages d’erreur détaillés.

2.10.4 Vérification de santé de la base de données pour Oracle

est un script qui récolte des informations sur la base de données Sentinel Oracle. Le script dbHealthCheck.sh est situé dans le dossier %esec_home%\bin. Le script effectue le suivant :

- 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
- chercher 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 qui inclut le script SQL requis peut être mis à jour à un rythme régulier. Il est recommandé de consulter régulièrement lesite du support technique de Novell (http://support.novell.com/techselect/index.html) pour obtenir d'éventuelles mises à jour.

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

Pour installer 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 défini dans l'environnement.
3. À l'aide de SQL*Plus, connectez-vous à la base de données comme Utilisateur de la base de données Sentinel.
4. Installez le package ESEC_DBA_UTL. À l'invite SQL (SQL>), entrez :

   ```
   @sp_esec_dba_utl.sql
   ```
5. Quittez SQL*Plus.

Pour exécuter 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 défini dans l'environnement.
2. Sur la machine du serveur de base de données Oracle, accédez à :

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

   ou à 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 >> <filename>
```

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 >> <filename>
```

2.10.5 Maintenance de la base de données

Le partitionnement de la base de données est configuré automatiquement lors de l'installation de Sentinel. L'administrateur est invité à consulter les paramètres dans Sentinel Data Manager et à les modifier au besoin. Pour plus d'informations sur Sentinel Data Manager, consultez « Sentinel Data Manager » dans le guide de l'utilisateur de Sentinel Control Center.

2.11 Moteur de corrélation

2.11.1 Synchronisation horaire

Le moteur de corrélation de Sentinel étant très sensible au temps, Novell recommande vivement de connecter toutes les machines Correlation Engine et Collector Manager à un serveur NTP (Network Time Protocol) ou un autre type de serveur horaire. Pour garantir le bon fonctionnement de Sentinel Correlation Engine, l'heure système de la machine doit être synchronisée à ± 30 secondes près avec toutes les machines Collector Manager.

2.11.2 Utilisation de la mémoire

Dans le langage de règle de corrélation, une fenêtre de temps est associée aux deux opérateurs Window et Trigger. Plus cette fenêtre de temps est grande, plus elle peut mémoriser des informations d'événements pour cette fenêtre. Cela affecte donc la quantité de mémoire nécessaire pour effectuer une corrélation dans la mémoire Sentinel. Si le moteur de corrélation utilise trop de mémoire, envisagez les possibilités suivantes :

- Installez le moteur de corrélation sur une machine spécifique et redéployez toutes les règles existantes dans le nouveau moteur de corrélation.
- Installez un nouveau moteur de corrélation et redéployez certaines règles existantes dans le nouveau moteur de corrélation.
- Adaptez la clause Window de vos règles de corrélation.
  - Spécifiez plus précisément le filtre des événements passés
  - Diminuez la taille de la fenêtre de temps.
- Adaptez la clause Trigger de vos règles de corrélation.
  - Diminuez la taille de la fenêtre de temps.

- Diminuez le seuil du nombre d'événements requis pour déclencher la règle.
- Choisissez des discriminateurs de faible cardinalité (par ex., type de périphérique).
- Si la cardinalité de votre discriminateur est faible (par ex., adresse IP source), diminuez le seuil du nombre d'événements requis pour déclencher la règle ainsi que la taille de la fenêtre de temps pour obtenir un résultat équivalent.

2.11.3 Évaluation court-circuit

Il est plus rapide de comparer des nombres que des chaînes et de comparer des chaînes que des expressions régulières. L'opération de filtrage effectue une évaluation court-circuit sur les expressions booléennes. En formulant votre expression attentivement, vous pouvez augmenter la vitesse d'évaluation.

2.11.4 Règles à format libre

S'il vous est impossible d'exprimer une règle de corrélation à l'aide de l'Assistant Règle de corrélation, créez une règle de format libre à l'aide du langage de règle de corrélation. Pour plus d'informations sur la création d'une règle de format libre, consultez la section “Moteur de corrélation” dans le guide de référence.

2.12 Fichiers journaux Sentinel

Il est recommandé de consulter périodiquement les fichiers journaux générés par Sentinel pour vérifier les éventuelles erreurs. Pour plus d'informations sur ces fichiers et leurs emplacements, reportez-vous à la section “Emplacements des journaux de Sentinel” dans le guide de référence.

Installation de Sentinel 6

3

Rubriques traitées dans ce chapitre :

3.1 Installation de Sentinel sous Linux, Solaris et Windows

Ce chapitre vous aide à installer Sentinel pour Oracle sous SUSE Linux Enterprise Server, Red Hat Enterprise Linux, et Solaris et Microsoft SQL Server sous Windows.

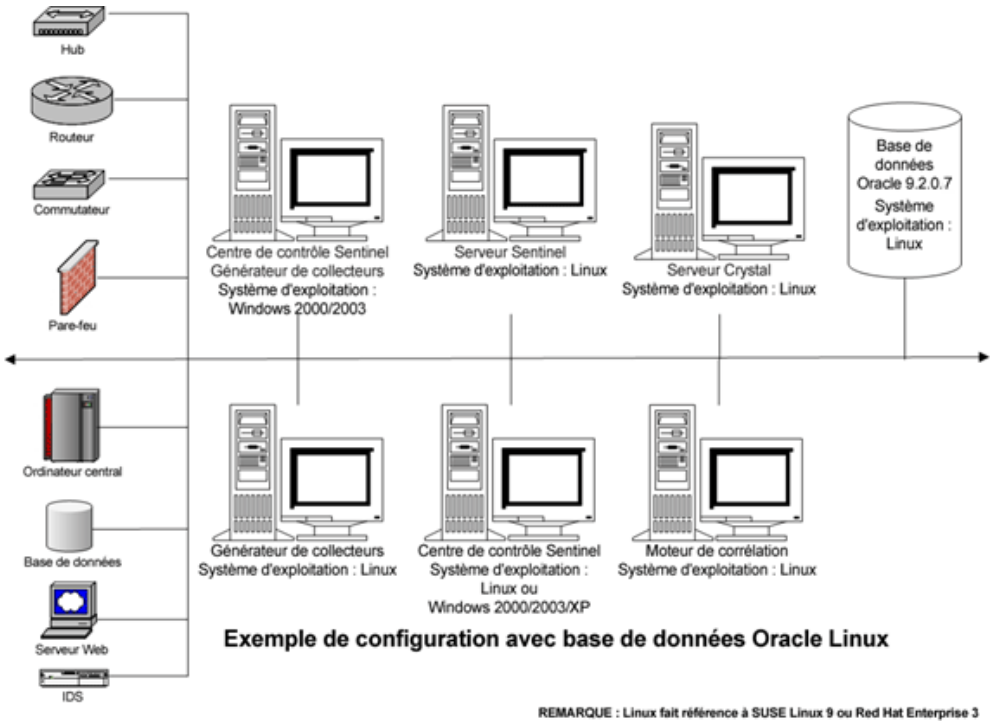
Si vous effectuez une nouvelle installation de Sentinel après en avoir désinstallé une version précédente, vous devrez supprimer manuellement certains fichiers et paramètres système qui pourraient subsister. Pour plus d'informations sur la désinstallation de Sentinel 6.0, reportez-vous au Chapitre 11, « Désinstallation de Sentinel », page 153. Pour plus d'informations sur la désinstallation de versions précédentes de Sentinel, consultez les versions de document correspondantes disponibles sur le site Web de documentation Novell à l'adressehttp://www.novell.com/documentation/ (http://www.novell.com/documentation/).

Remarque : pour installer Sentinel Server sous SLES, Novell recommande l'utilisation d'un système de fichiers autre que ReiserFS dans la mesure où des problèmes intermittents ont été constatés lors de l'exécution de Sentinel sous SLES à l'aide de ReiserFS. Bien qu'il existe plusieurs options, Novell a réalisé ses tests internes sur Sentinel à l'aide du système de fichiers ext3.

3.1.1 Configuration Sentinel

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.

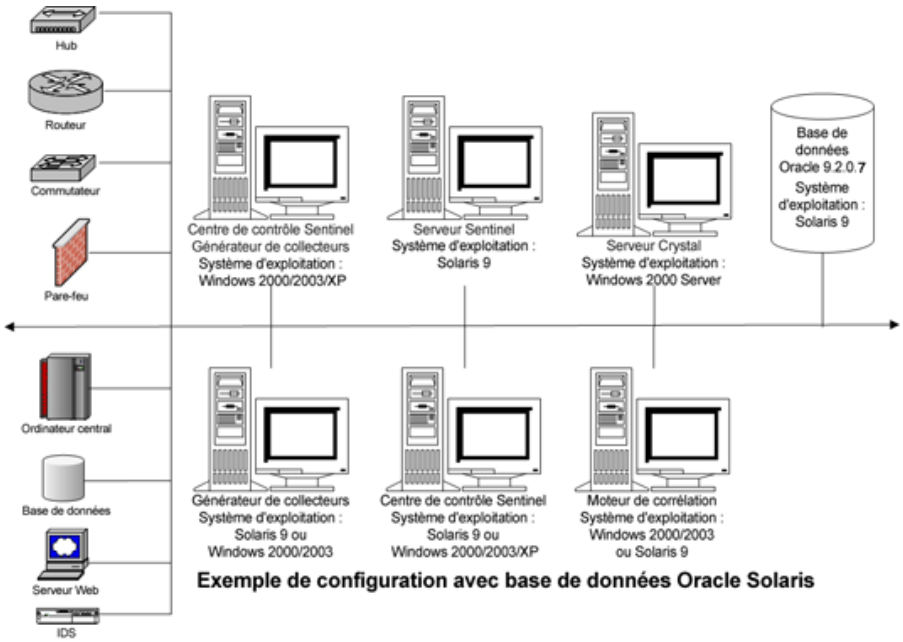
Sur Linux



Exemple de configuration avec base de données Oracle Linux

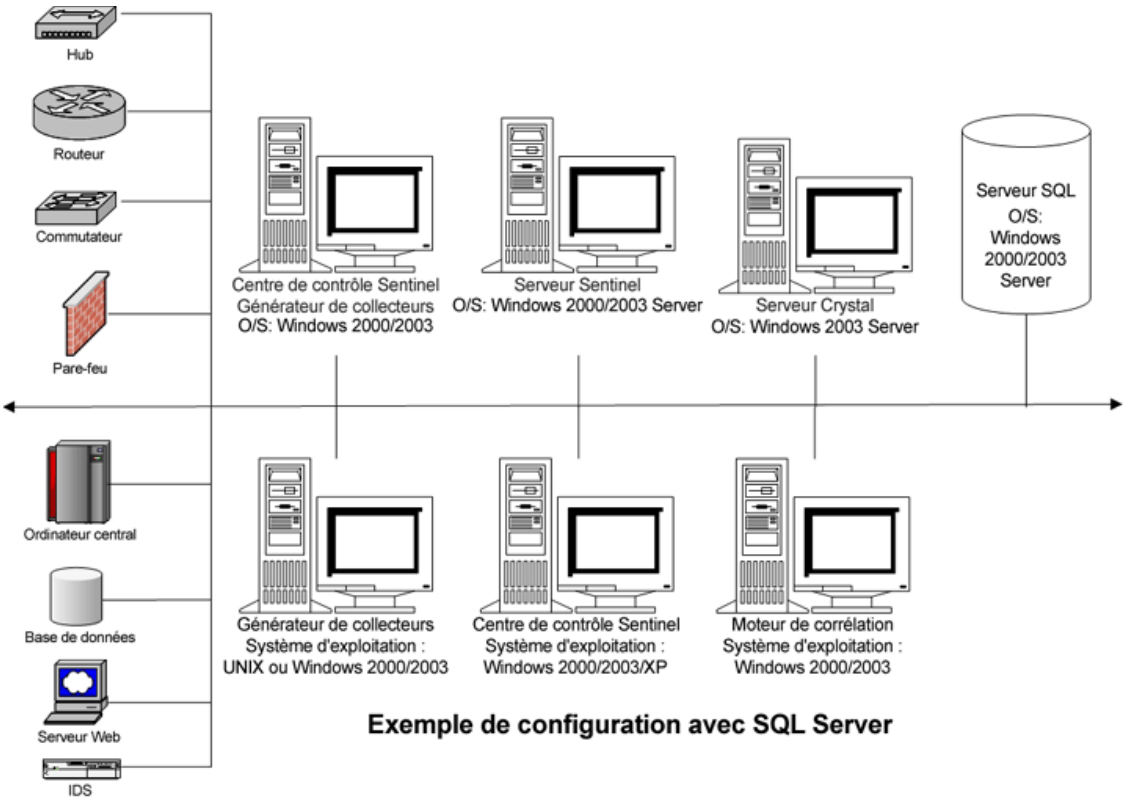
REMARQUE : Linux fait référence à SUSE Linux 9 ou Red Hat Enterprise 3

Sous Solaris



Exemple de configuration avec base de données Oracle Solaris

Sur Windows



Exemple de configuration avec SQL Server

3.1.2 Configuration requise pour l'installation de Sentinel 6.0

Avant d'installer Sentinel, vous devez répondre aux conditions suivantes :

- Vos machines doivent répondre à la configuration minimale requise et le système d'exploitation doit avoir été renforcé selon les meilleures pratiques de sécurité actuelles. Pour plus d'informations, reportez-vous à Chapitre 2, « Meilleures pratiques », page 19
- Pour installer Sentinel sous Solaris et Linux, installez Oracle Enterprise avec un partitionnement. Le gestionnaire de données Sentinel requiert cette fonction afin de gérer la base de données Sentinel.
- Vous devez avoir respecté les conditions requises pour installer les composants suivants :
  - Base de données Sentinel
  - Serveur Sentinel
  - Sentinel Control Center et Sentinel Collector Builder
  - Sentinel Advisor
- Vous devez avoir installé Oracle sous Linux, SUSE Linux, Red Hat Linux et Solaris.

Base de données Sentinel

Avant d'installer la base de données Sentinel, vous devez répondre aux conditions suivantes :

Sous Linux/Solaris :

- Sous Linux, vous devez disposer des références de login pour l'utilisateur du système d'exploitation Oracle (par défaut : oracle).
- Sur Solaris :
  - vous devez disposer d'une copie de Oracle 148673.1 SOLARIS: Quick Start Guide (Oracle 148673.1 SOLARIS: Démarrage rapide)
  - Un utilisateur du système d'exploitation Oracle (par défaut : oracle) est nécessaire.
- Sous Linux/Solaris, vérifiez que les variables d'environnement suivantes sont définies pour l'utilisateur du système d'exploitation Oracle :
  - ORACLE_HOME (par ex., echo $ORACLE_HOME pointe vers /opt/oracle/product/10gR2/db)
  - ORACLE_BASE (par ex., echo $ORACLE_BASE pointe vers /opt/oracle)
  - PATH (il faut $ORACLE_HOME/bin)
- Bien que cela ne soit PAS recommandé, si vous prévoyez de créer manuellement l'instance de la base de données Oracle dans laquelle la base de données Sentinel sera installée, reportez-vous à la rubrique relative à la “création et à la configuration d'une base de données pour des taux d'événements élevés” pour obtenir des instructions sur la création de votre instance Oracle à des fins de comptabilité avec Sentinel. Si vous choisissez cette option, vous devez quand même utiliser le programme d'installation de Sentinel pour ajouter les objets de base de données à l'instance de la base de données Oracle créée manuellement. Pour plus d'informations, reportez-vous à Section 3.3.2, « Installation personnalisée », page 62

Remarque : lors de l'utilisation d'une instance de la base de données Oracle, existante ou créée manuellement, elle ne doit contenir que l'utilisateur de la base de données Sentinel.

Sous Windows :

- Sous Windows, SQL Server 2005 SP1 doit être installé et en cours d'exécution.

Remarque : pour des raisons de performances, il est VIVEMENT recommandé, en cas d'installation dans RAID et à condition que l'environnement RAID le permette, de configurer le système pour que le journal des transactions pointe vers le disque d'écriture le plus rapide disponible, un disque physique séparé où sont stockés les fichiers de la base de données.

- Sous Windows, vous devez installer SQL Server avec une authentification en mode mixte permettant un login avec une authentification Windows ou SQL Server. Si vous installez SQL Server en mode non mixte, vous ne pourrez vous loguer qu'avec une authentification Windows.
- Pour modifier vos paramètres de mode d'authentification :
  - Dans Microsoft SQL Server Management Studio, cliquez avec le bouton droit sur le serveur dont vous souhaitez modifier les paramètres.
  - Sélectionnez les propriétés et cliquez sur Sécurité.
  - Parmi les deux options d'authentification, sélectionnez Mode d'authentification SQL Server et Windows ou Mode d'authentification Windows.
  - Veillez également à ce que le service MSSQLSERVER se logue avec un compte système local.
- Déterminez le nom de l'instance de SQL Server (valeur par défaut recommandée).

Remarque : si vous avez déjà nommé l'instance pendant l'installation de SQL Server, utilisez ce nom à l'invite du nom de l'instance de SQL Server lors de l'installation de la base de données Sentinel et/ou des composants DAS. Si vous n'avez pas nommé l'instance pendant l'installation de SQL Server, laissez le nom vide pendant l'installation (autrement dit, si vous insérez le nom d'hôte, n'ajoutez pas « \<nom_instance> » au nom d'hôte de la base de données.

- Déterminez le numéro de port de l'instance de SQL Server (1433 est la valeur par défaut).
- Si vous comptez utiliser l'authentification Windows pour un ou plusieurs utilisateurs Sentinel employés pendant l'installation de 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 :
  - Administrateur de la base de données Sentinel (esecdba, le propriétaire du schéma de la base de données)
  - Utilisateur de l'application Sentinel (esecapp, utilisé par les applications Sentinel pour se connecter à la base de données)
  - Administrateur Sentinel (esecadm, administrateur à des fins de login à Sentinel Control Center)
  - Utilisateur de rapports Sentinel (esecrpt, utilisé pour créer des rapports)

Remarque : par défaut, la base de données contiendra les trois premiers types d'utilisateurs.

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

Serveur Sentinel

Remarque : si vous n'installez pas la base de données Sentinel et le serveur Sentinel sur la même machine, vous devez d'abord installer la base de données Sentinel.

- Si vous installez le composant DAS, vous devez disposer du numéro de série de Sentinel et de la clé de licence (pour DAS).
- Choisissez un serveur SMTP (nom DNS). Ce composant est nécessaire pour l'envoi de courriers électroniques à partir de Sentinel.
- Sous Windows, accordez à un utilisateur le privilège « Ouvrir une session en tant que service », si vous installez DAS et utilisez un compte utilisateur Domaine Windows pour l'application Sentinel. Pour accorder ce privilège :
  - Ajoutez l'utilisateur dans « Stratégie de sécurité locale » sur la machine où vous comptez installer DAS (Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Stratégie de sécurité locale).
  - Sur la fenêtre Stratégie de sécurité locale, allez à Stratégies locales > Assignation des droits d’utilisateur.
  - Double-cliquez sur la stratégie Ouvrir une session en tant que service et ajoutez l'utilisateur.

Advisor

Pour installer Advisor, vous avez besoin d'un ID Advisor et d'un mot de passe fournis par Sentinel. Vous les recevez à l'achat du logiciel. Si vous choisissez Téléchargement direct sur Internet, utilisez le port sortant 443. Le logiciel Crystal Enterprise doit être installé sur votre système pour exécuter des rapports.

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. Pour plus d'informations, reportez-vous à Chapitre 4, « Configuration de l'Advisor », page 75.

3.2 Installation d'Oracle sous Linux, SUSE Linux, Redhat Linux et Solaris

Pour installer Oracle sous Linux/Solaris, vous devez effectuer les opérations suivantes :

- Définition des valeurs kernel
- Configuration du fichier init.ora sous Linux
- Sur Solaris :
  - Création d'un groupe et d'un compte utilisateur pour Oracle
  - Définition des variables d'environnement
  - Vérification de la configuration Solaris
- Installation d'Oracle 9.2.0.4
- Application du correctif Oracle 9.2.0.7

3.2.1 Définition des valeurs kernel

Important : les valeurs kernel proposées dans cette section sont des valeurs minimales uniquement. Vous ne devez les modifier que si vos paramètres système sont inférieurs aux valeurs minimales recommandées, et uniquement après consultation de votre administrateur système et de la documentation Oracle.

Pour définir les valeurs kernel sous Solaris :

Sous Solaris, les valeurs kernel suivantes doivent être définies dans le répertoire /etc/system.

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

1. Connectez-vous sous l'ID d'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 Redémarrer.

Pour définir les valeurs kernel sous Linux :

Sous Solaris, les valeurs kernel suivantes doivent être définies dans le répertoire /etc/system.

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

1 Connectez-vous sous l'ID d'utilisateur root.

2 Configurez les paramètres kernel en ajoutant le texte suivant à la fin du fichier « /etc/sysctl.conf » :

Remarque : Pour déterminer les valeurs actuelles pour un paramètre kernel particulier, exécutez la commande suivante :

sysctl <paramètre_kernel>

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

Sous SUSE LINUX

```
kernel.sem = 1024        32000   100      1024
kernel.shmmax = 2147483648
kernel.shmmni = 4096
vm.disable_cap_mlock=1
```

Sous REDHAT LINUX

```
# Kernel settings for 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 maximale du nombre de processus et « nofile » la limite maximale du nombre de fichiers ouverts. Ce sont les valeurs recommandées, mais elles peuvent être modifiées le cas échéant.

```
# Settings added for Oracle
oracle          soft    nproc   16384
oracle          hard    nproc   16384
oracle          soft    nofile  65536
oracle          hard    nofile  65536
```

3.2.2 Création d'un groupe et d'un compte utilisateur pour Oracle sous Solaris

Pour créer un groupe et un compte utilisateur et définir des variables d'environnement :

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
     ```

3.2.3 Définition de variables d'environnement pour Oracle sous Solaris

Pour configurer des variables d'environnement :

1. Loguez-vous comme utilisateur root.
2. 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
   ```

3.2.4 Vérification de la configuration Solaris

Pour configurer des variables d'environnement :

1. Allez sur le site Internet de Sun et téléchargez l'ensemble des correctifs recommandés pour Solaris 9 :
   - Ensemble de correctifs - DATE : 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.

3.2.5 Installation d'Oracle

Cette section explique comment installer Oracle sous :

- SUSE Linux
- Red Hat Linux
- Solaris

Important : Les instructions suivantes ne remplacent pas la documentation Oracle. Il s'agit seulement d'un exemple de scénario de configuration. Il est fortement conseillé de suivre ces instructions. Cette documentation part du principe que le répertoire privé des utilisateurs Oracle est / /home/oracle et qu'Oracle est installé dans /opt/oracle. Votre configuration peut être différente. Consultez la documentation concernant le système d'exploitation et Oracle, pour plus d'informations.

Sous SUSE Linux (SLES 9 SP3)

Pour installer Oracle sous SUSE Linux :

1. Respectez les instructions d'installation fournies dans le manuel d'installation de SLES 9. Installez SLES 9 avec les paquetages par défaut, le compilateur et les outils C/C++ et SP2.

   Remarque : si vous avez déjà installé SUSE Linux, vous pouvez utiliser YaST (Yet Another Setup Tool) dans l'interface SUSE Linux pour installer le compilateur et les outils C/C++.

   ---

2. Loguez-vous comme utilisateur root.
3. Installez gcc_old à l'aide de YaST.
4. Vérifiez que vous exécutez SP3 en entrant :

   ```
   SPident
   ```

   ou

   ```
   cat /etc/SuSE-release
   ```

   Vous devez obtenir :

   ```
   CONCLUSION: System is up-to-date!
         Found     SLES-9-i386-SP3
   ```

   ou

   ```
   SUSE LINUX Enterprise Server (i586)
   VERSION = 9
   PATCHLEVEL = 3
   ```

5. Pour automatiser la plupart des tâches de préinstallation d'Oracle et créer l'utilisateur Oracle, installez orarun.rpm fourni avec SLES 9.

   Remarque : consultez le document d'installation d'Oracle pour une liste complète de la configuration requise.

   ```
   rpm -i <path>/orarun-1.8-109.15.i586.rpm
   ```

   Remarque : orarun est également disponible sur le site http://www.novell.com (http://www.novell.com).

   ---

6. Le compte de l'utilisateur Oracle est désactivé. Activez-le, en remplaçant le shell /bin/false de l'utilisateur Oracle par /bin/bash à l'aide de l'outil d'administration des utilisateurs de YaST ou en modifiant le fichier /etc/passwd.
7. Définissez un nouveau mot de passe pour l'utilisateur oracle en utilisant YaST ou en entrant :
   ```
   /usr/bin/passwd oracle
   ```
8. Pour définir les paramètres kernel, exécutez
   ```
   /usr/sbin/rcoracle start
   ```
   Ignorez les erreurs éventuelles.
   ```
   /sbin/chkconfig oracle on
   ```
9. Passez à l'utilisateur Oracle :
   ```
   su - oracle
   ```
10. Pour installer 9.2.0.4 à partir du disque 1, exécutez le script :
    ```
    ./runinstaller
    ```
11. 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
12. À l'invite de création de la base de données, sélectionnez NON.
13. (Facultatif) Annulez tous les assistants de configuration lancés par le programme d'installation.
14. 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)
    ```
15. Pour appliquer le correctif 9.2.0.7 à Oracle, à partir du disque 1 de la distribution du correctif Oracle 9.2.0.7, exécutez le script :
    ```
    ./runInstaller
    ```
16. 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 Spécifiez l’emplacement des fichiers, sélectionnez comme nom cible « OUIHome » dans la liste déroulante (ou tout autre nom que vous avez indiqué comme nom cible lors de l’installation d’Oracle 9.2.0.4). Puis cliquez sur Suivant.
- En fonction de votre version, sur l'écran de sélection du produit à installer, sélectionnez 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.

17 Éditez le fichier init.ora pour spécifier le chemin du répertoire dans lequel écrire les données Sentinel archivées. Ces informations sont mentionnées dans le paramètre UTL_FILE_DIR. Vous disposez normalement de l'un des paramètres suivants :

- UTL_FILE_DIR = *

  ou

- UTL_FILE_DIR = <chemin répertoire spécifique>

Sous SUSE Linux (SLES 10)

Pour installer Oracle sous SUSE Linux :

1 Respectez les instructions d'installation fournies dans le manuel d'installation de SLES 10. Installez SLES 10 avec les paquetages par défaut, ainsi qu'Oracle Server Base, le compilateur et les outils C/C++.

2 Loguez-vous comme utilisateur root.

3 Installez le service pack SLES 10. Vérifiez les informations du service pack en entrant :

```
SPident
```

ou

```
cat /etc/SuSE-release
```

Au moment de la publication de cette documentation, le service pack SLES 10 n'était pas encore diffusé. Utilisez la version SPident ou cat/etc/SUSE pour vérifier.

Vous devez obtenir :

```
CONCLUSION: System is up-to-date!
      Found     SLES-10-x86_64-current
```

4 Pour automatiser la plupart des tâches de préinstallation d'Oracle et créer l'utilisateur Oracle, installez orarun.rpm fourni avec SLES 9.

Remarque : consultez le document d'installation d'Oracle pour une liste complète de la configuration requise.

```
rpm -ivh/orarun-1.9-21.2.x86_64.rpm
```

Remarque : orarun est également disponible sur le site http://www.novell.com (http://www.novell.com).

---

5 Le compte de l'utilisateur Oracle est désactivé. Activez-le, en remplaçant le shell /bin/false de l'utilisateur Oracle par /bin/bash à l'aide de l'outil d'administration des utilisateurs de YaST ou en modifiant le fichier /etc/passwd.

6 Définissez un nouveau mot de passe pour l'utilisateur oracle en utilisant YaST ou en entrant :

```
/usr/bin/passwd oracle
```

7. Modifiez au besoin l'environnement Oracle par défaut défini par orarun :
   - Modifiez le répertoire privé d'Oracle en éditant la variable ORACLE_HOME dans le fichier /etc/profile.d/oracle.sh.
   - La valeur ORACLE_SID définie par défaut par le programme d'installation d'orarun est « orcl ». Remplacez-la par ESEC dans le fichier /etc/profile.d/oracle.sh.
8. Pour définir les paramètres kernel, exécutez
   ```
   /usr/sbin/rcoracle start
   ```
9. Passez à l'utilisateur Oracle :
   ```
   su - oracle
   ```
10. Passez au répertoire de la base de données et exécutez ./runinstaller (programme d'installation universel d'Oracle). L'erreur suivante se produit :
11. Corrigez cette erreur en effectuant l'une des opérations suivantes :
    - Modifiez le fichier database/install/oraparam.ini pour ajouter la prise en charge de SUSE Linux 10. Après la modification du fichier oraparam.ini, la ligne [Certified Versions] ressemblera à ceci :
      ```
      [Certified Versions]
      Linux=redhat=3,SuSE-9,SuSE-10,redhat-4,UnitedLinux-1.0.asianux-1,asianux-2
      ```
    - Procédez à l'installation avec l'option -ignoreSysPrereqs
      ```
      i.e. ./runInstaller –ignoreSysPrereqs
      ```
12. Acceptez le répertoire d'inventaire par défaut ou sélectionnez un nouveau répertoire. Cliquez sur Suivant.
13. Parmi les types d'installation, sélectionnez Enterprise Edition. Cliquez sur Suivant.
14. Pour vérifier la configuration réseau requise, sélectionnez User Verified (Vérifié par l'utilisateur). Cliquez sur Suivant.
15. Parmi les options de configuration, sélectionnez Install Database Software only (Installer uniquement le logiciel de la base de données). Cliquez sur Suivant.
16. Le récapitulatif de l'installation s'affiche. Vérifiez-le et cliquez sur Install (Installer).
17. Exécutez les scripts spécifiés comme racine et cliquez sur OK une fois terminé.
18. Une fois l'installation réussie, cliquez sur Quitter.

Sous Red Hat Linux

Pour installer Oracle sous Red Hat Linux :

1. Connectez-vous sous l'ID d'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 /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 système ni dans l'environnement de l'administrateur Sentinel.

```
# Set the LD_ASSUME_KERNEL environment variable only for Red Hat 9,
# RHEL AS 3, and RHEL AS 4 !!
# Use the "Linuxthreads with floating stacks" implementation
instead of NPTL:
# for RH 9 and RHEL AS 3
export LD_ASSUME_KERNEL=2.4.1
# for RHEL AS 4
# export 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
# export TNS_ADMIN= Set if sqlnet.ora, tnsnames.ora, etc. are not
in $ORACLE_HOME/network/admin
export NLS_LANG=AMERICAN;
export ORA_NLS33=$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
# Set shell search paths
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 gcc ou 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 Sortez 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 chez Oracle.

```
su - root
unzip p3006854_9204_LINUX.zip
```

```
cd 3006854
sh rhel3_pre_install.sh
```

12. Sortez 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 9.2.0.7 à Oracle, à partir du disque 1 de la distribution du correctif Oracle 9.2.0.7, exécutez le script :
    ```
    ./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 Spécifiez l'emplacement des fichiers, sélectionnez comme nom cible « OUIHome » dans la liste déroulante (ou tout autre nom que vous avez indiqué comme nom cible lors de l'installation d'Oracle 9.2.0.4). Puis cliquez sur Suivant.
    - En fonction de votre version, sur l'écran de sélection du produit à installer, sélectionnez 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.

20 Déconnectez gcc :

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

21 Sortez pour retourner à l'invite d'utilisateur oracle.

```
Exit
```

22 Éditez le fichier init.ora pour spécifier le chemin du répertoire dans lequel écrire les données Sentinel archivées. Ces informations sont mentionnées dans le paramètre UTL_FILE_DIR. Vous disposez normalement de l'un des paramètres suivants :

- UTL_FILE_DIR = *

ou

- UTL_FILE_DIR = [chemin de répertoire spécifique]

Sous Solaris

Pour installer Oracle sous Solaris :

1 Connectez-vous sous l'ID d'utilisateur root.

2 Suivez la procédure prévue dans Oracle Note 148673.1 SOLARIS: Quick Start Guide (Note Oracle 148673.1 SOLARIS : démarrage rapide).

3 Installez Oracle 9i Release 2 (9.2.0.1) comme utilisateur Oracle. Une invite vous demande deux CD-ROM supplémentaires. Vous devez naviguer vers des répertoires différents pour chaque CD-ROM supplémentaire.

4 Appliquez le correctif Oracle 9.2.0.7. Reportez-vous à la documentation Oracle pour les procédures des correctifs.

5 Pour vérifier le niveau de correctif, comme utilisateur oracle UNIX, entrez :

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

Les résultats doivent indiquer la version 9.2.0.7. Pour quitter, entrez Quit.

6 Éliminez le répertoire créé pour le correctif.

7 Après l'installation des correctifs, éliminez les répertoires et fichiers de correctif.

8 Éditez le fichier init.ora pour spécifier le chemin du répertoire dans lequel écrire les données Sentinel archivées. Ces informations sont mentionnées dans le paramètre UTL_FILE_DIR. Vous disposez normalement de l'un des paramètres suivants :

- UTL_FILE_DIR = *

ou

- UTL_FILE_DIR = [chemin répertoire spécifique]

9 Redémarrer.

3.3 Installation de Sentinel

Sentinel prend en charge deux types d'installation. Il s'agit des champs suivants :

- **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.

- **Personnalisé:** permet une installation totalement distribuée.

3.3.1 Installation simple

Après avoir satisfait à la configuration requise mentionnée à la section précédente, vous pouvez procéder à l'installation de Sentinel.

Pour installer Sentinel :

1. Loguez-vous comme utilisateur root sous Solaris/Linux ou comme administrateur sous Windows.
2. Insérez et montez le CD d'installation de Sentinel.
3. Sous Linux/Solaris, assurez-vous que l'umask système est défini sur 0027 en exécutant la commande suivante à l'invite de commande à partir de laquelle vous exécutez le programme d'installation :

   ```
   umask 0027
   ```
4. Démarrez le programme d'installation en accédant au répertoire d'installation sur le CD-ROM et
   - sous Windows, exécutez setup.bat
   - sous Solaris/Linux :

   En mode GUI :

   ```
   ./setup.sh
   ```

   ou

   En mode texte (« console série ») :

   ```
   ./setup.sh –console
   ```
5. Cliquez sur la flèche bas et sélectionnez une des langues suivantes au choix.

Anglais	Italien
Français	Portugais (Brésil)
Allemand	Espagnol
Chinois simplifié	Japonais
Chinois traditionnel	

6. Après avoir lu l'écran d'accueil, cliquez sur Suivant.
7. Lisez et acceptez l'accord de licence utilisateur final, puis cliquez sur Suivant.
8. Acceptez le répertoire d'installation par défaut ou cliquez sur Parcourir afin d'indiquer l'emplacement de l'installation. Cliquez sur Suivant.
9. Sélectionnez Simple. Cliquez sur Suivant.
10. Dans cet écran, entrez les informations de configuration et cliquez sur Suivant.
    - Numéro de série
    - la clé de licence
    - Serveur SMTP

- E-mail

  Le nom DNS ou l'adresse IP du serveur SMTP entré ici vous aidera à configurer l'envoi de courriers électroniques à partir de Sentinel via l'ID de courrier électronique entré ici.

- Mot de passe système global

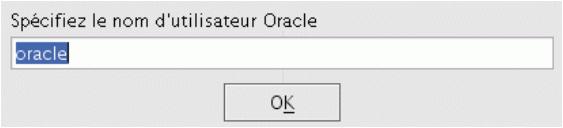
  Le mot de passe entré ici sera valable pour tous les utilisateurs par défaut, y compris l'administrateur Sentinel et les utilisateurs de la base de données. Pour plus d'informations sur la liste des utilisateurs de base de données par défaut créée pendant l'installation, reportez-vous à la Section 3.4.2, « Base de données Sentinel », page 73.

- Nom d'utilisateur et mot de passe Advisor

  Pour installer Advisor, entrez le nom d'utilisateur et le mot de passe qui vous ont été fournis à l'achat du logiciel. 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.

Remarque : si vous installez Advisor, l'installation de type Simple configure Advisor pour utiliser le téléchargement direct sur Internet avec un intervalle de mise à jour de 12 heures et toutes les notifications par message électronique activées.

Sous Solaris/Linux, vous serez invité à spécifier le nom d'utilisateur Oracle. Entrez-le, puis cliquez sur OK.

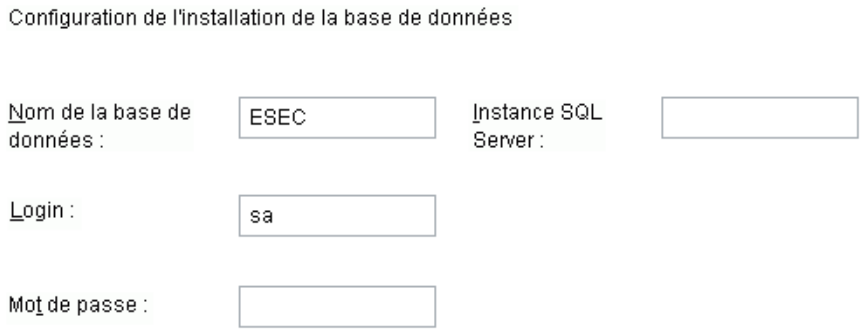


11 Pour la configuration de la base de données :

- Sélectionnez la plate-forme de la base de données cible.
- Entrez le nom de la base de données
  - Sous Linux/Solaris, spécifiez le fichier Oracle JDBC Driver.
  - Sous Windows, entrez les références de l'utilisateur de la base de données et le nom de l'instance SQL Server.

Cliquez sur Suivant.

En cas d'installation simple, la taille de la base de données est de 10 Go.



12 Un récapitulatif des paramètres de la base de données sélectionnés s'affiche. Cliquez sur Suivant. :

13 Un récapitulatif de l'installation s'affiche. Cliquez sur Installer.

14 Une fois l'installation réussie, cliquez sur Terminer

3.3.2 Installation personnalisée

Après avoir satisfait à la configuration requise mentionnée à la section précédente, vous pouvez procéder à l'installation de Sentinel.

Pour installer Sentinel :

1 Loguez-vous comme utilisateur root sous Solaris/Linux ou comme administrateur sous Windows.

2 Insérez et montez le CD d'installation de Sentinel.

3 Sous Linux/Solaris, assurez-vous que l'umask système est défini sur 0027 en exécutant la commande suivante à l'invite de commande à partir de laquelle vous exécutez le programme d'installation :

```
umask 0027
```

4 Démarrez le programme d'installation en accédant au répertoire d'installation sur le CD-ROM et

- sous Windows, exécutez setup.bat
- sous Solaris/Linux :

En mode GUI :

```
./setup.sh
```

ou

En mode texte (« headless ») :

```
./setup.sh –console
```

5 Cliquez sur la flèche bas et sélectionnez une des langues suivantes au choix.

Anglais	Italien
Français	Portugais (Brésil)
Allemand	Espagnol
Chinois simplifié	Japonais
Chinois traditionnel	

6 Après avoir lu l'écran d'accueil, cliquez sur Suivant.

7 Lisez et acceptez l'accord de licence utilisateur final, puis cliquez sur Suivant.

8 Acceptez le répertoire d'installation par défaut ou cliquez sur Parcourir afin d'indiquer l'emplacement de l'installation. Cliquez sur Suivant.

9 Sélectionnez Personnalisé. Cliquez sur Suivant.

10 Sélectionnez les composants de Sentinel à installer.

Remarque : pour plus d'informations sur l'installation de chaque composant pour diverses configurations, reportez-vous au Chapitre 2, « Meilleures pratiques », page 19 du guide d'installation.

Les options disponibles sont les suivantes :

base de données – il installe la base de données Sentinel	Sentinel Collector Service
Communication Server – installe le bus de message (iSCALE) et DAS Proxy	Générateur de collecteurs
Advisor	Centre de contrôle Sentinel
Moteur de corrélation	Gestionnaire de données Sentinel
DAS (pour la communication avec la base de données)	HP OpenView Service Desk
	Remedy Integration

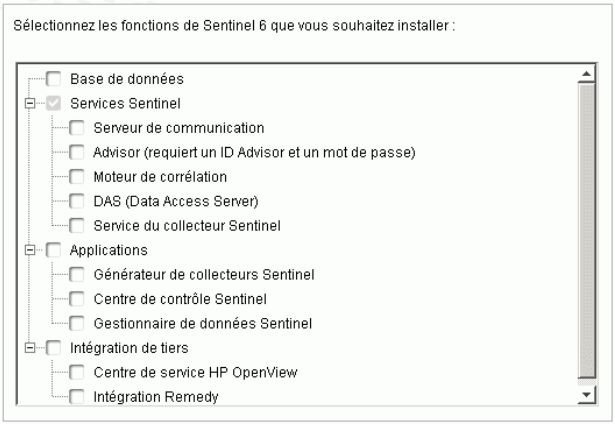
Remarque : pour plus d'informations sur l'installation de HP OpenView Service Desk ou de Remedy Integration, reportez-vous au guide d'intégration de produits tiers.

Remarque : lorsque vous sélectionnez ou désélectionnez un composant, vous constaterez un certain retard au niveau de l'interface.

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 : dans le cadre de l'installation du composant Sentinel Database, le programme d'installation place des fichiers dans le dossier %ESEC_HOME%\db.

Remarque : dans le cas d'une installation simple, la taille de la base de données pour MSSQL et ORACLE est de 10 Go.



11 Si vous avez sélectionné l'installation de DAS, vous devrez compléter les champs suivants :

- Numéro de série

- la clé de licence

12 Si vous avez sélectionné l'installation de composants d'intégration tiers, vous devrez fournir un mot de passe pour déverrouiller les composants d'intégration tiers sélectionnés. Pour plus d'informations, reportez-vous au guide d'intégration de produits tiers.

13 Sous Linux/Solaris, 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'administrateur du système d'exploitation – par défaut /export/home. Si le nom d'utilisateur est esecadm, le répertoire privé de l'utilisateur est /export/home/esecadm.

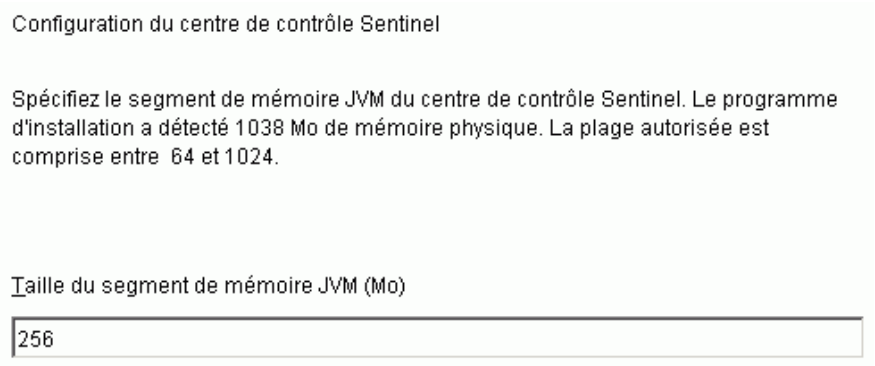
Remarque : pour répondre aux configurations de sécurité strictes requises par la certification des critères communs, reportez-vous à la section Définition de mots de passe – Meilleures pratiques du Chapitre 2, « Meilleures pratiques », page 19.

Remarque : l'utilisateur esecadm sera créé sans configuration de mot de passe. Pour se loguer comme utilisateur esecadm, vous devez d'abord configurer son mot de passe.

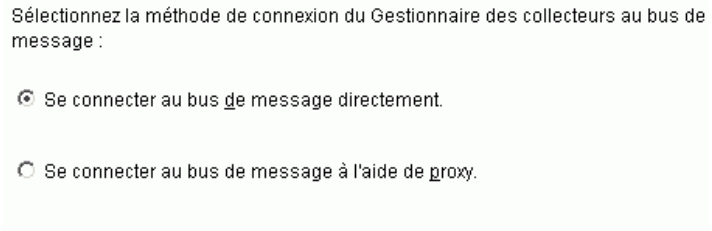
---

14 Si vous avez choisi d'installer Sentinel Control Center, le programme d'installation vous invite à entrer l'espace mémoire maximal à allouer à Sentinel Control Center. Indiquez la taille du segment de mémoire JVM (Mo) qui sera utilisée uniquement par Sentinel Control Center.

- Taille du segment de mémoire JVM (Mo) : par défaut, elle correspond à la moitié de la taille de la mémoire physique détectée sur la machine, avec un maximum de 1 024 Mo.



15 Deux options permettent d'établir la communication entre le serveur et les clients Sentinel. Vous pouvez sélectionner une communication directe avec le bus de message ou via proxy. Pour plus d'informations sur ces deux options, reportez-vous au Chapitre 8, « Couche de communication (iSCALE) », page 103 du guide d'installation.



16 Vous êtes invité à entrer les informations relatives au nom du serveur hôte/port. Entrez les informations requises et cliquez sur Suivant. Si vous sélectionnez une communication via proxy, vous serez invité à entrer également le port proxy du centre de contrôle Sentinel.

- Port du bus de message : port sur lequel le bus de message écoute. Il est utilisé par les composants qui se connectent directement au bus de message.
- Port proxy du centre de contrôle Sentinel : port que le serveur proxy SSL (DAS Proxy) écoute pour accepter les connexions authentifiées basées sur un nom d'utilisateur et un mot de passe. Étant donné que Sentinel Control Center vous invite à entrer un nom d'utilisateur et un mot de passe, il utilise ce port pour se connecter à Sentinel Server.
- Port proxy d'authentification basée sur un certificat : port que le serveur proxy SSL (DAS Proxy) écoute pour accepter les connexions authentifiées basées sur un certificat. Étant donné que Collector Manager ne peut pas vous inviter à entrer un nom d'utilisateur et un mot de passe, il utilise ce port pour se connecter à Sentinel Server s'il est configuré pour une connexion via proxy.

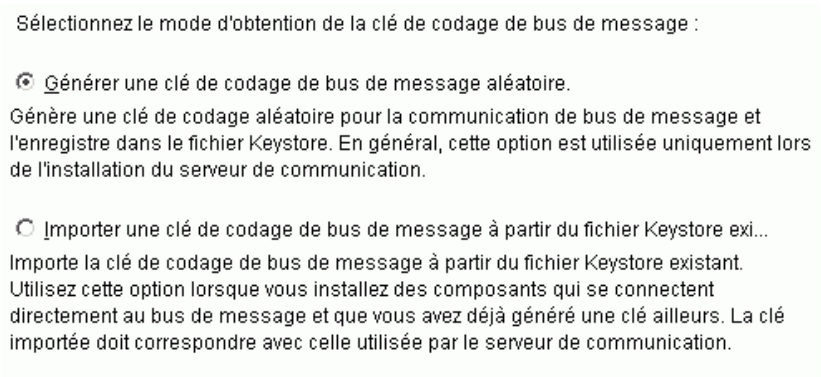
Remarque : les numéros de port doivent être identiques sur chaque machine du système Sentinel pour permettre les communications. Conservez ces informations pour les installations futures sur d'autres machines.

---

17 Si vous installez un composant qui établira une connexion directe au bus de message ou si vous installez Communication Server, vous devez indiquer comment obtenir la clé de codage de bus de message partagée :

- Générer une clé de codage aléatoire (option recommandée lors de l'installation de Communication Server)
- Importer une clé de codage à partir du fichier Keystore (option recommandée lors de l'installation d'autres composants). Vous serez invité à sélectionner le fichier à partir duquel importer la clé de codage.
- Le fichier .keystore se trouve dans le répertoire $ESEC_HOME/config sous Linux et Solaris ou dans %le répertoire ESEC_HOME%\config sous Windows.

18 Indiquez si vous souhaitez générer un fichier Keystore aléatoire ou importer un fichier existant à partir d'une autre machine du système Sentinel.



Remarque : tous les composants se connectant directement au bus de message doivent partager la même clé de codage. Novell recommande de générer une clé de codage aléatoire lors de l'installation de Communication Server et de l'importer lors de l'installation de

composants sur d'autres machines. Les composants qui se connectent via le proxy n'ont pas besoin de la clé de codage de bus de message partagée.

---

19 Si vous choisissez d'importer un fichier Keystore existant, vous devez accéder à son emplacement et sélectionner le fichier désiré. Cliquez sur Suivant.

20 Si vous choisissez d'installer DAS (Data Access Service), sélectionnez la quantité de RAM du système que vous souhaitez lui allouer. Pour les environnements distribués, il est recommandé de sélectionner la quantité de mémoire maximale, étant donné que la base de données exige une certaine quantité de mémoire.

21 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 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 : nom ou adresse IP de la base de données Sentinel existante à laquelle vous souhaitez connecter le composant DAS.
- Nom de la base de données : nom de l'instance de la base de données Sentinel à laquelle vous souhaitez connecter le composant DAS (par défaut, ESEC).
- Port de la base de données (par défaut : Microsoft SQL:1433 et Oracle:1521)
- Utilisateur de la base de données de l'application Sentinel : indiquez le login esecapp et entrez le mot de passe fourni à cet utilisateur lors de l'installation de la base de données Sentinel.

22 Configurez la base de données pour l'installation :

Sous Windows :

- Sélectionnez Microsoft SQL Server 2005 comme plate-forme du serveur de base de données cible.
  - Créer une nouvelle base de données avec les objets de la base de données : crée une nouvelle base de données Microsoft SQL et la remplit avec des objets de la base de données.
  - Ajouter les objets de la base de données à une base de données vide existante : ajoute uniquement les objets de la base de données à une base de données Microsoft SQL 2005 existante. la base de données existante doit être vide.
  - Spécifiez le répertoire du journal de l'installation de la base de données.

Cliquez sur Suivant.

- Spécifiez l'emplacement de stockage pour les éléments suivants :
  - Répertoire de données
  - Répertoire d'index
  - Répertoire des données du récapitulatif
  - Répertoire des index récapitulatifs
  - Répertoire du journal

Cliquez sur Suivant.

- Sélectionnez l'option de prise en charge de jeux de caractères par la base de données, à savoir Unicode ou ASCII seulement. Si vous sélectionnez des langues non asiatiques (langues autres que le chinois simplifié/traditionnel et le japonais dans la liste), le système

vous invite à choisir entre des bases de données Unicode et non Unicode. Sélectionnez un format de base de données, puis cliquez sur OK.

Remarque : pour installer une base de données Unicode, vous aurez besoin de davantage d'espace disque.

Remarque : si vous sélectionnez une langue asiatique, la base de données installée par défaut est Unicode. Cliquez sur Suivant.

- Spécifiez la taille de la base de données. Cliquez sur Suivant.
- Configurez les partitions de la base de données.
  - Vous pouvez choisir d'activer la gestion de partition automatique de base de données.
  - Pour les partitions de données, spécifiez le répertoire d'archivage ; entrez des données temporelles pour l'ajout et l'archivage des données.

Cliquez sur Suivant.

Sous Linux/Solaris :

- Sélectionnez la plate-forme du serveur de base de données cible.
  - Sélectionnez Oracle 10g dans la liste déroulante.
  - Sélectionnez Créer une nouvelle base de données avec les objets de la base de données.

Cliquez sur Suivant.

- Spécifiez le nom de l'utilisateur Oracle ou acceptez le nom d'utilisateur par défaut. Cliquez sur OK
- Si vous choisissez de créer une nouvelle base de données, entrez ce qui suit :
  - **Chemin du fichier du pilote JDBC d'Oracle :** (le nom du fichier JAR est généralement 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:** nom d'hôte de la machine sur laquelle installer la base de données. Le programme d'installation prend uniquement en charge la création d'une instance de base de données sur l'hôte local.
  - **Nom base de données** nom de l'instance de base de données à installer.
- 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 :

  Chemin du fichier du pilote JDBC d'Oracle : (le nom du fichier JAR est généralement 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 ou adresse IP de la base de données : nom ou adresse IP de l'hôte contenant 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 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.

port de base de données: La valeur par défaut est 1521

Mot de passe : pour 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.

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.

Remarque : le programme d'installation sauvegarde les fichiers tnsnames.ora et listener.ora dans le répertoire $ORACLE_HOME/network/admin. Il remplace le fichier listener.ora avec les informations de connexion de la base de données Sentinel, et ajoute ces informations au fichier tnsnames.ora. Si d'autres bases de données sont installées sur le même serveur que la base de données Sentinel, l'administrateur doit fusionner manuellement les informations des fichiers listener.ora sauvegardés dans le nouveau fichier et redémarrer le processus d'écoute Oracle, pour que les autres applications puissent continuer à se connecter à la base de données.

- Lors de la création d'une base de données, vous pouvez accepter l'espace mémoire et le port d'écoute par défaut ou en définir d'autres.
- Entrez l'utilisateur SYS et ses références, puis cliquez sur Suivant.
- Spécifiez la taille de la base de données. Vous avez le choix entre une taille standard, large ou personnalisée. Si vous optez pour une taille personnalisée, vous êtes invité à spécifier les valeurs suivantes :
  - 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)
- Spécifiez la taille totale de la base de données allouée aux espaces de table Événement et Récapitulatif d'événements.
- Spécifiez l'emplacement de stockage pour les éléments suivants :
  - Répertoire de données
  - Répertoire d'index
  - Répertoire des données du récapitulatif
  - Répertoire des index récapitulatifs
  - Répertoire du journal

  Cliquez sur Suivant.

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.

Pour des raisons de performances, le journal des modifications doit pointer vers le disque accessible en écriture le plus rapide.

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 <directory_path>
chmod –R 770 <directory_path>
```

- Partez du principe qu'« oracle » est le nom d'utilisateur Oracle et « dba » est le nom de groupe « oracle ».
- Configurez les partitions de la base de données.
  - Choisissez d'activer la gestion de partition automatique de base de données.
  - Spécifiez le répertoire d'archivage des partitions de données.
  - Spécifiez des données temporelles pour l'ajout et l'archivage des données.

  Cliquez sur Suivant.

23 Entrez les informations d'authentification pour :

- l'administrateur de la base de données Sentinel ;
- l'utilisateur de base de données de l'application Sentinel ;
- l'administrateur de Sentinel ;
- l'utilisateur de rapports Sentinel.

Cliquez sur Suivant.

24 Un récapitulatif des paramètres spécifiés pour la base de données s'affiche. Cliquez sur Suivant.

25 Si vous choisissez d'installer le DAS, configurez le support du courrier électronique Sentinel. Spécifiez le serveur SMTP et l'adresse de messagerie de l'expéditeur que le service d'exécution doit utiliser pour envoyer des messages (facultatif – vous pouvez modifier ces valeurs manuellement après l'installation [$ESEC_HOME\sentinel\config\execution.properties sous Linux/Solaris et %ESEC_HOME%\sentinel\config\execution.properties sous Windows.])

26 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.
- **indépendante:** Advisor est configuré comme un système isolé qui requiert une intervention manuelle pour recevoir une mise à jour de Sentinel.

27 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. Cliquez sur Suivant. Un message vous demande si vous voulez continuer (déconseillé), si votre nom d'utilisateur et votre mot de passe ne sont pas vérifiés. 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.

28 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 modifier les adresses électroniques Advisor en éditant les fichiers attackcontainer.xml et alertcontainer.xml. Pour plus d'informations, reportez-vous à la section relative à l'"onglet Advisor" dans le Guide de l'utilisateur de 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.

  Remarque : Les notifications d'erreurs sont toujours envoyées.

29 Cliquez sur Suivant. Un écran récapitulatif indiquant les fonctionnalités sélectionnées pour l'installation s'affiche. Cliquez sur Installer.

Remarque : Si vous choisissez d'installer HP OpenView Service Desk ou Remedy Integration, une invite vous demande des informations supplémentaires. Pour plus d'informations, reportez-vous au Guide d'intégration de produits tiers de Sentinel.

30 Une fois l'installation réussie, vous êtes invité à redémarrer. Cliquez sur Terminer pour redémarrer le système.

Remarque : 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.

Remarque : si vous prévoyez un haut débit d'événements (supérieur à 500 événements par seconde), vous devez suivre les instructions de configuration supplémentaires de la section "Setting up the Oracle Call Interface (OCI) Event Insertion Strategy in Database Creation [Configuration de la stratégie d'insertion d'événement OCI (Oracle Call Interface) lors de la création d'une base de données]."

Installation de la console sous Linux/Solaris

```
Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
   To select/deselect a feature or to view its children, type its
number:
     1.  [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0] 2
    1. Deselect 'Sentinel Services'
    2. View 'Sentinel Services' subfeatures
   Enter command [1] 2
```

```
Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1. [ ] Communication Server
        2. [ ] Advisor (Install requires Advisor ID and Password)
        3. [x] Correlation
        4. [x] DAS
        5. [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] 1

Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1. [x] Communication Server
        2. [ ] Advisor (Install requires Advisor ID and Password)
        3. [x] Correlation
        4. [x] DAS
        5. [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] -1

Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
   To select/deselect a feature or to view its children, type its
number:
     1. [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0]
```

Installation du client

Sentinel Control Center, Collector Builder et Sentinel Data Manager peuvent être installés à l'aide du programme d'installation complet ou client seulement. Le premier permet de choisir parmi les trois applications tandis que le second les installe toutes automatiquement.

Remarque : étant donné que le programme d'installation client seulement inclut automatiquement Collector Builder, il ne peut être utilisé que sous des systèmes d'exploitation Windows. Toutes ces applications Windows peuvent fonctionner avec un serveur Sentinel Linux.

Pour installer Sentinel Control Center et Collector Builder à l'aide du programme d'installation client seulement :

1. Accédez au CD et exécutez setup.sh (sous Linux et Solaris) ou setup.bat (sous Windows). L'Assistant d'installation s'ouvre.
2. Sélectionnez la langue de l'Assistant, puis cliquez sur OK.
3. L'écran de bienvenue de Sentinel s'affiche. Après avoir lu l'écran d'accueil, cliquez sur Suivant.
4. L'écran de l'accord de licence utilisateur final de Sentinel s'affiche. Lisez et 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. Entrez l'adresse de l'hôte sur lequel Communication Server est installé.
7. Sélectionnez Générer un fichier keystore aléatoire, puis cliquez sur Suivant.
8. Cliquez sur Suivant.
9. Un récapitulatif de l'installation s'affiche. Cliquez sur Installer.
10. Une fois l'installation réussie, cliquez sur Terminer

3.4 Configuration de post-installation

3.4.1 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 :

Remarque : cet exemple concerne une installation sous Linux/Solaris. Une configuration similaire doit être effectuée sous Windows.

1. Sur la machine où DAS est installé, loguez-vous en tant qu'administrateur Sentinel et accédez à :

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

2. Exécutez mailconfig de la façon suivante :

   ```
   ./mailconfig.sh -host <SMTP Server> -from <source email address> -user <mail authentication user> –password
   ```

Exemple:

```
./mailconfig.sh -host 10.0.1.14 -from my_name@domain.com -user
my_user_name –password
```

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

```
Enter your password:*********
Confirm your password:*********
```

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 DAS est installé, loguez-vous en tant qu'administrateur Sentinel et accédez à :

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

2. Exécutez mailconfigtest de la façon suivante :

   ```
   ./mailconfigtest.sh -to <destination email address>
   ```

   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.

   ```
   Email has been sent successfully!
   ```

   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 :

   ```
   Subject: Testing Sentinel mail property
   This is a test for Sentinel mail property set up. If you see this
   message, your Sentinel mail property has been configured correctly
   to send emails
   ```

3.4.2 Base de données Sentinel

Remarque : par défaut, le programme d'installation active la croissance automatique pour tous les espaces de table. La taille de croissance de fichier par défaut est de 200 Mo, mais la taille maximale de fichier dépend de la valeur indiquée lors de l'installation (par exemple, 2 000 Mo).

La gestion de partition automatique de la base de données Sentinel (archivage, déplacement et ajout des partitions) doit être programmée pour contrôler la taille des donnés d'événements. Elle peut être configurée à l'aide de Sentinel Data Manager (SDM).

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

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 accordé à l'utilisateur de la base de données Sentinel 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 compte utilisateur diffère de celui de l'administrateur Sentinel du système d'exploitation.

- **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.

3.4.3 Service de collecteurs

Lors de l'installation du service Collector, un collecteur nommé Collecteur général est configuré. Ce collecteur peut être utilisé pour tester l'installation.

Remarque : Pour plus d'informations, reportez-vous à Chapitre 5, « Tester l'installation », page 81

Remarque : pour plus d'informations sur les collecteurs, consultez le site http://support.novell.com/products/sentinel/collectors.html (http://support.novell.com/products/sentinel/collectors.html).

3.4.4 Mise à jour de la clé de licence (à partir de la clé d'évaluation)

Si vous vous procurez le produit après l'avoir évalué, suivez la procédure décrite ci-dessous pour mettre à jour votre clé de licence dans le système afin d'éviter une réinstallation.

Pour mettre à jour la clé de licence :

1. Loguez-vous en tant qu'esecadm à la machine hébergeant le composant DAS.
2. À l'invite de commande, accédez au répertoire $ESEC_HOME/bin.
3. Démarrez l'exécutable/softwarekey. Le menu suivant s'affiche. Veuillez complétez les informations demandées.
   - Enter Primary Key (Entrer une clé primaire)
   - Enter Secondary Key (Entrer une clé secondaire)
   - View Primary Key (Afficher une clé primaire)
   - View Secondary Key (Afficher une clé secondaire)
   - Quitter
4. Tapez 1 pour entrer une nouvelle clé primaire.

Configuration de l’Advisor

4

Rubriques traitées dans ce chapitre :

Ce chapitre explique comment configurer Sentinel pour exécuter les rapports Advisor directement à partir de Sentinel Control Center. Ces rapports sont créés par Novell à des fins de compte rendu et d'analyse. Une fois l'intégration à Sentinel Control Center configurée correctement, ils s'affichent sous l'onglet Advisor.

4.1 Présentation d'Advisor

Sentinel Advisor fournit des données en temps réel couvrant les vulnérabilités de l'entreprise, ainsi que des conseils d'expert et recommande des mesures de résolution de problèmes. Advisor fournit un système de détection des intrusions, un renvoi réciproque entre les signatures d’attaque IDS en temps réel et la base de connaissances d’Advisor sur des vulnérabilités.

Remarque : L’installation d’Advisor est facultative. Cependant, il reste un composant nécessaire si vous voulez utiliser la détection d’exploits Sentinel ou les fonctions de création de rapports Advisor. Advisor est un service de données basé sur une formule d'abonnement.

Les systèmes pris en charge sont les suivants :

Systèmes de détection d'intrusions	Scanners de vulnérabilité
Cisco Secure IDS	eEYE Retina
Enterasys Dragon Host Sensor	Foundstone Foundscan
Enterasys Dragon Network Sensor	ISS Database Scanner
Intrusion.com (SecureNet_Provider)	ISS Internet Scanner
ISS BlackICE	ISS System Scanner
ISS RealSecure Desktop	ISS Wireless Scanner
ISS RealSecure Network	Nessus
ISS RealSecure Server	nCircle IP360
ISS RealSecure Guard	Qualys QualysGuard
Snort	**Pare-feux**
Symantec Network Security 4.0 (ManHunt)	Cisco IOS Firewall
Symantec Intruder Alert	
McAfee IntruShield	

4.2 Installation de l’Advisor

Remarque : Advisor doit être installé sur la même machine que DAS (Database Access Service).

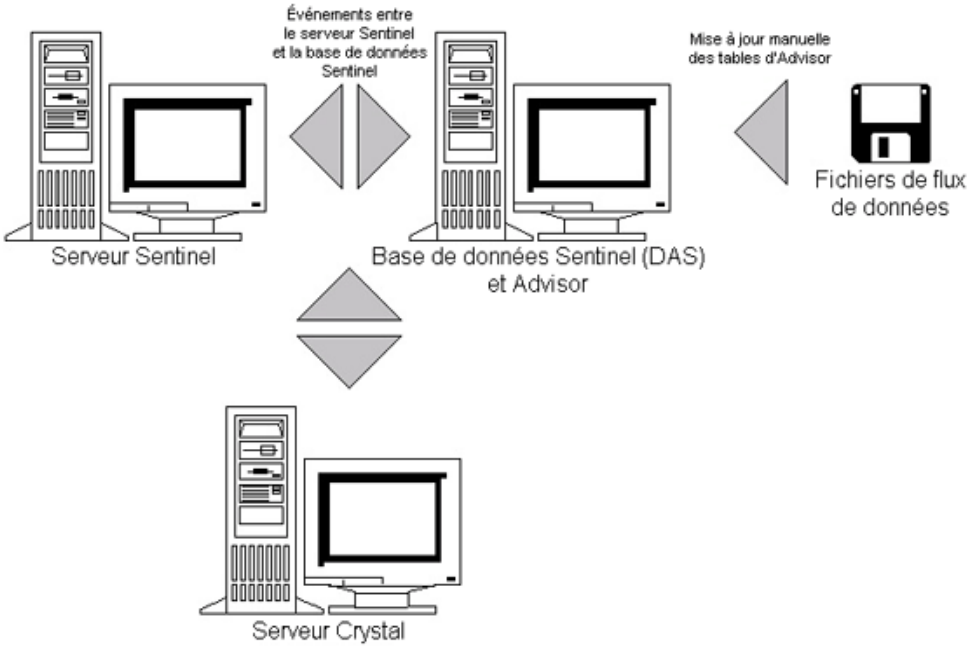
Vous avez le choix entre deux options d'installation, à savoir :

- indépendante
- téléchargement direct d’Internet

Remarque : avant d’installer l’Advisor, vérifiez que vous avez l’ID Advisor et le mot de passe de qui vous ont été assignés par Novell. Pendant l’installation, un invite vous demande le nom d’utilisateur et le mot de passe.

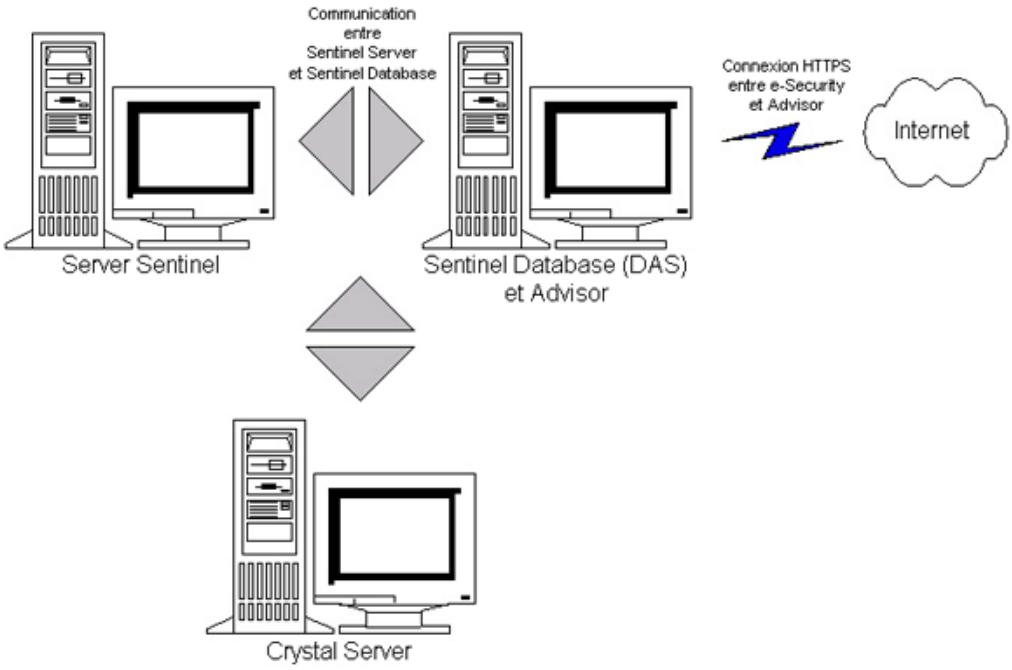
4.2.1 Configuration indépendante

À l’installation indépendante, l’Advisor est un système isolé qui requiert une intervention manuelle pour recevoir des mises à jour de Novell.



4.2.2 Configuration de téléchargement direct d’Internet

Au téléchargement direct d’Internet, 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.



4.3 Rapports Advisor

Crystal BusinessObjects Enterprise™ XI est l'outil de création de rapport intégré à Sentinel. Pour plus d'informations sur l'installation de Crystal BusinessObjects Enterprise™ XI, reportez-vous au Chapitre 9, « Crystal Reports pour Windows », page 109 et au Chapitre 10, « Crystal Reports pour Linux », page 137 dans le Guide d'installation.

Remarque : Crystal Server n'est requis que si vous prévoyez d'exécuter des rapports. Si vous n'allez utiliser Advisor que pour la détection d'exploits, il n'est pas nécessaire d'installer un serveur Crystal.

Pour exécuter Crystal Reports sur Advisor :

- Installez et configurez Crystal Server. Pour plus d'informations, reportez-vous au Chapitre 9, « Crystal Reports pour Windows », page 109du Guide d'installation.
- Publiez Advisor Crystal Reports sur Crystal Server. Pour plus d'informations, reportez-vous à la section relative à l'importation des modèles de rapport.

4.3.1 Configuration des rapports Advisor

Si vous voulez exécuter des rapports Advisor (Crystal Reports), effectuez la procédure suivante dans l'ordre indiqué. Vous n'avez pas besoin d'effectuer la procédure suivant si vous ne voulez utiliser Advisor que pour la détection d'exploits.

- Si ce n'est pas déjà fait, effectuez les actions suivantes (pour plus d'informations, reportez-vous au Chapitre 9, « Crystal Reports pour Windows », page 109 dans le Guide d'installation) :
  - Installez Microsoft Internet Information Server (IIS)
  - Installez Crystal BusinessObjects Enterprise™ 11

- Pour la base de données Sentinel sous Oracle (Solaris/Linux) – Configurez le pilote natif Oracle (pour les installations Oracle)
- Pour la base de données Sentinel sous Microsoft SQL 2005 (Windows) – Configurer ODBC (Open Database Connectivity)
- Appliquez le correctif à Crystal Reports. Pour plus d'informations, reportez-vous au Chapitre 9, « Crystal Reports pour Windows », page 109 du Guide d'installation.

- Installez Advisor – Pour plus d'informations sur l'installation d'Advisor, reportez-vous au Chapitre 7, « Installation des composants Sentinel », page 97 du Guide d'installation.
- Importez les modèles Crystal Report
- Créez une page Web Crystal
- Configurez Sentinel Control Center pour intégrer le serveur Crystal Enterprise

---

Remarque : pour plus d'informations sur l'importation de modèles de rapport et la configuration de Sentinel Control Center pour l'affichage des rapports Advisor, reportez-vous au Chapitre 9, « Crystal Reports pour Windows », page 109 et au Chapitre 10, « Crystal Reports pour Linux », page 137 du Guide d'installation.

4.4 Mise à jour de données sur les tables Advisor

Sauf si vous avez une configuration indépendante, les données sur les tables Advisor sont mises à jour automatiquement pendant le suivant téléchargement d'alimentation Advisor programmé. Cependant, les données peuvent être mises à jour manuellement. Pour plus d'informations sur la mise à jour manuelle, reportez-vous à la section « Advisor Usage and Maintenance » (Utilisation et maintenance d'Advisor) dans le guide de l'utilisateur de Sentinel.

4.5 Réinitialiser le mot de passe Advisor (seulement téléchargement direct)

Si vous exécutez Advisor sous le mode de téléchargement direct et vous venez d'obtenir un nouveau mot de passe Advisor ou le mot de passe Advisor défini pendant l'installation est incorrect, vous devez réinitialisez le mot de passe Advisor codifié enregistré dans de fichier de configuration de l'Advisor.

La mise à jour du mot de passe Advisor codifié n'est pas applicable si vous exécutez Advisor sous une configuration indépendante parce que, sous ce mode-là, le mot de passe n'est pas enregistré dans le fichier de configuration Advisor.

Pour réinitialiser le mot de passe Advisor codifié enregistré dans le fichier de configuration Advisor, effectuez les étapes suivantes :

1. Sur UNIX, loguez-vous comme esecadm ou sur Windows, loguez-vous comme utilisateur aux droits administratifs. Loguez-vous sur la machine oÃƒÂ¹ l'Advisor est installÃƒÂ©.
2. Instructions d'installation:

   Pour UNIX :

   ```
   $ESEC_HOME/bin
   ```

   Pour Windows:

```
%ESEC_HOME%\bin
```

3 Exécutez la commande suivante :

Pour UNIX :

```
./adv_change_passwd.sh <newpassword>
```

Pour Windows:

```
adv_change_passwd.bat <newpassword>
```

où <nouveau_mot_de_passe> correspond au mot de passe Advisor que vous souhaitez définir.

Tester l’installation

5

Rubriques traitées dans ce chapitre :

5.1 Tester l’installation

Sentinel est installé avec un collecteur de démonstration qui permet de tester de nombreuses fonctions de base du système. À l'aide de ce collecteur, vous pouvez tester Active Views, la création d'incidents, les règles de corrélation et les rapports. La procédure suivante décrit la procédure pour tester le système et les résultats attendus. Il se peut que vous n'obteniez pas exactement les mêmes événements, mais vos résultats doivent être similaires à ceux ci-dessous.

Au niveau de base, ces tests vous permettent de vérifier les points suivants :

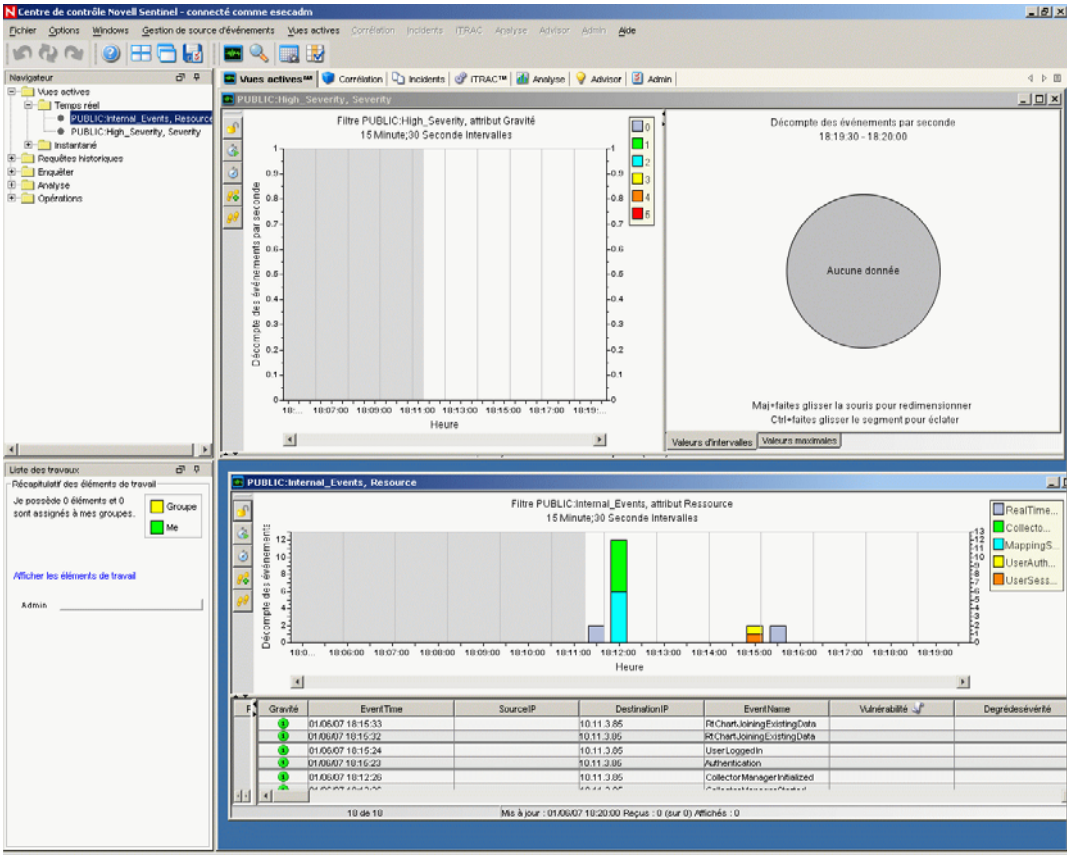
- les services Sentinel sont en fonctionnement ;
- la communication via le bus de message est fonctionnelle ;
- des événements d'audit interne sont envoyés ;
- des événements peuvent être envoyés à partir de Collector Manager ;
- des événements sont insérés dans la base de données et peuvent être récupérés à l'aide d'une requête d'événements historiques ou du serveur de création de rapport ;
- il est possible de créer et de visualiser des incidents ;
- Correlation Engine évalue les règles et déclenche des événements corrélés ;
- Sentinel Data Manager parvient à se connecter à la base de données et à lire les informations de partition.

Si l'un de ces tests échoue, consultez le journal de l'installation et les autres fichiers journaux, et contactez le support technique Novell si nécessaire.

Pour tester l'installation :

1 Double-cliquez sur l'icône de Sentinel Control Center sur le Bureau.

2 Loguez-vous au système comme l'administrateur Sentinel spécifié lors de l'installation (esecadm par défaut). Sentinel Control Center s'ouvre et affiche l'onglet Active Views présentant une fenêtre intitulée « PUBLIC:All, Severity » (PUBLIC : Tout, Gravité).

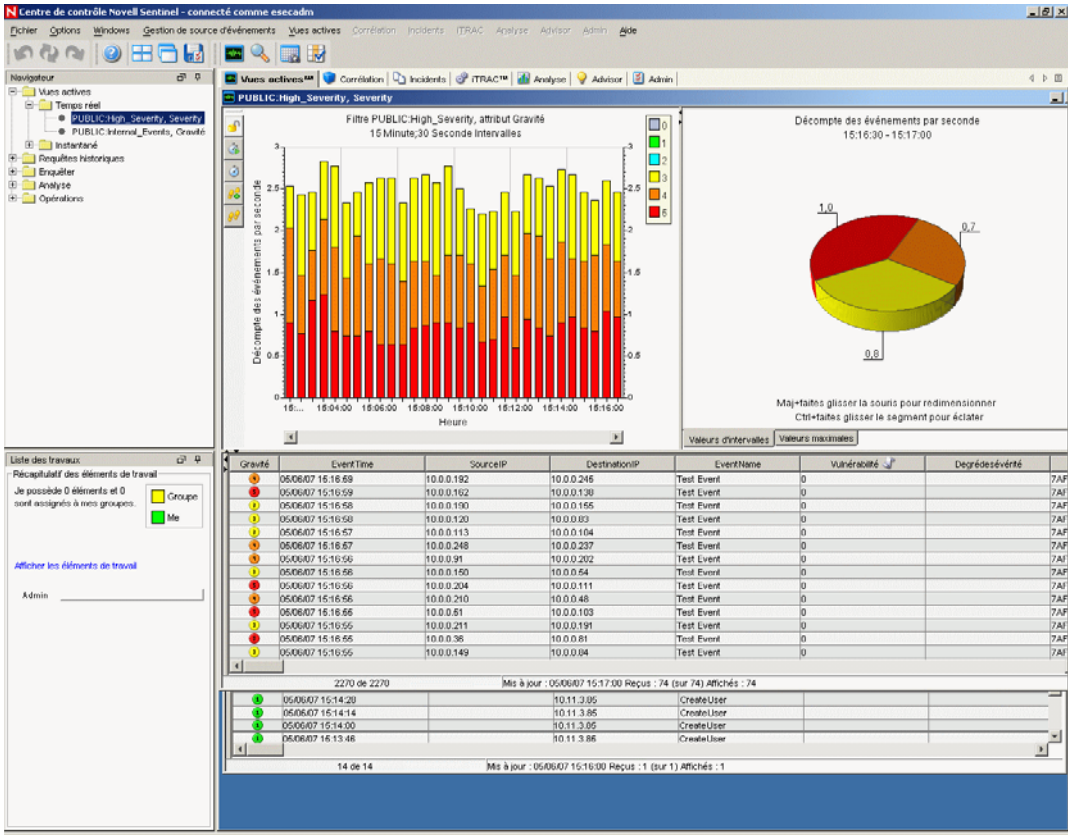


3 Accédez au menu Gestion de source d'événements et choisissez Vue en direct.

4 Dans la vue graphique, cliquez avec le bouton droit sur Source d'événements 5 eps et sélectionnez Démarrer.

5 Fermez la fenêtre Gestion de source d'événements (vue en direct).

6 Accédez à l'onglet Active Views. Il affiche une fenêtre intitulée « PUBLIC: High_Severity, Severity » (Public : Gravité_élevée, Gravité). Il se peut que vous deviez attendre un certain temps avant que le collecteur démarre et que les données apparaissent dans la fenêtre.



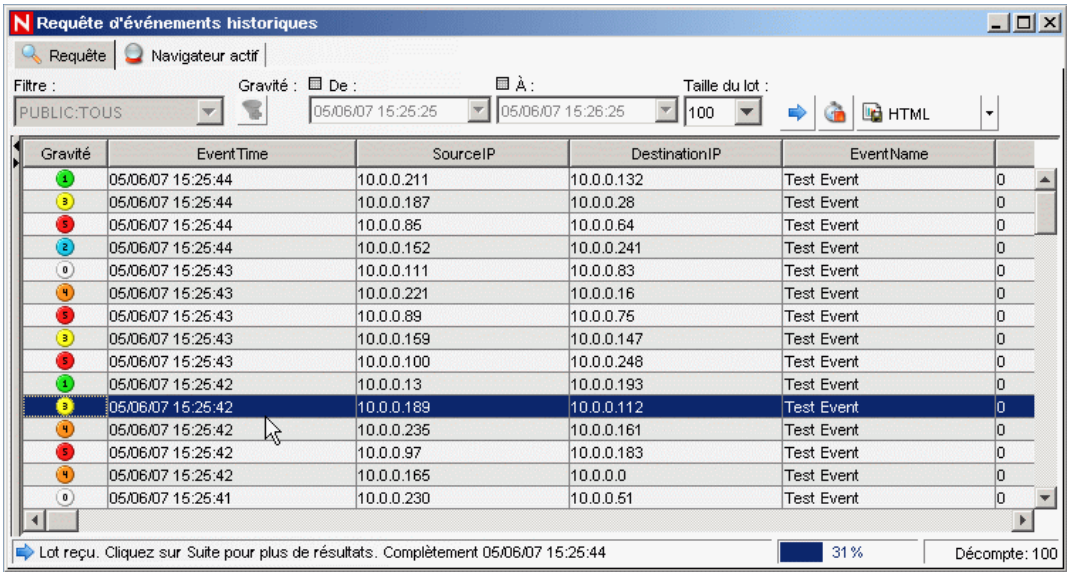
7 Cliquez sur le bouton Requête d'événement dans la barre d'outils. La fenêtre Requête d'événements historiques s'affiche.

8 Dans cette fenêtre, cliquez sur la flèche bas Filtre pour sélectionner un filtre. Mettez en surbrillance le filtre Public: All (Public : Tout), puis cliquez sur Sélectionner.

9 Choisissez une période qui couvre la période d'activité du collecteur. Sélectionnez la plage de dates à l'aide des listes déroulantes De et À.

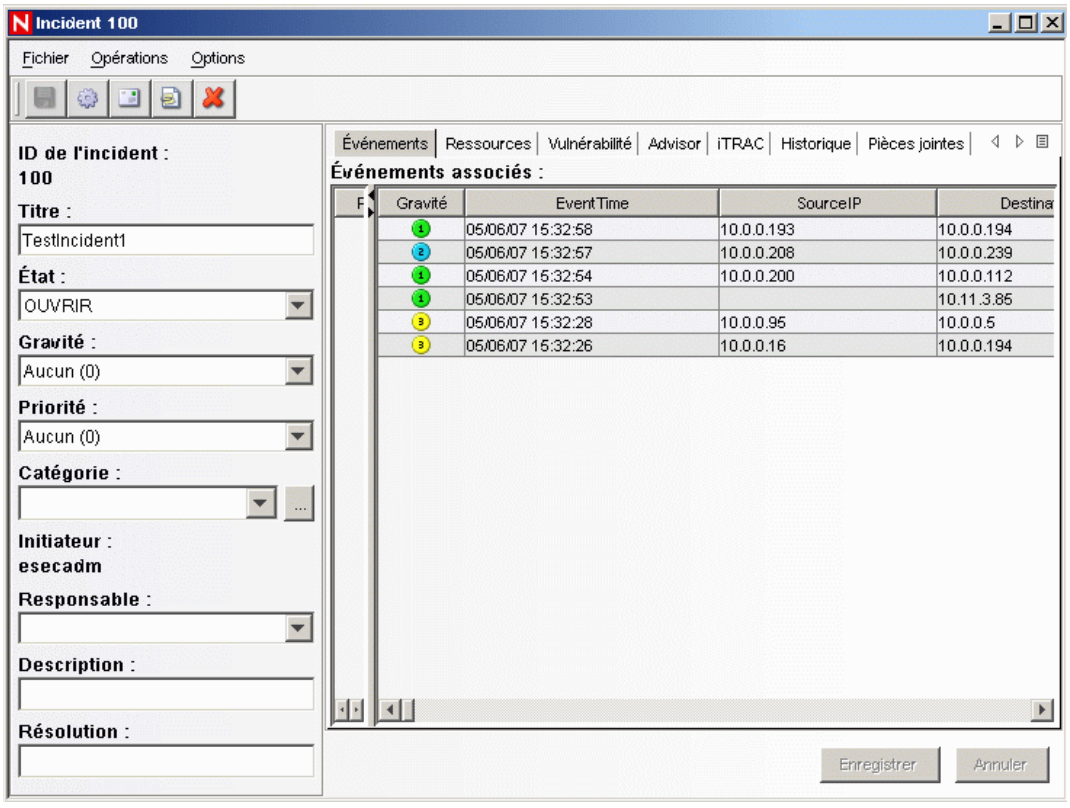
10 Sélectionnez une taille de lot à partir de la liste déroulante correspondante.

11 Cliquez sur l'icône de loupe pour exécuter la requête.



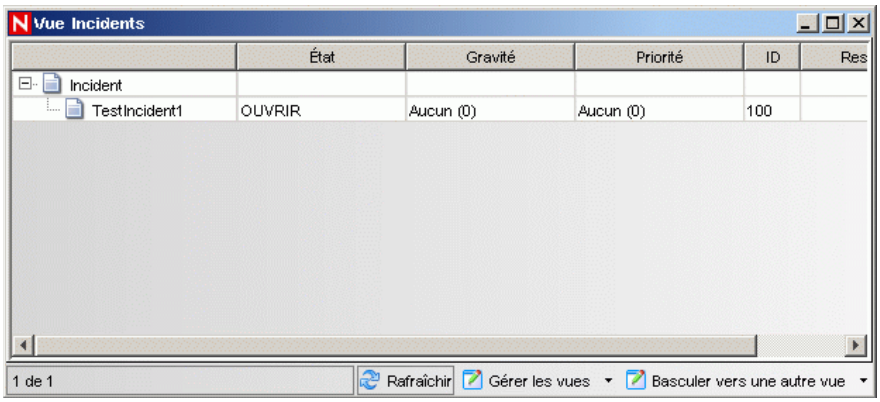
12 Maintenez la touche Ctrl ou Maj enfoncée et sélectionnez plusieurs événements dans la fenêtre Requête d'événements historiques.

13 Cliquez avec le bouton droit, puis sélectionnez Créer un incident.

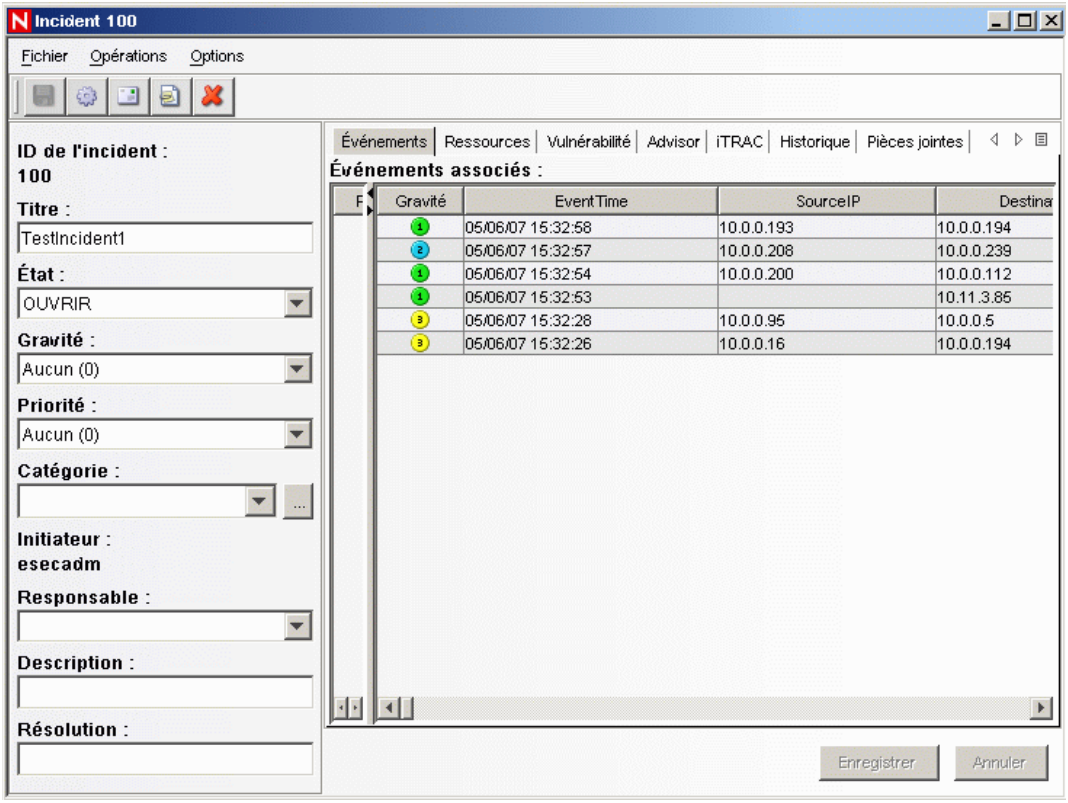


14 Nommez l'incident TestIncident1 et cliquez sur Créer. Une notification de réussite s'affiche. Cliquez sur OK.

15 Accédez à l'onglet Incident. Le gestionnaire de vues d'incidents s'affiche. Il vous permet de voir l'incident que vous venez de créer.



16 Double-cliquez sur l'incident pour l'ouvrir.



17 Fermez la fenêtre de l'incident. Pour ce faire, allez dans Fichier > Quitter ou cliquez sur le « X » dans le coin supérieur droit de la fenêtre.

18 Cliquez sur l'onglet Analyse. Dans la fenêtre de navigation, ouvrez le dossier Historical Reports (Rapports d'historique).

19 Cliquez sur Requête d'événement.

20 Cliquez sur Analyse > Créer un rapport ou sur l'icône Créer un rapport. Une fenêtre Requête d'événement s'ouvre. Définissez ce qui suit :

- le délai
- filtre
- le niveau de gravité
- taille du lot (il s'agit du nombre d'événements à afficher. Les événements sont affichés du plus ancien au plus récent)

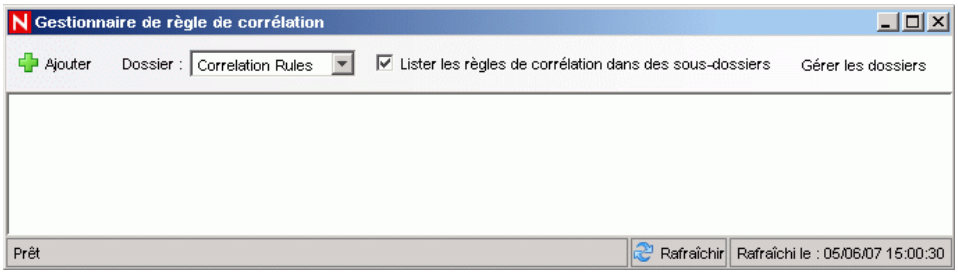
21 Cliquez sur le bouton Rafraîchir la requête.

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

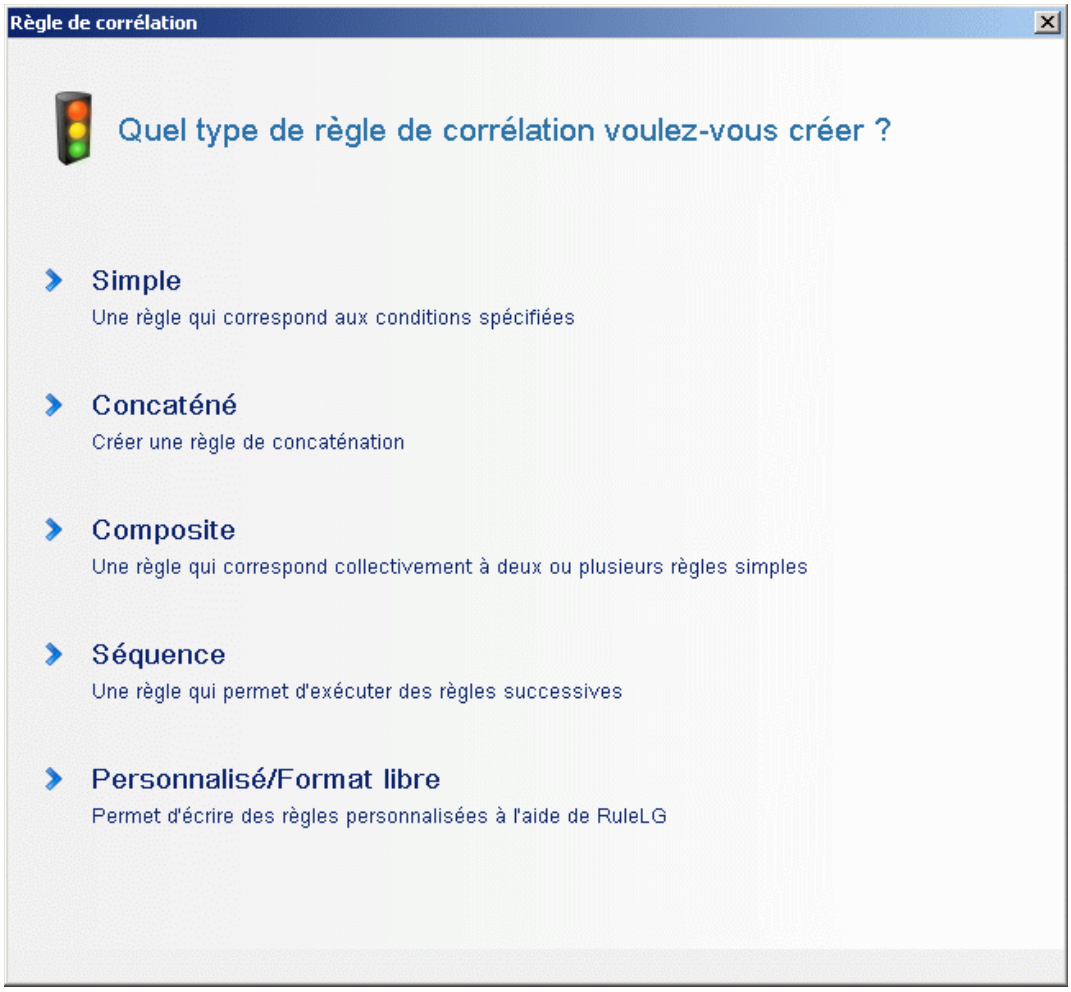
23 Vous pouvez réorganiser les colonnes par glisser-déplacer. Vous pouvez également changer l'ordre de tri d'une colonne en cliquant sur son en-tête.

24 Lorsque votre requête est terminée, elle est ajoutée à la liste de requêtes rapides dans le navigateur.

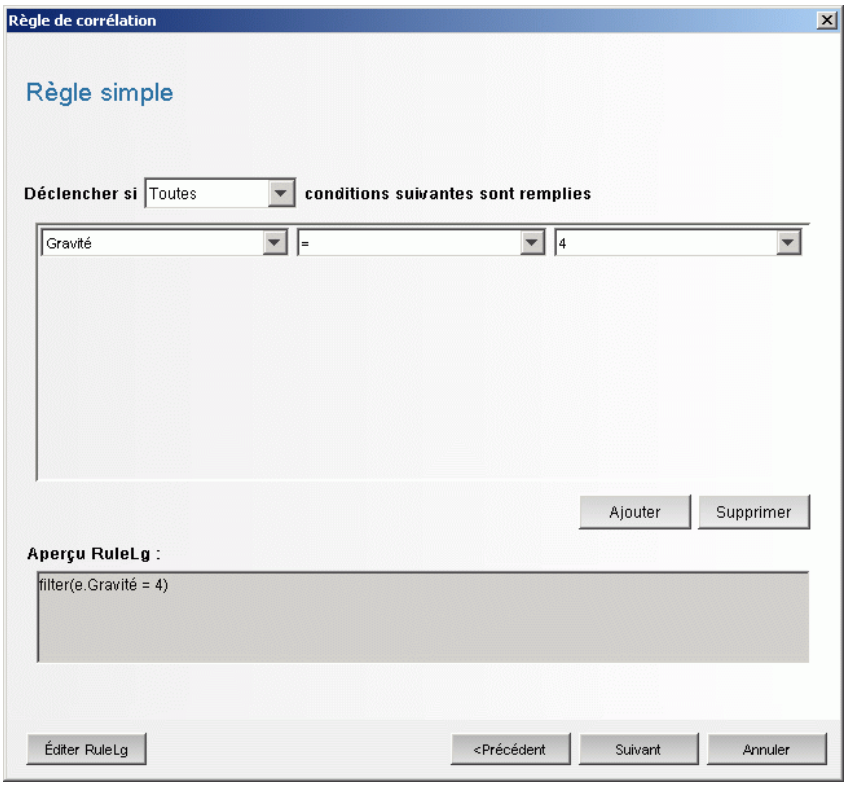
25 Accédez à l'onglet Corrélation. Le gestionnaire de règle de corrélation s'affiche.



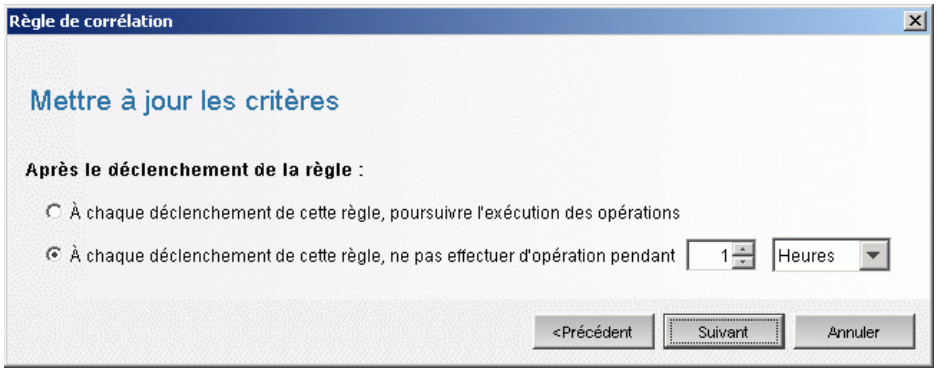
26 Cliquez sur Ajouter. L'Assistant de règle de corrélation s'ouvre.



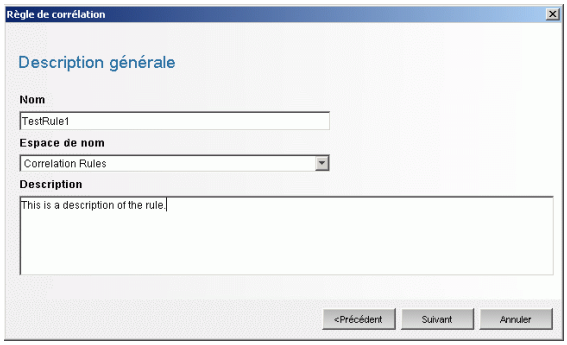
27 Cliquez sur Simple. La fenêtre Règle simple s'affiche.



28 Utilisez les menus déroulants pour définir un critère de gravité de 4. Cliquez sur Suivant. La fenêtre Mettre à jour les critères s'affiche.



29 Sélectionnez l'option « À chaque déclenchement de cette règle, ne pas effectuer d'opération pendant » et utilisez le menu déroulant pour définir la période sur 1 minute. Cliquez sur Suivant. La fenêtre Description générale s'affiche.

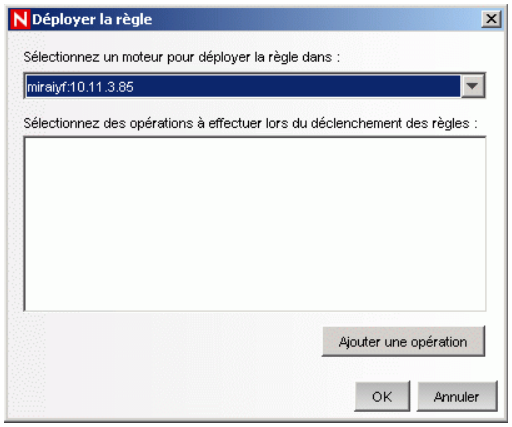


30 Nommez la règle « TestRule1 », entrez une description, puis cliquez sur Suivant.

31 Sélectionnez « Non, ne pas créer d'autre règle », puis cliquez sur Suivant.

32 Ouvrez la fenêtre Gestionnaire de règle de corrélation.

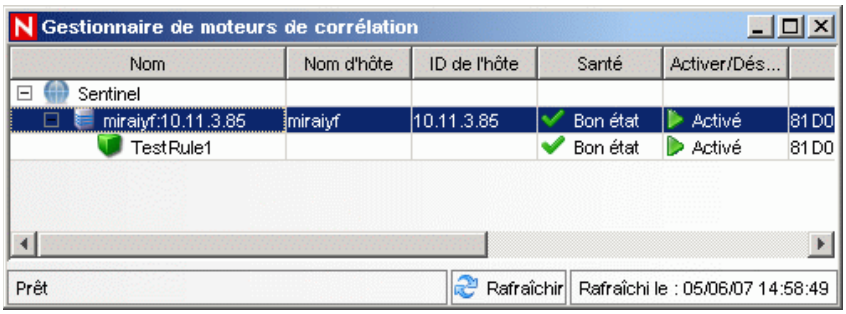
33 Mettez en surbrillance une règle, puis cliquez sur le lien Déployer les règles. La fenêtre Déployer la règle s'affiche.



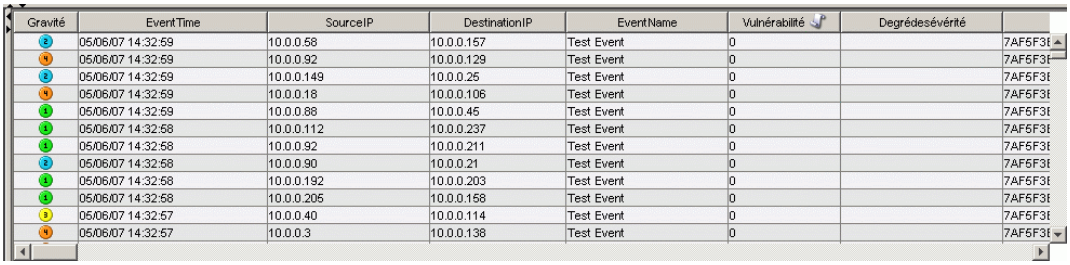
34 Dans cette fenêtre, sélectionnez dans la liste déroulante le moteur à utiliser pour déployer la règle.

35 Sélectionnez une action « Envoyer un message électronique » à associer à la règle, puis cliquez sur OK.

36 Sélectionnez le gestionnaire de moteurs de corrélation. Sous le moteur de corrélation, vous pouvez voir que la règle est déployée/activée.



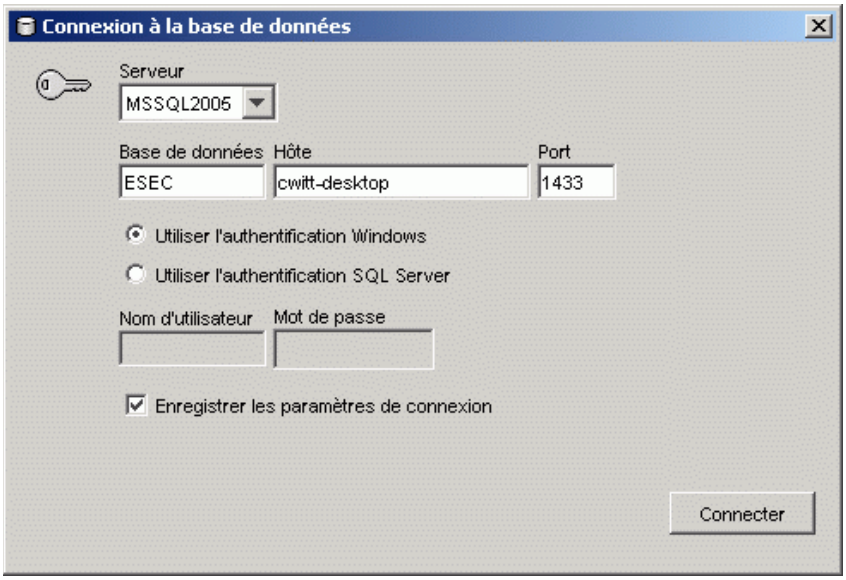
37 Accédez à l'onglet Active Views et vérifiez que l'événement corrélé a bien été généré.



38 Fermez Sentinel Control Center.

39 Double-cliquez sur l'icône Sentinel Data Manager (SDM) sur le Bureau.

40 Loguez-vous à SDM comme l'administrateur de la base de données Sentinel spécifié lors de l'installation (esecdba par défaut).



41 Cliquez sur chaque onglet pour vous assurer que vous pouvez y accéder.

42 Fermez Sentinel Data Manager.

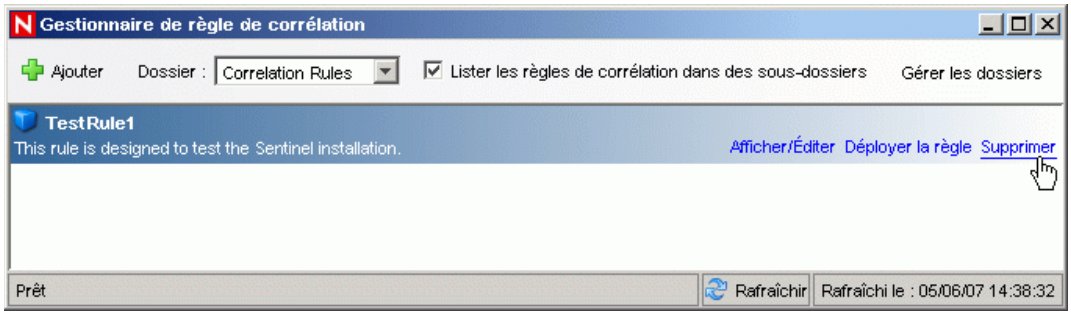
Si vous avez pu effectuer toutes ces étapes sans erreur, vous avez réussi une vérification de base de l'installation du système Sentinel.

5.2 Nettoyage après test

Une fois la vérification du système terminée, vous devez supprimer les objets créés pour les tests.

Pour effectuer le nettoyage après le test du système :

1. Loguez-vous au système comme l'administrateur Sentinel spécifié lors de l'installation (par défaut esecadm).
2. Accédez à l'onglet Corrélation.
3. Ouvrez le gestionnaire de moteurs de corrélation.
4. Dans celui-ci, cliquez avec le bouton droit sur TestRule1 et sélectionnez Annuler le déploiement de la règle.
5. Ouvrez le gestionnaire de règle de corrélation.
6. Sélectionnez TestRule1, puis cliquez sur Supprimer.



7. Accédez au menu Gestion de source d'événements et choisissez Vue en direct.
8. Dans la hiérarchie de source d'événements graphique, cliquez avec le bouton droit sur Collecteur général, puis sélectionnez Arrêter.
9. Fermez la fenêtre Gestion de source d'événements.
10. Accédez à l'onglet Incidents.
11. Ouvrez le gestionnaire de vues d'incidents.
12. Sélectionnez TestIncident1, cliquez avec le bouton droit et choisissez Supprimer.

5.3 Mise en route

Vous pouvez maintenant commencer à utiliser votre système. Pour plus d'informations, reportez-vous à la section “Quick Start” (Démarrage rapide) du manuel SCC User Guide (Guide de l'utilisateur de SCC).

Mise à niveau vers Sentinel 6

6

Rubriques traitées dans ce chapitre :

Ce chapitre explique dans les grandes lignes la mise à niveau d'anciennes versions vers Sentinel 6.0. Les principales étapes consistent à sauvegarder les anciennes versions, installer/désinstaller les logiciels, changer la configuration et migrer les données.

Remarque : le présent document ne décrit pas en détail les procédures de mise à niveau. Des informations détaillées sont fournies dans la documentation relative à l'installation du correctif disponible sur le site Web de documentation de Novell (http://www.novell.com/documentation/).

Les programmes d'installation de correctifs disponibles pour la mise à niveau vers Sentinel 6.0 sont les suivants :

- Sentinel 4.x vers Sentinel 6.0 ;
- Sentinel 5.x vers Sentinel 6.0.

Par rapport à ses anciennes versions, Sentinel 6.0 a enregistré plusieurs changements importants qui peuvent affecter votre mise à niveau. Ceux-ci sont exposés plus en détail dans la documentation relative à l'installation des correctifs.

- Il s'agit de changements mineurs apportés au schéma de base de données entre Sentinel 5.x et 6.0 et majeurs entre Sentinel 4.x et 6.0. En raison de ces changements, Sentinel 6.0 est fourni avec une nouvelle bibliothèque de rapports et les rapports personnalisés peuvent nécessiter des adaptations.
- La nouvelle structure de gestion de source d'événements peut nécessiter quelques changements mineurs au niveau des collecteurs afin d'utiliser de nouveaux connecteurs.
- De nouvelles autorisations utilisateur sont disponibles pour les utilisateurs de Sentinel Control Center.
- La configuration système requise a également changé, y compris la prise en charge de plusieurs nouvelles plates-formes.
- La structure de répertoire ayant changé, les scripts qui réfèrent à des chemins de répertoire peuvent nécessiter une mise à jour.

6.1 Mise à niveau de Sentinel 5.x vers Sentinel 6.0

Points à retenir :

- Le passage de la version 5.x à la version 6.0 de Sentinel est une mise à niveau directe (in-place) qui utilise le programme d'installation des correctifs Sentinel.

- La migration de données de Microsoft SQL Server 2000 pour Sentinel 5.x vers Microsoft SQL Server 2005 pour Sentinel 6.0 est prise en charge. (SQL Server 2000 n'est plus compatible avec Sentinel 6.)
- La migration de données d'Oracle 9i pour Sentinel 5.x vers Oracle 10g pour Sentinel 6.0 est prise en charge.
- La migration de données d'une base de données non Unicode vers une autre Unicode n'est pas prise en charge.
- Lors d'une migration de données réussie, les règles de corrélation et les modèles de processus de travail iTRAC ne sont pas migrés. Les règles de corrélation peuvent être exportées de la version 5.x, puis importées dans la version 6.0. Les modèles de processus de travail iTRAC doivent en revanche être recréés dans Sentinel 6.0.

Pour effectuer une mise à niveau de Sentinel 5.x vers Sentinel 6.0 :

- Vérifiez la configuration système requise
  - Vérifiez que la configuration matérielle du système satisfait aux exigences matérielles mentionnées au Chapitre 2, « Meilleures pratiques », page 19.
  - Vérifiez que les versions du système d'exploitation et de la base de données satisfont à la configuration système requise mentionnée au Chapitre 2, « Meilleures pratiques », page 19.
- Sauvegardez les composants nécessaires
  - Serveur Sentinel
  - Gestionnaire des collecteurs Sentinel
  - Serveur de création de rapport Crystal
  - Serveur de base de données
  - Scripts de collecteur
  - Exporter les règles de corrélation
  - Sauvegarder les processus de travail iTRAC
- Exécutez le programme d'installation des correctifs fourni par Novell
- Installez la base de données Sentinel 6.0
- Effectuez la migration des données
- Installez Sentinel 6.0 (sans la base de données)
- Configurez les objets
  - Mettez à jour les autorisations utilisateur
  - Mettez à jour les configurations de menu
  - Reconfigurez les paramètres de messagerie électronique
  - Redéployez les collecteurs (des modifications peuvent être requises pour des collecteurs sélectionnés)
  - Redéployez les rapports

6.2 Mise à niveau de Sentinel 4.x vers Sentinel 6.0

Points à retenir :

- La migration de données de Microsoft SQL Server 2000 pour Sentinel 4.x vers Microsoft SQL Server 2005 pour Sentinel 6.0 est prise en charge. (SQL Server 2000 n'est plus compatible avec Sentinel 6.)
- La migration de données d'Oracle 9i pour Sentinel 4.x vers Oracle 10g pour Sentinel 6.0 est prise en charge.
- Lors d'une migration de données réussie, les objets suivants sont migrés de Sentinel 4.x vers Sentinel 6.0 :
  - les utilisateurs et les autorisations assignées
  - Filtres
  - les options de configuration de menu contextuel
  - les balises CV renommées
  - les configurations de partition
  - les cas de 4.x qui sont migrés vers 6.0 en tant qu'incidents
  - les incidents et les évènements liés aux incidents
- Même si la migration de données réussit, les règles de corrélation et certains événements ne sont pas migrés. Les règles de corrélation peuvent être exportées de la version 5.x, puis importées dans la version 6.0. Les événements associés à un incident sont migrés, mais les autres ne le sont pas.

Pour effectuer une mise à niveau de Sentinel 4.x vers Sentinel 6.0 :

- Configuration système requise
  - Vérifiez que la configuration matérielle du système satisfait aux exigences matérielles mentionnées au Chapitre 2, « Meilleures pratiques », page 19. Il se peut que vous deviez mettre à jour votre infrastructure matérielle étant donné que la configuration requise pour Sentinel 4.x diffère de celle de Sentinel 6.0.
  - Vérifiez que les versions du système d'exploitation et de la base de données satisfont à la configuration système requise mentionnée au Chapitre 2, « Meilleures pratiques », page 19.
  - Sauvegardez les composants nécessaires
  - Serveur Sentinel
  - Gestionnaire des collecteurs Sentinel
  - Serveur de création de rapport Crystal
  - Serveur de base de données
  - Scripts de collecteur
  - Exporter les règles de corrélation
  - Sauvegarder les processus de travail iTRAC
- Exécutez le programme d'installation des correctifs fourni par Novell

- Installez la base de données Sentinel 6.0
  - Il se peut que vous deviez installer une nouvelle base de données ou une nouvelle instance de base de données. Le schéma de base de données de Sentinel 4.x diffère de celui de Sentinel 6.0. Certaines tables ont été ajoutée et d'autre supprimées de Sentinel 6.0. L'installation d'une nouvelle base de données ou d'une nouvelle instance de base de données créerait/supprimerait ces tables de Sentinel 6.0.
- Effectuez la migration des données
- Installez Sentinel 6.0 (sans la base de données)
- Configurez les objets
  - Mettez à jour les autorisations utilisateur
  - Mettez à jour les configurations de menu
  - Reconfigurez les paramètres de messagerie électronique
  - Redéployez les collecteurs (des modifications peuvent être requises pour des collecteurs sélectionnés)
  - Modifiez et redéployez les rapports

Installation des composants Sentinel

7

Rubriques traitées dans ce chapitre :

Il existe plusieurs scénarios dans lesquels vous pouvez être amené à devoir ajouter des composants à une installation existante :

- Une machine comporte déjà certains composants Sentinel mais d'autres sont requis (par exemple, une machine contient Collector Manager mais il conviendrait d'y ajouter Sentinel Control Center).
- Dans un environnement à haut débit d'événements, il peut être intéressant d'ajouter un nouveau gestionnaire des collecteurs ou un moteur de corrélation pour des raisons de performances.

Grâce au programme d'installation Sentinel, ces scénarios sont très simples à envisager.

7.1 Installation d'un nouveau composant sur une machine Sentinel

Occasionnellement, il peut être nécessaire d'ajouter une machine supplémentaire à l'environnement Sentinel. Si l'utilisation de la mémoire est élevée sur le moteur de corrélation, vous pouvez décider d'en ajouter un autre. Vous pouvez ajouter un gestionnaire des collecteurs sur un site distant pour collecter les données au niveau local, ou un employé peut avoir besoin de Sentinel Control Center sur son Bureau.

Avant d'installer des composants Sentinel sur une nouvelle machine, plusieurs conditions préalables doivent être remplies :

- adresse IP ou nom d'hôte de la machine hébergeant Communication Server ;
- accès à une copie du fichier .keystore à partir de n'importe quelle machine de l'installation Sentinel existante ;
- fichier .keystore disponible dans le répertoire %ESEC_HOME%\config (sous Windows) ou $ESEC_HOME/config (sous Linux et Solaris) ;
- accès requis au fichier .keystore à partir de la machine sur laquelle vous effectuez l'installation ;
- numéros de port utilisés dans l'installation Sentinel initiale.

Remarque : le fichier .keystore et les numéros de port doivent être identiques sur chaque machine du système Sentinel pour garantir le bon fonctionnement des communications. Il existe toutefois

deux exceptions : le fichier .keystore n'est pas requis si vous installez Sentinel Control Center ni si vous installez Collector Manager à l'aide d'un type de communication proxy SSL.

Pour ajouter des composants :

1. Loguez-vous en tant qu'utilisateur disposant de droits d'administrateur (sous Windows) ou en tant qu'utilisateur root (sous Solaris).
2. Insérez le CD d'installation Sentinel dans l'unité de CD-ROM.
3. Accédez au CD et double-cliquez sur :
   - Sous Solaris

     En mode GUI :

     `./setup.sh`

     ou

     En mode texte (« headless ») :

     `./setup.sh –console`
   - Sous Windows, setup.bat.

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

     ---
4. Après avoir lu l'écran d'accueil, cliquez sur Suivant.
5. Lisez et acceptez l'accord de licence utilisateur final, puis cliquez sur Suivant.
6. Si vous installez un composant supplémentaire, un écran s'affiche indiquant l'emplacement de la précédente installation ainsi que les composants déjà installés. Si vous installez une nouvelle copie de Sentinel, un écran s'affiche indiquant le répertoire d'installation par défaut. Cliquez sur Parcourir pour changer de répertoire d'installation. Cliquez sur Suivant.
7. Sélectionnez les composants à ajouter.

   Scénario 1 : installation d'applications uniquement :

   7a Sélectionnez le type d'installation « Personnalisée », puis cliquez sur Suivant.

   7b Sélectionnez les applications (Sentinel Collector Builder, Sentinel Control Center et Sentinel Data Manager), puis cliquez sur Suivant.

   7c Une invite relative à la taille du segment de mémoire JVM (Java Virtual Machine) s'affiche. Cliquez sur Suivant.

   Taille du segment de mémoire JVM (Mo) : par défaut, cette valeur est définie comme la moitié de la taille de la mémoire physique détectée sur la machine, avec un maximum de 1 024 Mo. Elle correspond au maximum de taille heap JVM seulement utilisée par Sentinel Control Center.

   7d Vous êtes invité à entrer les informations relatives au nom du serveur hôte/port. Entrez les informations requises, puis cliquez sur Suivant.

Scénario 2 : installation de Correlation Engine (composants supplémentaires) après l'installation de l'application :

7e Sélectionnez Correlation Engine, puis cliquez sur Suivant.

7f Sélectionnez la méthode d'obtention de la clé de bus de message. Spécifiez si vous souhaitez générer un fichier keystore aléatoire ou importer un fichier existant à partir

d'une autre machine du système Sentinel. Si vous optez pour la deuxième méthode, vous devez accéder à l'emplacement et sélectionnez le fichier keystore. Cliquez sur Suivant.

Scénario 3 : installation simultanée de Correlation Engine et des applications :

7g Sélectionnez le type d'installation « Personnalisée », puis cliquez sur Suivant.

7h Sélectionnez les applications (Sentinel Collector Builder, Sentinel Control Center et Sentinel Data Manager) et Correlation Engine, puis cliquez sur Suivant.

7i Une invite relative à la taille du segment de mémoire JVM (Java Virtual Machine) s'affiche. Cliquez sur Suivant.

7j Vous êtes invité à entrer les informations relatives au port proxy de Sentinel Control Center et au nom d'hôte de Communication Server. Entrez les informations requises, puis cliquez sur Suivant.

7k Sélectionnez la méthode d'obtention de la clé de codage de bus de message. Spécifiez si vous souhaitez générer un fichier keystore aléatoire ou importer un fichier existant à partir d'une autre machine du système Sentinel. Si vous optez pour la deuxième méthode, vous devez accéder à l'emplacement et sélectionnez le fichier keystore. Cliquez sur Suivant.

Scénario 4 - Installation simultanée du service Sentinel Collector et des applications :

7l Sélectionnez le type d'installation « Personnalisée », puis cliquez sur Suivant.

7m Sélectionnez les applications (Sentinel Collector Builder, Sentinel Control Center et Sentinel Data Manager) et le service Sentinel Collector, puis cliquez sur Suivant.

7n Une invite relative à la taille du segment de mémoire JVM (Java Virtual Machine) s'affiche. Cliquez sur Suivant.

7o Vous avez le choix entre deux méthodes de communication entre les clients Sentinel et le serveur. La communication peut en effet s'effectuer en se connectant au bus de message directement ou à l'aide d'un proxy. Cliquez sur Suivant.

7p Vous êtes invité à entrer les informations relatives au port du bus de message, au port proxy de Sentinel Control Center et au nom d'hôte de Communication Server. Entrez les informations requises, puis cliquez sur Suivant.

Remarque : Si vous sélectionnez « Se connecter au bus de message à l'aide de proxy », une option supplémentaire « Port d'authentification du certificat de gestionnaire des collecteurs » s'offre à vous.

7q Sélectionnez la méthode d'obtention de la clé de bus de message. Spécifiez si vous souhaitez générer un fichier keystore aléatoire ou importer un fichier existant à partir d'une autre machine du système Sentinel. Si vous optez pour la deuxième méthode, vous devez accéder à l'emplacement et sélectionnez le fichier keystore. Cliquez sur Suivant.

8 L'écran Récapitulatif s'affiche. Passez en revue le récapitulatif de l'installation, puis cliquez sur Installer.

9 Une fois l'installation terminée, une invite vous demande de redémarrer. Choisissez de redémarrer votre ordinateur et cliquez sur Terminer.

7.1.1 Installation de la base de données Sentinel

Pour installer la base de données Sentinel 6 :

1. Si Sentinel était déjà installé, avant de procéder à la nouvelle installation, supprimez les variables d'environnement suivantes sous Windows.
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
2. Loguez-vous en tant qu'utilisateur disposant de droits d'administrateur (sous Windows) ou en tant qu'utilisateur root (sous Solaris ou Linux).
3. Insérez le CD d'installation Sentinel dans l'unité de CD-ROM.
4. Accédez au CD et double-cliquez sur :
   - Sous Linux/Solaris,

     En mode GUI :

     `./setup.sh`

     ou

     En mode texte (« headless ») :

     `./setup.sh -console`
   - Sous Windows, setup.bat.

   Remarque : l'installation en mode de console n'est pas prise en charge sous Windows.
5. Après avoir lu l'écran d'accueil, cliquez sur Suivant.
6. Lisez et acceptez l'accord de licence utilisateur final, puis cliquez sur Suivant.
7. Acceptez le répertoire d'installation par défaut ou cliquez sur Parcourir afin de spécifier un autre emplacement. Cliquez sur Suivant.

8. Pour le type d'installation, sélectionnez Personnalisée (par défaut). Cliquez sur Suivant.
9. Dans la fenêtre de sélection des fonctionnalités, désélectionnez toutes les options, puis cochez la case Base de données. Cliquez sur Suivant.

   Remarque : veillez à désélectionner la fonctionnalité 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.
10. Configurez la base de données pour l'installation :
    - Sous Windows :

    10a Sélectionnez la plate-forme du serveur de base de données cible.
    - Sélectionnez Microsoft SQL Server 2005.

- Spécifiez le répertoire du journal de l'installation de la base de données.

Cliquez sur Suivant.

10b Spécifiez l'emplacement de stockage pour les éléments suivants :

- Répertoire de données
- Répertoire d'index
- Répertoire des données du récapitulatif
- Répertoire des index récapitulatifs
- Répertoire du journal

Cliquez sur Suivant.

10c Sélectionnez l'option de prise en charge de jeux de caractères par la base de données, à savoir Unicode ou ASCII seulement. Cliquez sur Suivant.

10d Spécifiez la taille de la base de données. Cliquez sur Suivant.

10e Configurez les partitions de la base de données.

- Vous pouvez choisir d'activer la gestion de partition automatique de base de données.
- Pour les partitions de données, spécifiez le répertoire d'archivage ; entrez les données temporelles pour l'ajout et l'archivage des données.

Cliquez sur Suivant.

Sous Linux/Solaris :

10f Sélectionnez la plate-forme du serveur de base de données cible.

- Sélectionnez Oracle 10g dans la liste déroulante.
- Sélectionnez Créer une nouvelle base de données avec les objets de la base de données.

Cliquez sur Suivant.

10g Spécifiez le nom de l'utilisateur Oracle ou acceptez le nom d'utilisateur par défaut. Cliquez sur OK

10h Sélectionnez le pilote JDBC Oracle et spécifiez le nom de la base de données. Cliquez sur Suivant.

10i Acceptez le port d'écoute et l'espace mémoire par défaut ou spécifiez de nouvelles valeurs.

10j Entrez l'utilisateur SYS et ses références, puis cliquez sur Suivant.

10k Spécifiez la taille de la base de données. Cliquez sur Suivant.

10l Spécifiez l'emplacement de stockage pour les éléments suivants :

- Répertoire de données
- Répertoire d'index
- Répertoire des données du récapitulatif
- Répertoire des index récapitulatifs
- Répertoire du journal

Cliquez sur Suivant.

10m Configurez les partitions de la base de données.

- Choisissez d'activer la gestion de partition automatique de base de données.

- Spécifiez le répertoire d'archivage des partitions de données.
- Spécifiez des données temporelles pour l'ajout et l'archivage des données.

Cliquez sur Suivant.

11 Entrez les informations d'authentification pour :

- l'administrateur de la base de données Sentinel ;
- l'utilisateur de base de données de l'application Sentinel ;
- l'administrateur de Sentinel ;
- l'utilisateur de rapports Sentinel.

Cliquez sur Suivant.

12 Un récapitulatif des paramètres spécifiés pour la base de données s'affiche. Cliquez sur Suivant.

13 Un récapitulatif de l'installation s'affiche. Cliquez sur Installer.

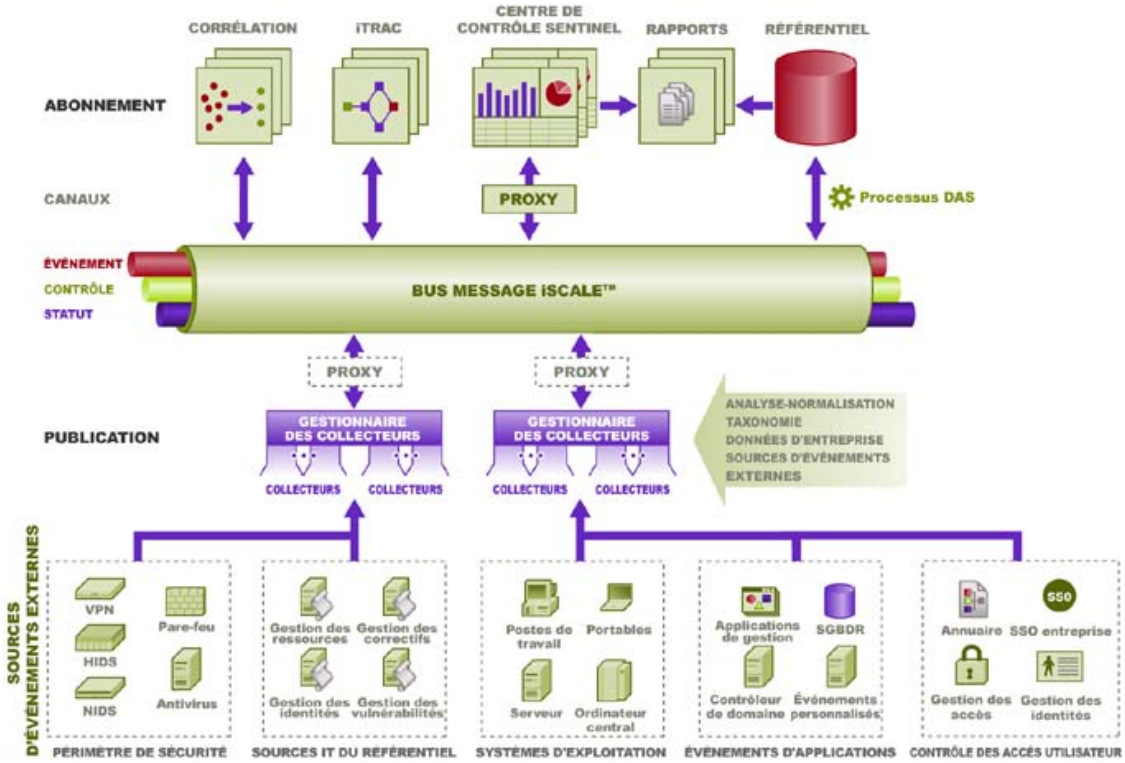
14 Si l'installation réussit, choisissez de redémarrer votre système et cliquez sur Terminer.

Couche de communication (iSCALE)

8

Rubriques traitées dans ce chapitre :

La couche de communication (iSCALE) reliant tous les composants de l'architecture consiste en une connexion TCP/IP codée élaborée sur une épine dorsale JMS (Java Messaging Service). Sentinel 6 comporte un proxy SSL facultatif pour sécuriser les composants Collector Manager et Sentinel Control Center s'ils sont installés en dehors du pare-feu.



Lors de l'installation de Collector Manager, deux options de communication s'offrent à vous :

- **Se connecter au bus de message directement (par défaut) :** cette option est la plus simple et la plus rapide. Toutefois, Collector Manager doit alors connaître la clé de codage du bus de message partagé, ce qui peut comporter un risque si Collector Manager s'exécute sur une machine exposée à des menaces au niveau de la sécurité (par exemple, une machine dans la DMZ). Cette option code les communications à l'aide du codage AES 128 bits sur la base de la valeur consignée dans un fichier appelé .keystore.
- **Se connecter au bus de message à l'aide de proxy :** Cette option permet de renforcer la sécurité en configurant Collector Manager de manière à ce qu'il se connecte via un serveur proxy SSL. Dans ce cas, l'authentification et le codage basés sur un certificat seront utilisés

pour ne pas devoir stocker le fichier .keystore sur la machine Collector Manager. Cette option est intéressante lorsque Collector Manager est installé dans un environnement moins sécurisé.

Vous pouvez choisir l'une de ces deux options lors de l'installation de Collector Manager. Sentinel Control Center utilise le proxy par défaut.

8.1 Communication directe et proxy SSL

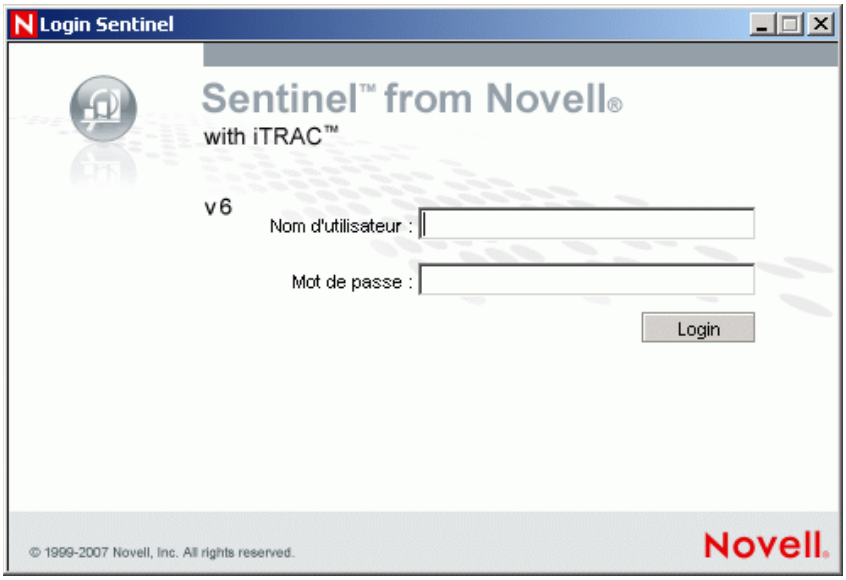
Les composants Sentinel pouvant utiliser le proxy SSL sont Sentinel Control Center et Collector Manager.

8.1.1 Centre de contrôle Sentinel

Sentinel Control Center utilise le proxy SSL par défaut. Sentinel Control Center se connecte à SSL via le port proxied_client. Ce port est configuré pour utiliser uniquement l'authentification de certificat SSL côté serveur. L'authentification côté client utilise le nom et le mot de passe de l'utilisateur de Sentinel Control Center.

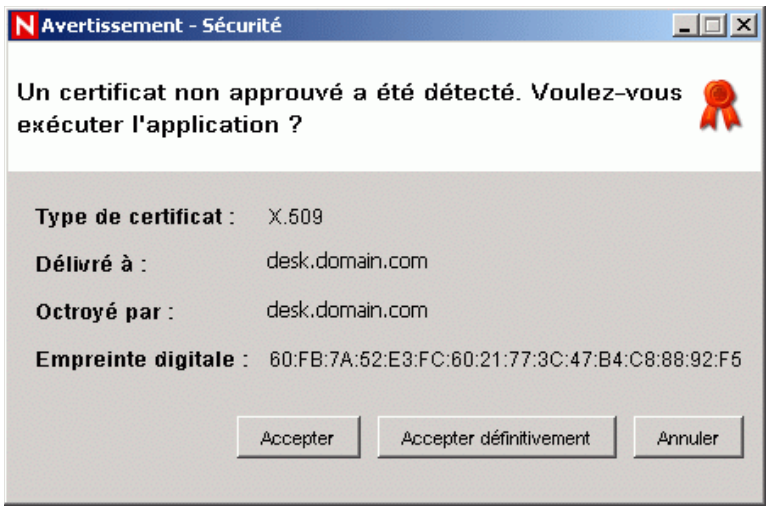
Pour vous loguer à Sentinel Control Center la première fois :

1. Allez dans Démarrer > Tous les programmes > Sentinel et sélectionnez Sentinel Control Center. La fenêtre Login Sentinel s'affiche.



2. Entrez vos références d'utilisateur pour vous loguer à Sentinel Control Center.
   - Nom d'utilisateur et mot de passe en cas d'utilisation de l'authentification SQL Server OU
   - Domaine\nom d'utilisateur et mot de passe en cas d'utilisation de l'authentification Windows
3. Cliquez sur Login.

4 Lors de la première tentative de login, un avertissement tel qu'illustré ci-dessous s'affiche.



5 Si vous cliquez sur Accepter, ce message apparaîtra à chaque fois que vous tenterez d'ouvrir Sentinel sur votre système. Pour éviter cela, vous pouvez cliquer sur Accepter définitivement.

Pour démarrer Sentinel Control Center sous Linux et Solaris :

1 En tant qu'administrateur Sentinel (esecadm), accédez au répertoire :
`$ESEC_HOME/bin`

2 Exécutez la commande suivante :
`control_center.sh`

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

4 Une fenêtre Certificat s'affiche. Cliquez sur Accepter.

Les utilisateurs de Sentinel Control Center doivent répéter la procédure susmentionnée pour accepter un nouveau certificat dans les cas suivants :

- réinstallation de Sentinel Communication Server ;
- déplacement de Sentinel Communication Server vers un nouveau serveur.

8.1.2 Gestionnaire des collecteurs

Collector Manager peut être installé en mode proxy (à l'aide du proxy SSL) ou directement (connexion directe au bus de message).

- Pour les composants Collector Manager davantage exposés à des risques d'attaques (par exemple, une machine en DMZ), le proxy SSL offre la méthode de communication la plus sûre.
- Pour les composants Collector Manager moins exposés ou nécessitant un débit d'événements élevé, ou encore pour ceux installés sur la même machine que DAS (Data Access Service), la communication directe au bus de message est recommandée.

Collector Manager se connecte à SSL via le proxied_trusted_client. Pour permettre à Collector Manager de se relancer sans intervention de l'utilisateur après un redémarrage, ce port est configuré de manière à utiliser l'authentification de certificat SSL à la fois côté serveur et client. Une relation

d'approbation est établie entre le proxy et Collector Manager (échange de certificats), les futures connexions utilisant les certificats pour s'authentifier. Cette relation d'approbation est configurée automatiquement durant l'installation.

La relation d'approbation doit être réinitialisée pour chaque composant Collector Manager qui utilise le proxy SSL dans les cas suivants :

- réinstallation de Sentinel Communication Server ;
- déplacement de Sentinel Communication Server vers un nouveau serveur.

Pour réinitialiser la relation d'approbation pour un gestionnaire des collecteurs :

1. Loguez-vous au serveur Collector Manager en tant qu'administrateur Sentinel (esecadm par défaut).
2. Ouvrez dans un éditeur de texte le fichier configuration.xml situé dans le répertoire $ESEC_HOME/config ou %ESEC_HOME%\config.
3. Modifiez les services « Collector_Manager », « agentmanager_events » et « Sentinel » dans le fichier configuration.xml pour qu'ils utilisent l'ID de stratégie « proxied_trusted_client ». Voici un extrait du fichier à titre d'exemple :

```
<service name="Collector_Manager" plugins=""
strategyid="proxied_trusted_client"/>
<service name="agentmanager_events" plugins=""
strategyid="proxied_trusted_client"/>
<service name="Sentinel" plugins=""
strategyid="proxied_trusted_client"/>
```

4. Enregistrez le fichier et quittez.
5. Dans un éditeur de texte, ouvrez le fichier sentinel.xml situé dans le répertoire $ESEC_HOME/config ou %ESEC_HOME%\config.
6. Supprimez les composants suivants du fichier sentinel.xml :

```
<obj-component id="SentinelRemoteLoggingService">
<!-- Must be after the service manager -->
<class>esecurity.ccs.comp.audit.LogHandlerService</class>
<property name="Level">SEVERE</property>
</obj-component>
```

7. Enregistrez le fichier et quittez.
8. Exécutez le fichier %ESEC_HOME%\bin\register_trusted_client.bat (ou .sh sous UNIX). Vous obtenez un résultat similaire à celui-ci :

```
E:\Program Files\novell\sentinel6>bin\register_trusted_client.bat
Please review the following server certificate:
Type:X.509
Issued To:foo.bar.net
Issued By:foo.bar.net
Would you like to accept this certificate? [Y/N] (defaults to N): Y
Please enter a Sentinel username and password that has permissions
to register a trusted client.
Username: esecadm
Password:*********
*Writing to keystore file: E:\Program
Files\novell\sentinel6\config\.proxyClientKeystore
```

9 Redémarrez le service Sentinel sur le serveur hébergeant Communication Server. Attendez la fin de l'initialisation de DAS Proxy.

10 Redémarrez le service Sentinel sur le serveur hébergeant Collector Manager.

11 Répétez cette procédure pour tous les composants Collector Manager utilisant la communication proxy.

8.2 Modifications de la clé de codage

L'installation Sentinel permet à l'administrateur de générer une nouvelle clé de codage aléatoire (stockée dans le fichier .keystore) ou d'importer un fichier .keystore existant. Quelle que soit la méthode utilisée, le fichier .keystore doit être le même sur chaque machine dans l'environnement Sentinel pour garantir le bon fonctionnement des communications.

Remarque : Le fichier .keystore n'est pas requis sur la machine hébergeant la base de données pour autant que cette dernière soit le seul composant Sentinel installé sur cette machine.

La clé de codage peut être modifiée à l'aide d'un utilitaire nommé keymgr. Dans le répertoire lib d'une installation Sentinel ($ESEC_HOME/lib ou %ESEC_HOME%\lib), le programme génère un fichier nommé .keystore. Ce fichier doit être copié dans le même répertoire sur chaque machine sur laquelle un composant Sentinel est installé.

Pour changer la clé de codage pour la communication directe :

1 Pour UNIX, loguez-vous en tant qu'administrateur Sentinel (par défaut, esecadm). Pour Windows, loguez-vous en tant qu'utilisateur disposant de droits d'administrateur.

2 Instructions d'installation:

Pour Windows:

```
%ESEC_HOME%\bin
```

Pour UNIX :

```
$ESEC_HOME/bin
```

3 Exécutez la commande suivante :

Sous Windows :

```
"%ESEC_JAVA_HOME%\java" -jar keymgr.jar –-keyalgo AES --keysize 256 –-keystore <filename, usually .keystore>
```

Sous UNIX :

```
$ESEC_JAVA_HOME/java -jar keymgr.jar --keyalgo AES --keysize 256 --keystore <filename, usually .keystore>
```

4 Copiez le fichier .keystore sur chaque machine comportant un composant Sentinel (sauf en cas d'utilisation de la communication proxy). Le fichier doit être copié dans le répertoire suivant :

Pour Windows:

```
%ESEC_HOME%\config
```

Pour UNIX :

```
$ESEC_HOME/config
```

8.2.1 Modifications du mot de passe Advisor

Si vous utilisez Advisor en mode de téléchargement direct, vous devez mettre à jour les mots de passe stockés dans les fichiers de configuration d'Advisor. Ces mots de passe sont codés en utilisant les informations du fichier .keystore et doivent être recréés à l'aide de la nouvelle valeur .keystore.

Pour coder le mot de passe Advisor après une modification de clé de codage :

1. Pour UNIX, loguez-vous en tant qu'administrateur Sentinel (par défaut, esecadm) sur la machine sur laquelle Advisor est installé. Pour Windows, loguez-vous en tant qu'utilisateur disposant de droits d'administrateur.
2. Changez les répertoires en :

   Pour UNIX :

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

   Pour Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```
3. Entrez les commandes suivantes :

   Pour UNIX :

   ```
   ./adv_change_passwd.sh <newpassword>
   ```

   Pour Windows:

   ```
   adv_change_passwd.bat <newpassword>
   ```

Crystal Reports pour Windows

9

Rubriques traitées dans ce chapitre :

Crystal Businessobjects Enterprise™ XI est un outil de création de rapport.

Ce chapitre traite de l'installation et de la configuration de Crystal Reports Server pour Sentinel.

Sentinel prend en charge l'exécution de Crystal Reports Server sur les plates-formes suivantes :

- Windows – Prise en charge si la base de données Sentinel fonctionne sous Windows ou Linux ;
- Linux – Prise en charge si la base de données Sentinel fonctionne sous Linux.

Ce chapitre traite de l'exécution de Crystal Reports Server sous Windows. Pour plus d'informations sur l'exécution de Crystal Reports Server sous Linux, reportez-vous au Chapitre 10, « Crystal Reports pour Linux », page 137.

Pour installer Crystal Reports Server :

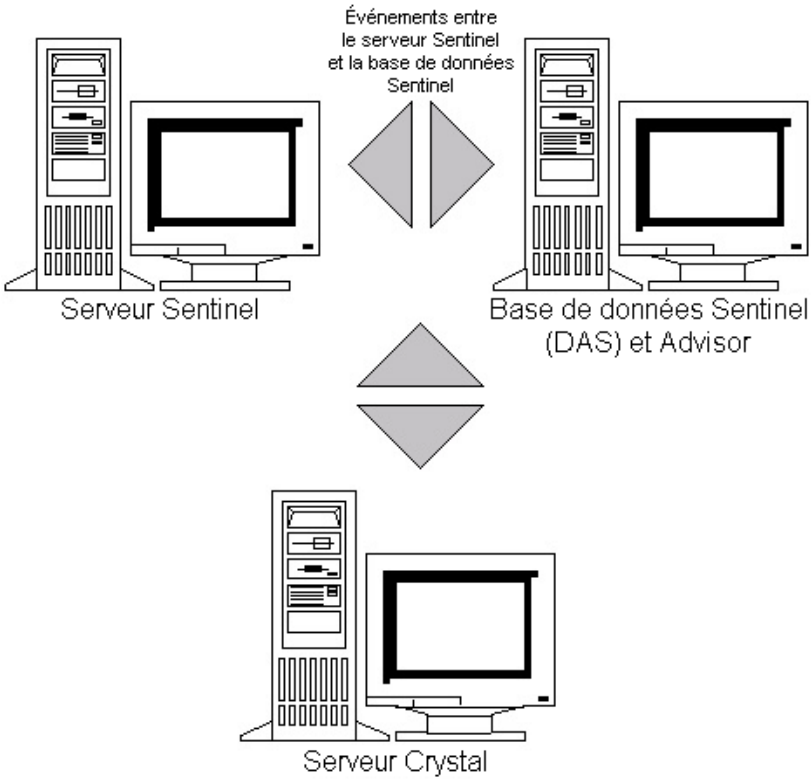
1. installer Microsoft IIS et ASP.NET
2. installer Microsoft SQL (en fonction de la configuration comme authentification Windows ou authentification SQL Server)
3. installer Crystal Server
   - configurer ODBC (Open Database Connectivity) pour l'authentification SQL

     ou
   - Installation et configuration du logiciel Oracle 9i Client
4. configurer inetmgr
5. correctif Crystal Reports
6. publication (importation) de Crystal Reports
7. configuration du compte « Utilisateur nommé »

8. test de la connectivité serveur Web
9. augmentation de la limite de rafraîchissement des enregistrements pour les rapports de Crystal Enterprise Server
10. Configuration de Sentinel Control Center pour l'intégration avec Crystal Enterprise Server.

L’installation devrait être faite dans l'ordre indiqué ci-dessous :

Remarque : vous devez installer Crystal Reports Server dans l'ordre indiqué ci-dessus.



9.1 Présentation

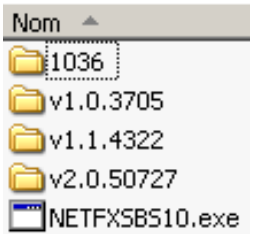
Crystal Reports Server requiert une base de données pour stocker les informations concernant le système et ses utilisateurs. Cette base de données est connue comme base de données CMS (Central Management Server). CMS est un serveur qui stocke les informations concernant le système de Crystal Reports 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 Microsoft SQL Server locale. Le programme d'installation de Crystal Reports Server permet de configurer la base de données CMS sur une base de données MSDE en l'absence de serveur local Microsoft SQL 2005 Server. Sentinel ne prend pas en charge de configuration MSDE.

9.2 Configuration système requise

Windows® 2003 Server avec SP1 avec une partition formatée NTFS avec IIS (Microsoft Internet Information Server) et NET.ASP installés Sentinel ne prend pas en charge Crystal XI sur Windows® 2000 Server.

.NET Framework 1.1 (installé par défaut sur Windows 2003. BusinessObjects Enterprise™ XI 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 :

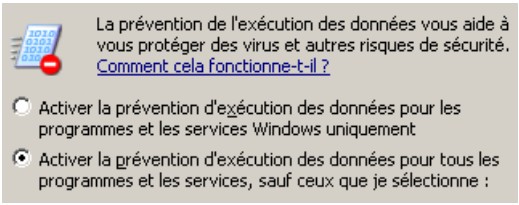


9.3 Configuration requise

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 Windows essentiels. C'est notamment utile pour éviter l'« Erreur 1920. Service Crystal Report Cache Server sous Windows 2003 ».

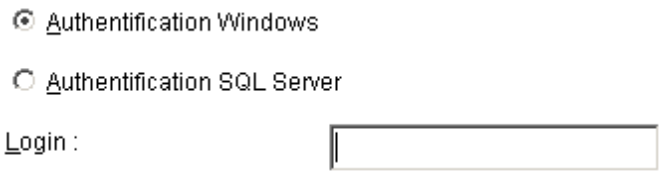
   Pour accéder à DEP, sélectionnez Panneau de configuration > Système > Onglet Avancé > Paramètres de performances > Prévention de l'exécution des données.

   Sélectionnez Activer la prévention d'exécution des données pour les programmes et les services Windows uniquement.



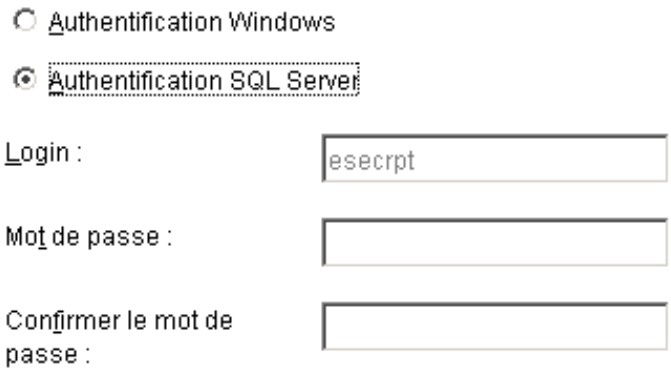
   Si vous voulez exécuter les rapports Sentinel à l'aide de l'authentification Windows NT, vérifiez que le compte de domaine Windows pour les rapports Sentinel existe déjà dans la base de données Sentinel. Cela est fait pendant l'installation Sentinel en sélectionnant

l’authentification Windows, lors de la configuration de la méthode d’authentification pour l’utilisateur des rapports Sentinel, comme illustré ci-dessous.



3 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 Microsoft SQL, cela s'effectue pendant l'installation Sentinel pour Microsoft 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.

4 Pour Oracle - Oracle 9i Client Release 2 (9.2.0.1.0), installez-le avant Crystal Businessobjects Enterprise™ XI.

5 Pour Microsoft SQL Server, installez Microsoft SQL 2005 avant Crystal Reports Server XI.

6 Résolution vidéo de 1 024 x 768 ou supérieure

7 Installez Microsoft Internet Information Server (IIS) et ASP.NET

Remarque : Sentinel ne prend pas en charge MSDE. Installez Microsoft SQL 2005 avant Crystal Reports Server XI.

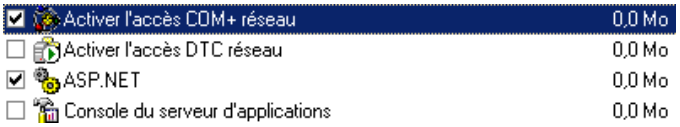
9.3.1 Installation de Microsoft Internet Information Server (IIS) et d'ASP.NET

Pour ajouter les composants Windows, le CD d'installation de Windows 2003 Server peut s'avérer nécessaire.

Pour installer IIS et ASP.NET :

1. Sous Windows, allez dans le Panneau de configuration > Ajouter ou supprimer des 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.
7. Cliquez sur Suivant. Une invite vous demande le CD d'installation Windows.
8. Cliquez sur Terminer.

9.4 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 de registre. ce qui est particulièrement utile lorsque l'installation est endommagée. Accédez au site Web BusinessObjects suivant pour obtenir les procédures relatives à la désinstallation manuelle de BusinessObjects Enterprise XI : http://support.businessobjects.com/library/kbase/articles/c2017905.asp (http://support.businessobjects.com/library/kbase/articles/c2017905.asp).

Remarque : l'URL ci-dessus était correct lors de la publication de ce document.

9.5 Utilisation de Crystal Reports

Pour plus d'informations concernant l'utilisation de Crystal Reports pour la création de rapport Sentinel, reportez-vous à la documentation de Crystal Reports et au Sentinel User's Guide (Guide de l'utilisateur de Sentinel).

9.6 Présentation générale de l'installation

9.6.1 Présentation de l'installation pour Microsoft SQL 2005 Server avec l'authentification Windows

Pour installer Microsoft SQL Server avec l'authentification Windows :

1. Installez Crystal Reports Server XI : lors de l'installation de l'application Sentinel , si vous sélectionnez l'authentification Windows pour l'utilisateur des rapports Sentinel, suivez le lien vers la Section 9.7.1, « Installation de Crystal Server pour Microsoft SQL 2005 Server avec l'authentification Windows », page 115.
2. Configurez ODBC (Open Database Connectivity).
3. Assignez Crystal Reports pour l'utilisation avec Sentinel.
4. Appliquez le correctif à Crystal Reports.
5. Publiez les rapports.
6. Définissez l'utilisateur comme compte Utilisateur nommé.
7. Importez les modèles Crystal Report
8. Créez une page Web Crystal (Configuration de .NET Administration Launchpad).
9. Configurez Sentinel sur le serveur Crystal Enterprise Server.

Remarque : Vous devez installer Microsoft SQL Server avec l'authentification Windows dans l'ordre indiqué ci-dessus.

9.6.2 Présentation de l'installation pour Microsoft SQL 2005 Server avec l'authentification SQL Server

Pour installer Microsoft SQL Server avec l'authentification SQL Server :

1. Installez Crystal Reports Server XI.

   Remarque : lors de l'installation de l'application Sentinel , si vous sélectionnez l'authentification SQL Server pour l'utilisateur des rapports Sentinel, suivez le lien vers la Section 9.7.2, « Installation de Crystal Server pour Microsoft SQL 2005 Server avec l'authentification SQL », page 121.

   ---

2. Configurez ODBC (Open Database Connectivity).
3. Assignation de Crystal Reports pour l'utilisation avec Sentinel
4. Importez les modèles Crystal Report
5. Créez une page Web Crystal (Configuration de .NET Administration Launchpad).
6. Configurez Sentinel sur le serveur Crystal Enterprise Server.

Remarque : Vous devez installer Microsoft SQL Server avec l'authentification SQL Server dans l'ordre indiqué ci-dessus.

9.6.3 Présentation de l'installation pour Oracle

Pour installer Oracle :

Pour installer correctement Crystal Reports, effectuez les tâches suivantes dans l'ordre indiqué.

1. Installer Oracle 9i Client
2. Installez Crystal Reports Server XI. Pour plus d'informations, reportez-vous à Section 9.7.2, « Installation de Crystal Server pour Microsoft SQL 2005 Server avec l'authentification SQL », page 121.
3. Configurez le pilote natif Oracle.
4. Assignation de Crystal Reports pour l'utilisation avec Sentinel
5. Importez les modèles Crystal Report
6. Créez une page Web Crystal (Configuration de .NET Administration Launchpad).
7. Configurez Sentinel sur le serveur Crystal Enterprise Server.

Remarque : Vous devez installer Oracle dans l'ordre indiqué ci-dessus.

9.7 Installation

Cette section explique comment installer Crystal Server pour :

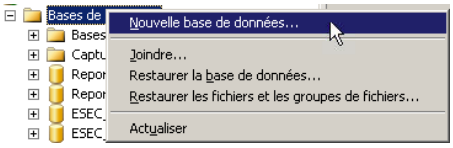
- une base de données Sentinel Microsoft SQL 2005 Server avec l'authentification Windows ;
- une base de données Sentinel Microsoft SQL 2005 Server avec l'authentification SQL Server ;
- base de données Sentinel Oracle

9.7.1 Installation de Crystal Server pour Microsoft SQL 2005 Server avec l'authentification Windows

Pour installer BOE XI Crystal Server avec l'authentification Windows :

1. Installez Microsoft SQL 2005 en mode mixte.
2. Lancez Microsoft SQL Management Studio.
3. Dans le volet de navigation, agrandissez Bases de données.

   Mettez en surbrillance et cliquez droit sur Base de données et sélectionnez Nouvelle base de données…



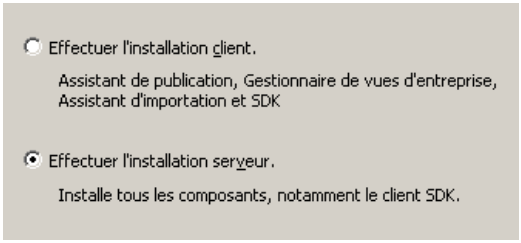
4 Dans le champ Nom de la base de données, indiquez BOE11, puis cliquez sur OK.

5 Quittez Microsoft SQL Management Studio.

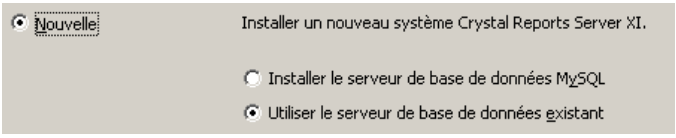
6 Insérez le CD de Crystal Reports XI Server dans l'unité de CD-ROM.

7 Si le lancement automatique est inactif sur la machine, exécutez setup.exe.

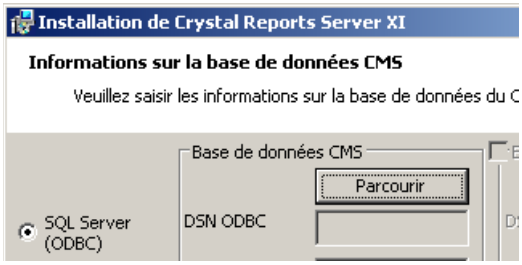
8 Dans la fenêtre Sélectionner l'installation de client ou de serveur, sélectionnez Effectuer l'installation du serveur.



9 Pour le type d'installation, sélectionnez Nouveau et ne sélectionnez pas Installer MSDE ou utiliser SQL Server local existant.



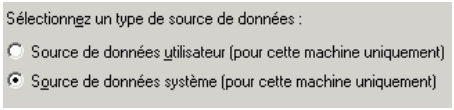
10 Dans le volet de la base de données CMS, cliquez sur Parcourir.



11 Cliquez sur l'onglet Source de données de la machine.

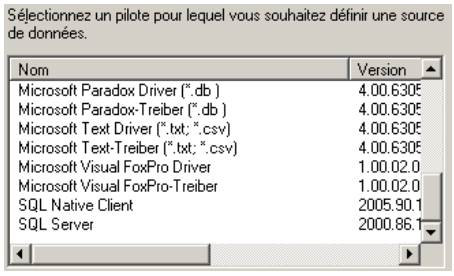
12 Cliquez sur Nouveau.

13 Sélectionnez Source de données du système.



Cliquez sur Suivant.

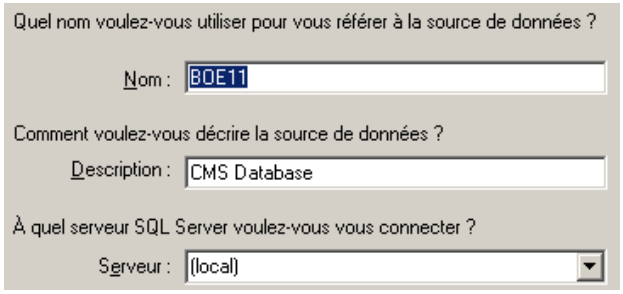
14 Défilez vers le bas pour sélectionner SQL Server, puis cliquez sur Suivant.



15 Une nouvelle source s'affiche, cliquez sur Terminer.

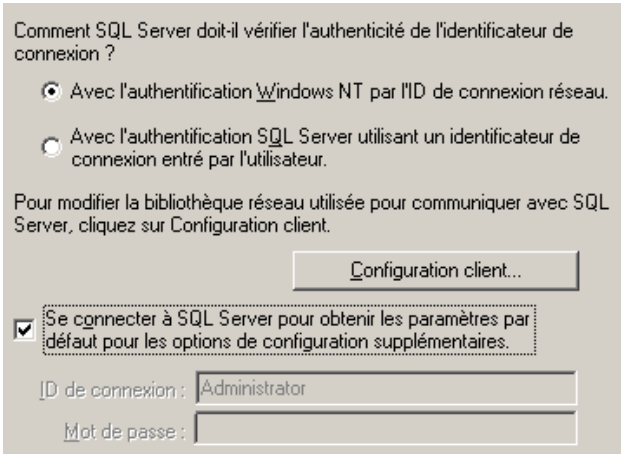
16 Dans la fenêtre Créer une nouvelle source de données vers SQL Server, spécifiez les éléments suivants :

- nom de votre source de données (par ex. BOE_XI)
- description (facultative)
- Pour le serveur, cliquez sur la flèche bas et sélectionnez (local).



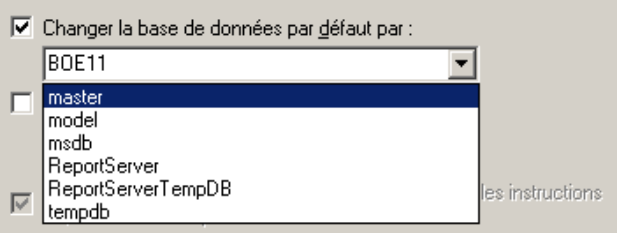
Cliquez sur Suivant.

Si ce n'est déjà fait, sélectionnez l'authentification Windows NT, puis cliquez sur Suivant.



Remarque : l'ID de login (en gris) correspond à votre nom de login Windows.

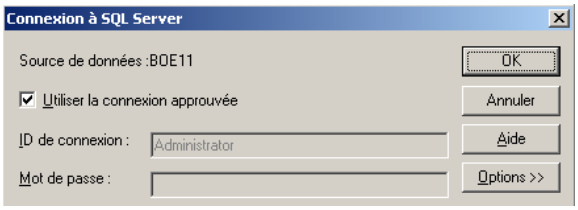
Cochez la case Changer la base de données par défaut par. Remplacer la base de données par défaut par BOE11. Cliquez sur Suivant.



17 Dans la fenêtre Créer une nouvelle source de données vers SQL Server, cliquez sur Terminer.

18 Cliquez sur Tester la source de données et testez cette dernière. Si le test réussit, cliquez sur OK.

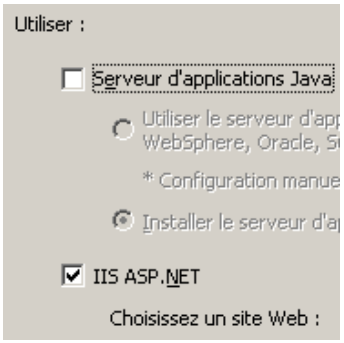
Dans la fenêtre Sélectionner une source de données, sélectionnez BOE11, puis cliquez sur OK successivement, jusqu'à ce que vous obteniez le login SQL Server. Assurez-vous que l'option Utiliser connexion approuvée est sélectionnée. Cliquez sur OK.



Remarque : l'ID de login (en gris) correspond à votre nom de login Windows.

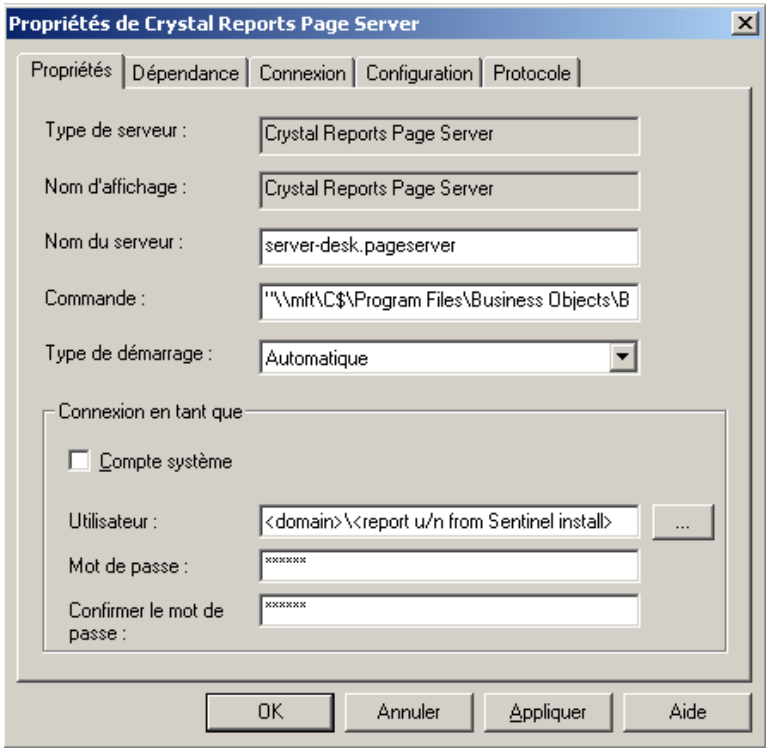
19 Dans la fenêtre Type d'adaptateur au composant Web, sélectionnez IIS ASP.NET.

Remarque : Si vous n'avez pas installé IIS et ASP.NET via le Panneau de configuration > Ajouter ou supprimer des programmes > Ajouter ou supprimer des composants Windows, IIS et ASP.NET sont grisés.



1 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.

- Cliquez sur Démarrer > Tous les programmes > BusinessObjects > Crystal Reports Server> Central Configuration Manager.
- Cliquez avec le bouton droit sur Crystal Reports Page Server et sélectionnez Arrêter.
- Cliquez de nouveau avec le bouton droit sur Crystal Reports Page Server et sélectionnez Propriétés.
- 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 Cliquez sur OK.



2 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

Pour configurer une source de données ODBC pour l'authentification Windows :

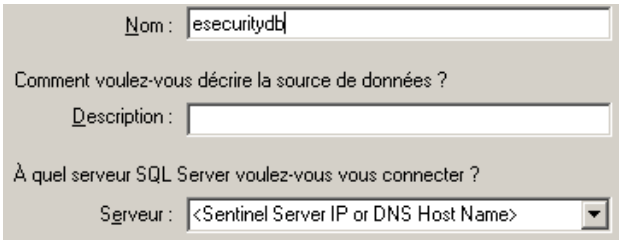
1 Sous Windows, allez dans le Panneau de configuration > Outils d'administration > Sources de données (ODBC)

2 Cliquez sur l'onglet DSN du système et cliquez sur Ajouter.

3 Sélectionnez SQL Server. Cliquez sur Terminer.

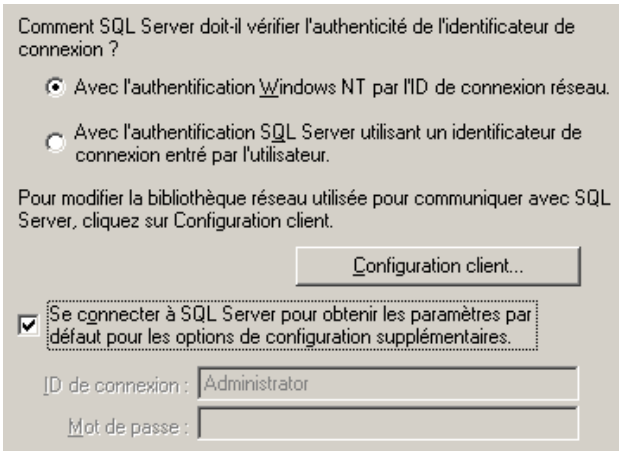
4 Un écran s'affiche demandant les informations de configuration de l'unité :

- nom de source de données, entrez esecuritydb
- champ Description (facultatif), entrez une description
- champ Serveur, entre le nom d'hôte ou l'adresse IP du serveur Sentinel



Cliquez sur Suivant.

Sur l'écran suivant, sélectionnez Authentification Windows.



Remarque : l'ID de login (en gris) correspond à votre nom de login Windows.

---

5 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.

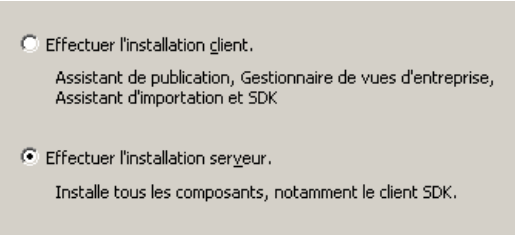
6 Cliquez sur Terminer.

7 Cliquez sur Tester source de données…. Vous devriez obtenir une connexion réussie. Cliquez sur OK jusqu'à la fermeture.

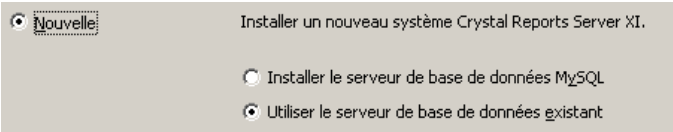
9.7.2 Installation de Crystal Server pour Microsoft SQL 2005 Server avec l'authentification SQL

Pour authentifier BOE XI Crystal Server SQL :

Dans la fenêtre Sélectionner l'installation de client ou de serveur, sélectionnez Effectuer l'installation du serveur.

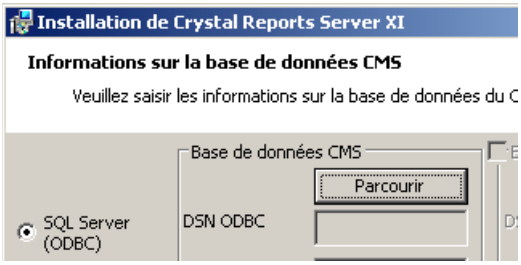


1 Installez un nouveau système BusinessObjects Enterprise avec installation de MSDE ou utilisez le serveur SQL Server local existant.



Remarque : Les serveurs Crystal Server et Microsoft SQL Server doivent se trouver sur la même machine.

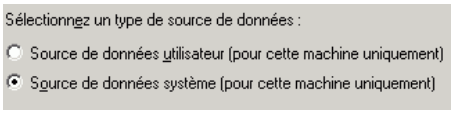
2 Dans le volet de la base de données CMS, cliquez sur Parcourir.



3 Cliquez sur l'onglet Source de données de la machine.

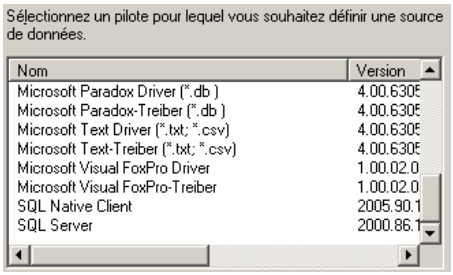
4 Cliquez sur Nouveau.

Sélectionnez Source de données du système.



Cliquez sur Suivant.

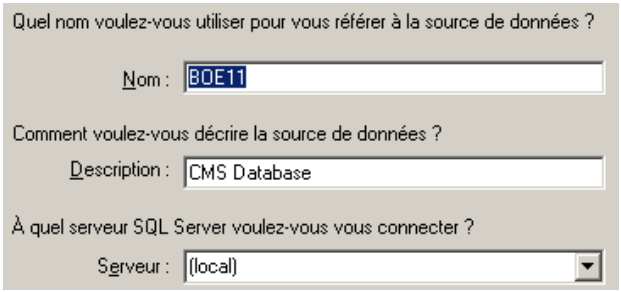
Défilez vers le bas pour sélectionner SQL Server, puis cliquez sur Suivant.



Une nouvelle source s'affiche, cliquez sur Terminer.

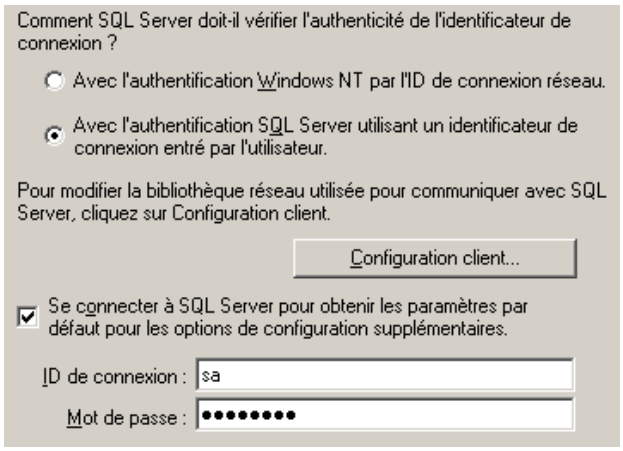
5 Dans la fenêtre Créer une nouvelle source de données vers SQL Server, spécifiez les éléments suivants :

- nom de votre source de données (par ex. BOE_XI)
- description (facultative)
- Pour le serveur, cliquez sur la flèche bas et sélectionnez (local).

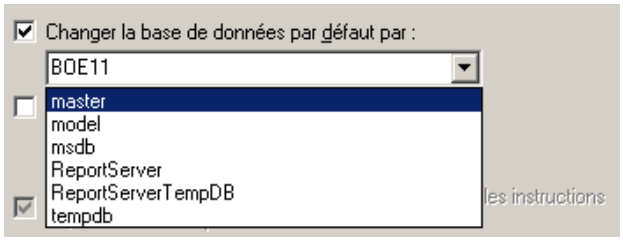


Cliquez sur Suivant.

6 Si ce n'est déjà fait, sélectionnez l'authentification avec SQL Server, tapez sa comme nom d'utilisateur et entrez le mot de passe correspondant. Cliquez sur Suivant.



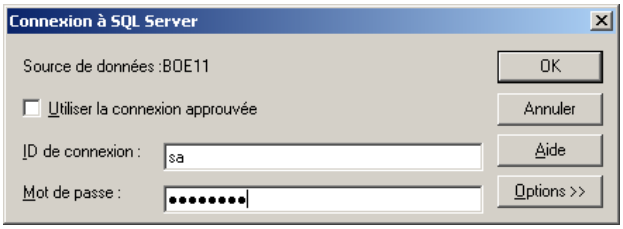
Cochez la case Changer la base de données par défaut par. Remplacer la base de données par défaut par BOE11. Cliquez sur Suivant.



7 Dans la fenêtre Créer une nouvelle source de données vers SQL Server, cliquez sur Terminer.

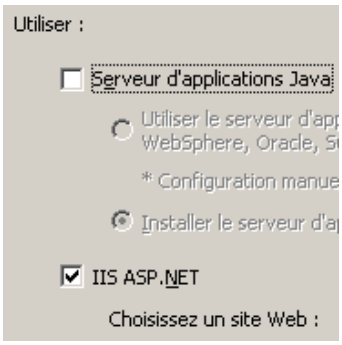
8 Cliquez sur Tester la source de données et testez cette dernière. Si le test réussit, cliquez sur OK.

Dans la fenêtre Sélectionner une source de données, sélectionnez BOE11, puis cliquez sur OK successivement, jusqu'à ce que vous obteniez le login SQL Server. Assurez-vous que l'option Utiliser la connexion approuvée n'est PAS sélectionnée. Cliquez sur OK. Cliquez sur Suivant.



9 Dans la fenêtre Type d'adaptateur au composant Web, sélectionnez IIS ASP.NET.

Remarque : Si vous n'avez pas installé IIS et ASP.NET via le Panneau de configuration > Ajouter ou supprimer des programmes > Ajouter ou supprimer des composants Windows, IIS et ASP.NET sont grisés.



configurer ODBC (Open Database Connectivity) pour l'authentification SQL

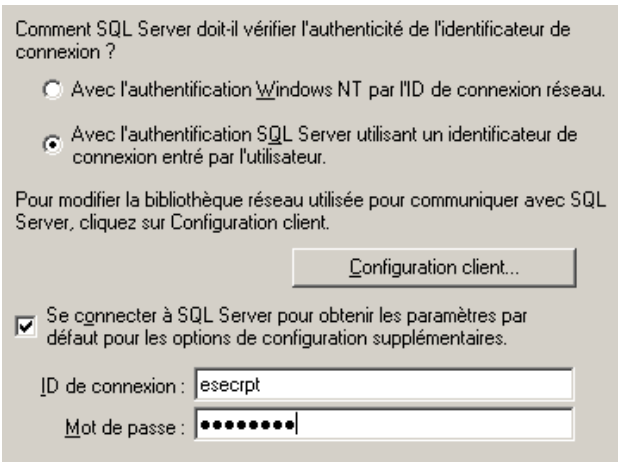
Cette procédure configure une source de données ODBC entre Crystal Reports sous Windows et SQL Server. Elle doit être effectuée sur la machine de Crystal.Server

Pour configurer une source de données ODBC pour Windows :

1. Sous Windows, allez dans le Panneau de configuration > Outils d'administration > 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 esecuritydb
   - 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.

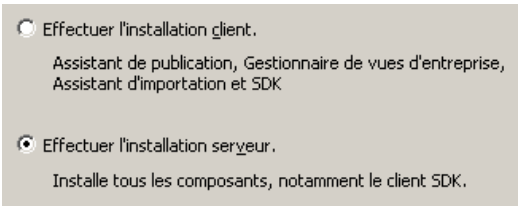
7 Cliquez sur Terminer.

8 Cliquez sur Tester la source de données et testez cette dernière. Si le test réussit, cliquez sur OK. Cliquez sur OK jusqu'à la fermeture.

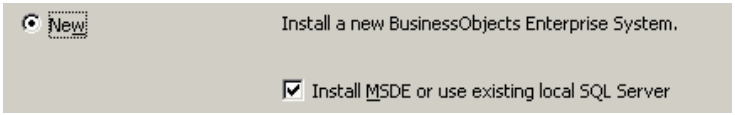
9.7.3 Installation de Crystal Server pour Oracle

Pour installer Crystal Reports Server XI pour Oracle :

- Effectuer l'installation du serveur



- Installer un nouveau système BusinessObjects Enterprise avec Installer MSDE ou utiliser le serveur SQL Server local existant.

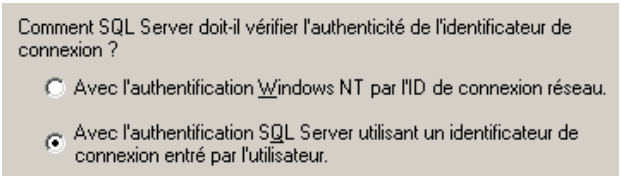


Remarque : les serveurs Crystal Server et Microsoft SQL Server 2005 doivent se trouver sur la même machine.

- IIS ASP.NET

Remarque : Si vous n’avez pas installé IIS et ASP.NET via le Panneau de configuration > Ajouter ou supprimer des programmes > Ajouter ou supprimer des composants Windows, IIS et ASP.NET sont grisés.

- 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 du service TNS : ESEC
- Utilisateur (facultatif) : esecrpt

Après l’installation, créez une configuration du nom de service Net local.

Pour créer une configuration de 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 ESECURITYDB

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.

9.8 Configuration pour toutes les authentifications et configurations

9.8.1 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

Pour configurer inetmgr :

1. Copier le fichier web.config à partir de :
   `C:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content`

   pour c:\Inetpub\wwwroot.
2. Lancez le gestionnaire des services Internet en cliquant sur Démarrer > Exécuter. Entrez inetmgr et cliquez sur OK.
3. Agrandissez (ordinateur local) > Sites Web > Site Web par défaut > businessobjects.
4. Sous 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. Redémarrez IIS en agrandissant (ordinateur local) > Sites Web > Site Web par défaut, sélectionnez Site Web par défaut et cliquez avec le bouton droit >Démarrer.

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. Ces fichiers sont disponibles dans la distribution de Sentinel Reports, qui peut être téléchargée à partir du site du support technique de Novell.

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.

Pour appliquer le correctif à Crystal Reports :

1. Procurez-vous la distribution de Sentinel Reports à partir du site du support technique de Novell.

   Remarque : il est vivement recommandé de consulter les notes de publication de Sentinel Reports avant d'effectuer cette tâche. Elle peut impliquer des fichiers et scripts mis à jour ainsi que des étapes supplémentaires.

2. Depuis la distribution de Sentinel Reports, accédez au répertoire « patch » et copiez tous les fichiers *.html et *.js à l'emplacement des fichiers de la visionneuse, qui est par défaut :

   ```
   C:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content\Enterprise115\viewer\en
   ```

3. Depuis la distribution de Sentinel Reports, accédez au répertoire « patch » et copiez tous les fichiers *.asp et *.js dans :

   ```
   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 dans Crystal Reports Server à l'aide de Crystal Publishing Wizard. La dernière série de modèles de rapport peut être téléchargée à partir du site du support technique de Novell.

Publication des modèles de rapport à l'aide de Crystal Publishing Wizard.

Remarque : il est vivement recommandé de consulter les notes de publication de Sentinel Reports avant d'effectuer cette tâche. Elle peut impliquer des fichiers et scripts mis à jour ainsi que des étapes supplémentaires.

Publication de modèles Crystal Report

Remarque : si vous republiez les modèles de rapports, supprimez la dernière importation de modèles de rapports.

1. Cliquez sur Démarrer > Tous les programmes > Businessobjects > Crystal Reports Server> Publishing Wizard.
2. Cliquez sur Suivant.
3. Connexion. 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. Depuis la distribution de Sentinel Reports, accédez à :

   Pour une base de données Sentinel s'exécutant sous Microsoft SQL :

   `Crystal_v11\SQL-Server`

   Pour une base de données Sentinel s'exécutant sous Oracle :

   `Crystal_v11\Oracle`

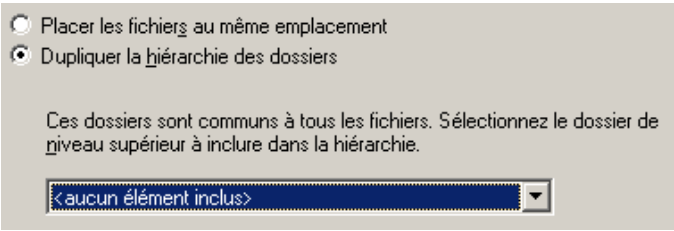
   Cliquez sur OK.
6. Cliquez sur Suivant.

   Dans la fenêtre de spécification de l'emplacement, cliquez sur Nouveau dossier (coin supérieur droit) et créez un dossier nommé SentinelReports. Cliquez sur Suivant.

7 Sélectionner:

- Hiérarchie de dossiers dupliquée.

Cliquez sur la flèche bas et choisissez de ne rien inclure.



Cliquez sur Suivant.

8 Dans la fenêtre Confirmer emplacement, cliquez sur Suivant.

Dans la fenêtre de spécification des catégories, entrez le nom de catégorie de votre choix (Sentinel, par exemple), sélectionnez-le, puis cliquez sur le bouton +.

Remarque : seul le premier rapport apparaît sous la catégorie, après avoir cliqué sur Suivant.

cliquez sur Suivant.

9 Dans la fenêtre Spécifier rafraîchissement de référentiel, cliquez Activer tout pour activer le rafraîchissement de référentiel. Cliquez sur Suivant.

10 Dans la fenêtre Spécifier sauvegarder données enregistrées, cliquez Activer tout pour sauvegarder les données enregistrées lors de la publication des rapports. Cliquez sur Suivant.

11 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.

12 Cliquez sur Suivant pour ajouter les objets.

13 Cliquez sur Suivant.

14 Une liste publiée s'affiche, cliquez sur Terminer.

Lors de la publication des modèles Sentinel pour Crystal Reports sur le serveur Crystal Enterprise Server, les modèles doivent se trouver dans le répertoire SentinelReports.

9.8.2 Configuration du compte Utilisateur nommé

La clé de licence fournie avec Crystal Server est une clé de compte Utilisateur nommé. Le compte Guest doit être changé, passant d'« Utilisateur simultané » à « Utilisateur nommé ».

Pour définir le compte Guest comme Utilisateur nommé :

1 Cliquez sur Démarrer > Tous les programmes > BusinessObjects > Crystal Reports Server > .Net Administration Launchpad.

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. Cliquez sur Se loguer.
5. Sur le panneau Organiser, cliquez sur Utilisateurs.
6. Cliquez sur Guest.
7. Changez le type de connexion en passant d'Utilisateur simultané à Utilisateur nommé.
8. Cliquez sur Mettre à jour.
9. Déloguez-vous et fermez la fenêtre ou avancez vers la section Configuration de.NET Administration Launchpad.

9.8.3 Configuration des autorisations de rapport

Cette procédure explique comment utiliser .NET Administration Launchpad afin de configurer les autorisations relatives aux rapports pour vous permettre de consulter et de modifier des rapports à la demande.

Pour configurer des autorisations de rapport :

1. Si ce n'est déjà fait, démarrez .NET Administration Launchpad (cliquez sur Démarrer > Tous les programmes > BusinessObjects > 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 SentinelReports.
6. Sélectionner tout.
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.
9. Cliquez sur Mettre à jour.
10. Déloguez-vous et fermez la fenêtre.

Test de la connexion du serveur Web à la base de données

Pour tester la connexion du serveur Web à la base de données :

1. Si ce n'est déjà fait, démarrez .Net Administration Launchpad (Démarrer > Tous les programmes > BusinessObjects > 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. Allez dans Dossiers > SentinelReports > Événements 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

Pour tester la connectivité avec le serveur Web :

1 Entrez sur une autre machine mais sur le même réseau que le serveur Web

2 Entrez

```
http://<DNS name or IP address of your web server>/businessobjects/
enterprise11/WebTools/adminlaunch/default.aspx
```

Une page Web Crystal BusinessObjects devrait s'afficher.

9.8.4 Désactivation des 10 principaux rapports Sentinel

Par défaut, les 10 principaux rapports Sentinel sont activés. Pour les désactiver, vous devez :

- désactiver le regroupement ;
- désactiver EventFileRedirectService.

Pour désactiver le regroupement :

1 Démarrer Sentinel Data Manager

2 Connexion.

3 Cliquez sur l'onglet Données de la création de rapport.

4 Désactivez les récapitulatifs suivants :

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Cliquez sur Actif dans la colonne relative à l'état pour qu'il devienne Inactif.

Nom du récapitulatif	Heure	Attributs	Source	Statut
EventDestSummary	1 heure	CUST_ID.RSRC_ID ...	TransformedEvent	Actif
EventSevDestTxnmyS...	1 heure	CUST_ID.DEST_EV ...	TransformedEvent	Inactif
EventSevDestEvtSum...	1 heure	CUST_ID.DEST_EV ...	TransformedEvent	Inactif
EventSevDestPortSum...	1 heure	SEV.DEST_PORT.C ...	TransformedEvent	Inactif
EventSevSummary	1 heure	CUST_ID.SEV.EVT ...	TransformedEvent	Actif
EventSrcSummary	1 heure	CUST_ID.RSRC_ID ...	TransformedEvent	Actif

Pour désactiver EventFileRedirectService :

1 Sur la machine DAS, à l'aide de l'éditeur de texte, ouvrez :

Pour UNIX :

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

Pour Windows:

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

2. Pour EventFileRedirectService, changez l'état en désactivé (off).

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

3. Redémarrez le composant DAS en suivant les instructions ci-dessous :

Sous Windows :

```
Use Service Manager to stop then start the "sentinel" service.
```

9.8.5 Augmentation de la limite de rafraîchissement des enregistrements pour les rapports de Crystal Enterprise Server

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 d'enregistrements, vous devez reconfigurer Crystal Page Server. Pour ce faire, vous pouvez utiliser Central Configuration Manager ou la page Web Crystal.

Pour reconfigurer Crystal Page Server via Central Configuration Manager :

1. Cliquez Démarrer > Tous les programmes > BusinessObjects > 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 <value greater than 20000 or 0 to disable the
default limit>
```

5. Redémarrez Crystal Page Server.

Pour reconfigurer Crystal Page Server via la page Web Crystal :

1. Cliquez sur Démarrer > Tous les programmes > BusinessObjects > Crystal Reports Server > .Net Administration Launchpad.
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.

9.8.6 Configuration de Sentinel Control Center pour l'intégration avec Crystal Enterprise Server.

Sentinel Control Center peut être configuré pour une intégration avec Crystal Enterprise Server, ce qui permet de consulter Crystal Reports à partir Sentinel Control Center.

Pour activer l'intégration de Sentinel Control Center avec Crystal Enterprise Server, suivez les instructions ci-dessous.

Remarque : cette configuration doit être effectuée uniquement après l'installation de Crystal Enterprise Server et la publication de Crystal Reports sur ce dernier.

Pour configurer Sentinel en vue de son intégration avec 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://<hostname_or_IP_of_web_server>/
   GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Analysis
   ```

   Remarque : <nom_hôte_ou_IP_du_serveur_Web> doit être remplacé par le nom d'hôte ou l'adresse IP 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://<hostname_or_IP_of_web_server>/
   GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Advisor
   ```

   Remarque : <nom_hôte_ou_IP_du_serveur_Web> doit être remplacé par le nom d'hôte ou l'adresse IP 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.

Crystal Reports pour Linux

10

Rubriques traitées dans ce chapitre :

Crystal Business Objects Enterprise™ XI est l'un des outils de création de rapport fonctionnant avec Sentinel.

Ce chapitre traite de l'installation et de la configuration de Crystal Reports Server pour Sentinel.

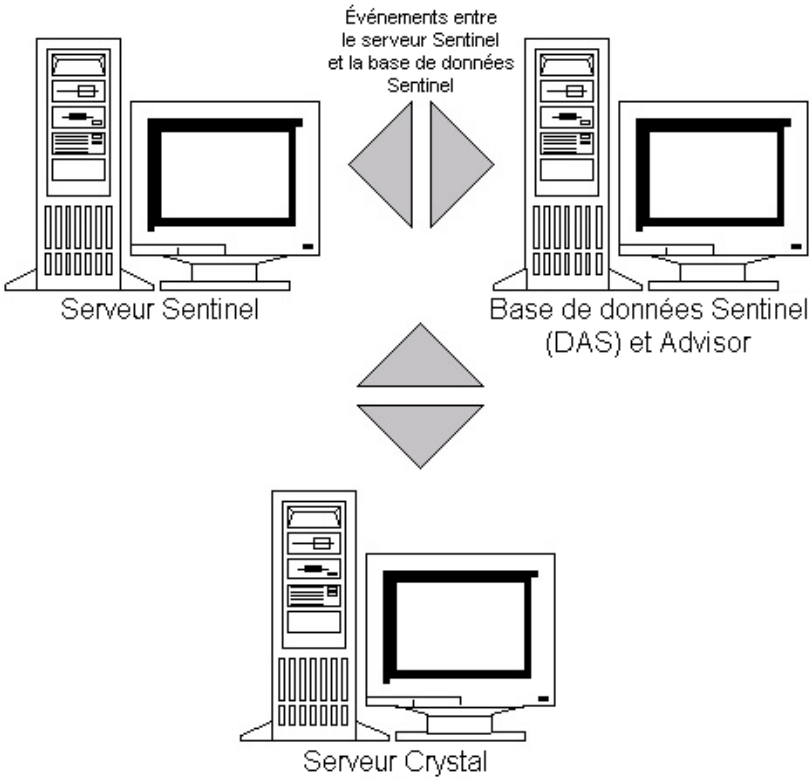
Sentinel prend en charge l'exécution de Crystal Reports Server sur les plates-formes suivantes :

- Windows – Prise en charge si la base de données Sentinel fonctionne sous Windows, Linux ou Solaris ;
- Linux – Prise en charge si la base de données Sentinel fonctionne sous Linux ou Solaris.

Ce chapitre traite de l'exécution de Crystal Reports Server sous Linux. Pour plus d'informations sur Crystal Reports Server sous Windows, reportez-vous au Chapitre 9, « Crystal Reports pour Windows », page 109 dans le Guide d'installation.

Remarque : l'installation doit être effectuée dans l'ordre indiqué ci-dessous.

- Préinstallation et installation de Crystal BusinessObjects Enterprise™ XI
- 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)
- augmentation de la limite de rafraîchissement des enregistrements pour les rapports de Crystal Enterprise Server
- Configuration de Sentinel Control Center pour l'intégration avec Crystal Enterprise Server.



10.1 Utilisation de Crystal Reports

Pour plus d'informations sur l'utilisation de Crystal Reports pour les rapports Sentinel, reportez-vous au Chapitre 9, « Crystal Reports pour Windows », page 109 dans le Guide d'installation.

10.2 Configuration

- Versions Linux :
  - SUSE Linux Enterprise Server (SLES) 9 SP 22
  - 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)

10.3 Installation

10.3.1 Préinstallation de Crystal BusinessObjects Enterprise™ XI

Pour préinstaller Crystal BusinessObjects Enterprise :

1. Si la base de données Sentinel n'est pas sur la même machine que Crystal Server, vous devez alors 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 parce que 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 le cas échéant ; 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 (successivement) 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 configuré dans l'environnement de l'utilisateur crystal. Pour cela, 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, alors ouvrez 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. Pour cela, 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 et faire pointer le nom de service esecuritydb vers la base de données Sentinel. Pour faire cela sur une machine Crystal Server.

    10a Loguez-vous comme utilisateur oracle.

    10b Changez les répertoires vers $ORACLE_HOME/network/admin

    10c Faites une copie du fichier tnsnames.ora..

    10d Ouvrez le fichier tnsnames.ora pour l'éditer.

10e Si la base de données Sentinel est sur la machine Crystal Server, il doit y avoir déjà une entrée dans le fichier tnsnames.ora vers base de données Sentinel. Par exemple, si la base de données Sentinel est nommée ESEC, il y a une entrée égale à la suivante :

```
ESEC =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

10f Si la base de données Sentinel est sur la machine Crystal Server, il doit y avoir déjà une entrée dans le fichier tnsnames.ora vers base de données Sentinel.

10g 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 « esecuritydb ». Par exemple, quant l'entrée mentionnée en haut est copiée et renommée correctement, elle semblera à :

```
esecuritydb =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

10h Vérifiez que la partie HÔTE de l'entrée est correcte (par ex. assurez-vous qu'elle n'est pas définie comme hôte local si le Crystal Server et la base de données Sentinel sont dans des machines différentes.

10i Enregistrez les changements dans le fichier tnsnames.ora.

10j Exécutez la commande suivante pour vérifier que le nom de service esecuritydb est correctement configuré :

```
tnsping esecuritydb
```

10k Si la commande est exécutée avec succès, vous devrez obtenir un message déclarant que la connexion est OK.

10.3.2 Installation de Crystal BusinessObjects Enterprise™ XI

Pour installer Crystal BusinessObjects Enterprise :

1. Loguez-vous comme utilisateur crystal.
2. Changez les répertoires vers le DISK_1 du programme d'installation Crystal.
3. Exécuter:

   ```
   ./install
   ```
4. Sélectionnez la langue : français
5. Sélectionnez Nouvelle Installation

6 Accepter le contrat de licence

7 Entrez le code clé du produit

8 Entrez le répertoire d'installation :
`/opt/crystal_xi`

9 Sélectionnez User Install (Installation par l'utilisateur)

10 Sélectionnez New Install (Nouvelle installation)

11 Sélectionnez Install MySQL (Installer MySQL)

12 Entrez les informations de configuration pour MySQL :

12a Utiliser le port par défaut 3306

12b Mot de passe Admin

13 Entrez plus d'informations de configuration pour MySQL :

13a Default DB Name (Nom de la base de données par défaut) : BOE11

13b User id (ID utilisateur) : mysqladm

13c Mot de passe

14 Entrez plus d'informations de configuration pour MySQL :

14a Local Name Server (Nom du serveur local) : <nom_hôte_machine_locale>

14b Default CMS Port Number (Numéro de port CMS par défaut) : 6400

15 Sélectionnez Install Tomcat (Installer Tomcat)

16 Entrez les informations de configuration de Tomcat :

16a Default Receive HTTP requests port (Port par défaut pour la réception des requêtes HTTP) : 8080

16b Default Redirect jsp requests port (Port par défaut pour la réorientation des requêtes jsp) : 8443

16c Default Shutdown Hook port (Port de raccordement d'arrêt par défaut) : 8005

17 Appuyez sur Enter pour lancer l'installation

10.3.3 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. Ces fichiers sont disponibles dans la distribution de Sentinel Reports, qui peut être téléchargée à partir du site du support technique de Novell.

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.
GetReports.asp	Fichier utilisé par Sentinel Control Center pour établir une connexion avec Crystal Server et afficher la liste de rapports.
GetReportURL.jsp	Fichier utilisé pour prendre en charge les liens hypertexte entre les rapports

Pour appliquer le correctif à Crystal Reports :

1. Procurez-vous la distribution de Sentinel Reports à partir du site du support technique de Novell.

   Remarque : il est vivement recommandé de consulter les notes de publication de Sentinel Reports avant d'effectuer cette tâche. Elle peut impliquer des fichiers et scripts mis à jour ainsi que des étapes supplémentaires.

2. Depuis la distribution de Sentinel Reports, accédez au répertoire « patch » et copiez tous les fichiers *.html et *.js à l'emplacement des fichiers de la visionneuse, qui est par défaut :
   `/opt/crystal_xi/bobje/webcontent/enterprise11/viewer/en/`
3. Depuis la distribution de Sentinel Reports, accédez au répertoire « patch » et copiez tous les fichiers *.jsp dans :
   `/opt/crystal_xi/bobje/tomcat/webapps/esec-script/`

   Remarque : Créez un dossier nommé esec-script
4. Copiez tous les fichiers *.jar :
   ```
   From:
   /opt/crystal_xi/bobje/tomcat/webapps/jsfadmin/WEB-INF/lib/
   To:
   /opt/crystal_xi/bobje/tomcat/webapps/esec-script/WEB-INF/lib
   ```

   Remarque : créez une structure de dossiers WEB-INF/lib

10.4 Publication de modèles Crystal Report

Remarque : il est vivement recommandé de consulter les notes de publication de Sentinel Reports avant d'effectuer cette tâche. Elle peut impliquer des fichiers et scripts mis à jour ainsi que des étapes supplémentaires.

Ces modèles de rapport sont créés par Novell pour utiliser avec l'analyse de Sentinel Control Center et l'onglet Advisor.

Il y deux méthodes de publication de rapports.

- Crystal Publishing Wizard
- Crystal Reports Central Management Console

Remarque : Pour générer l'un des 10 principaux rapports, le regroupement doit être activé et EventFileRedirectService doit également être activé dans le fichier DAS_Binary.xml. Pour obtenir des informations sur la procédure d'activation du regroupement, reportez-vous à la section Onglet Données de rapport du gestionnaire de données Sentinel dans le guide de l'utilisateur de Sentinel ou consultez la Section 10.8, « Activation de Sentinel Top 10 des rapports », page 147.

10.4.1 Publication des modèles de Rapport - Crystal Publishing Wizard.

Remarque : une plate-forme Window est requise pour l'exécution de Crystal Publishing Wizard.

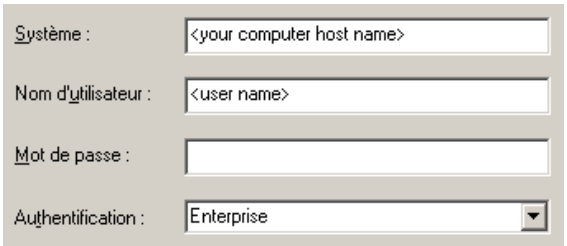
Pour importer des modèles Crystal Report :

Remarque : si vous importez (publiez) les modèles de rapports de nouveau, 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. Connexion. 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 devrez utiliser un autre utilisateur différent de l'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. Depuis la distribution de Sentinel Reports, accédez à :

   `Crystal_v11\Oracle`

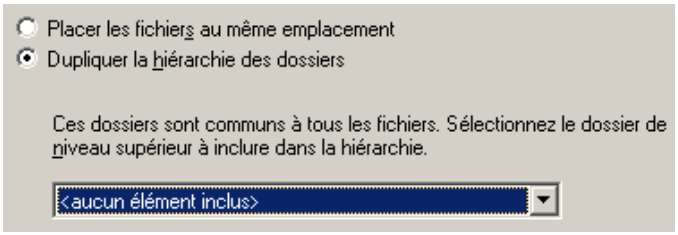
   Cliquez sur OK.

6 Cliquez sur Suivant.

7 Dans la fenêtre de spécification de l'emplacement, cliquez sur Nouveau dossier (dans le coin supérieur droit) et créez un dossier nommé eSecurity_Reports. Cliquez sur Suivant.

8 Sélectionner:

- Hiérarchie de dossiers dupliquée.
- Cliquez sur la flèche bas et choisissez de ne rien inclure.



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 Cliquez sur Terminer.

Quand les modèles Sentinel pour Crystal Reports sont publiés dans Crystal Enterprise server, les modèles doivent se trouver dans le répertoire eSecurity_Reports.

10.4.2 Publication des modèles de Rapport - Central Management Console.

Lors de la publication des rapports à l'aide de Central Management Console, le rapport ne peut pas être publié en lot, comme dans l'utilisation de Publishing Wizard poussé par Windows.

Pour importer des modèles Crystal Report :

1. Ouvrez un navigateur Web et entrez l'URL suivant :
   `http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise11/adminlaunch`
2. Cliquez sur Central Management Console
3. Loguez-vous sur le Crystal Server.
4. Sous le panneau Organiser, cliquez sur Dossiers.
5. Au coin supérieur droit, cliquez sur Nouveau dossier….
6. Créez un dossier nommé eSecurity_Reports. Cliquez sur OK.
7. Cliquez sur eSecurity_Reports.
8. Cliquez sur l'onglet Sous-dossiers et créez les sous-dossiers suivants.
   - vulnérabilité_Advisor
   - gestion incidents
   - évènements internes
   - évènements sécurité
   - Top 10
9. Cliquez sur Accueil.
10. Cliquez sur Objets.
11. Cliquez sur Nouveau Objet.
12. Sur la gauche de la page, sélectionnez Rapport.
13. Cliquez sur Parcourir et accédez au dossier suivant avec la distribution de Sentinel Reports :
    `Crystal_v11\Oracle`
    Choisissez un dossier et sélectionnez un rapport.
14. Sélectionnez eSecurity_Reports, puis 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. Pour ajouter les autres rapports, répétez les étapes 9 à 17 jusqu'à ce qu'ils soient tous ajoutés.

10.5 Utilisation de Crystal XI Web Server

Crystal Server XI sous Linux installe un serveur Web par le biais duquel vous pouvez effectuez des tâches administratives, aussi bien que publier et voir des rapports.

Le portal administratif est accéder via le navigateur à l'URL suivant :

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise11/adminlaunch
```

Le portal non administratif (utilisation générale) est accéder via le navigateur à l'URL suivant :

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise11
```

10.5.1 test de la connectivité serveur Web

Pour tester la connectivité avec le serveur Web :

1. Accédez à une autre machine située sur le même réseau que le serveur Web.
2. Entrez

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise11/adminlaunch
   ```
3. Une page Web Crystal BusinessObjects devrait s'afficher.

10.6 Configurer un compte d'« utilisateur nommé »

La clé de licence fournie avec Crystal Server est une clé de compte Utilisateur nommé. Le compte Guest doit être changé, passant d'« Utilisateur simultané » à « Utilisateur nommé ».

Pour définir le compte Guest comme Utilisateur Nommé :

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

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise11/adminlaunch
   ```
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. Sur le panneau Organiser, cliquez sur Utilisateurs.
5. Cliquez sur Guest.
6. Changez le type de connexion en passant d'Utilisateur simultané à Utilisateur nommé.
7. Cliquez sur Mettre à jour.
8. Déloguez-vous et fermez la fenêtre.

10.7 Configuration des autorisations de rapport

Cette procédure explique comment utiliser Administration Launchpad afin de configurer les autorisations relatives aux rapports pour vous permettre de consulter et de modifier des rapports à la demande.

Pour configurer des autorisations de rapport :

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

   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise11/adminlaunch
   ```

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. Sur le volet Organiser, cliquez sur Dossiers.
6. Cliquez une fois sur eSecurity_Reports.
7. Sélectionner tout.
8. Cliquez sur l'onglet Droits.
9. Pour Tout le monde, sur le menu déroulant vers la droite sélectionnez Affichage à la demande.
10. Cliquez sur Mettre à jour.
11. Déloguez-vous et fermez la fenêtre.

10.8 Activation de Sentinel Top 10 des rapports

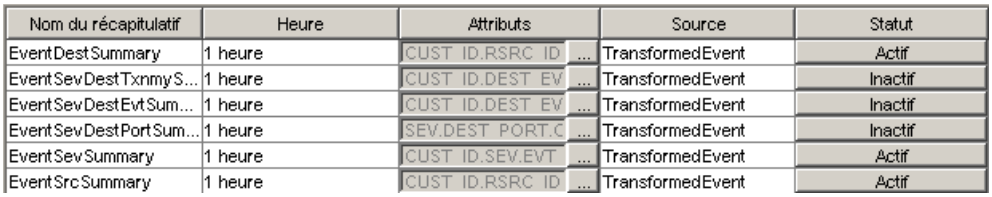
Pour activer Sentinel Top 10 Reports vous devez :

- activer Regroupement
- activer EventFileRedirectService

Pour activer le regroupement :

1. Dans l'interface graphique Sentinel Control Center, cliquez sur l'onglet Admin.
2. Dans le volet de navigation, cliquez sur Données de rapport ou sur le bouton Données de rapport.
3. Activez les résumés suivants :
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

Cliquer sur Inactif dans la colonne Status pour passer à Actif.



Nom du récapitulatif	Heure	Attributs	Source	Statut
EventDestSummary	1 heure	CUST_ID.RSRC_ID ...	TransformedEvent	Actif
EventSevDestTxnmyS...	1 heure	CUST_ID.DEST_EV ...	TransformedEvent	Inactif
EventSevDestEvtSum...	1 heure	CUST_ID.DEST_EV ...	TransformedEvent	Inactif
EventSevDestPortSum...	1 heure	SEV.DEST_PORT.C ...	TransformedEvent	Inactif
EventSevSummary	1 heure	CUST_ID.SEV.EVT ...	TransformedEvent	Actif
EventSrcSummary	1 heure	CUST_ID.RSRC_ID ...	TransformedEvent	Actif

Pour activer 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, transformez l'état en « actif ».
   `<property name="status">on</property>`
3. Redémarrer le processus DAS_Binary. Ce qui peut être fait à l'aide de Sentinel Control Center or en redémarrant la machine.

   Utilisation de Sentinel Control Center :

   - Loguez-vous au Sentinel Control Center comme un utilisateur aux droits d'administrateur. Cet utilisateur doit avoir les autorisations Vues du serveur suivantes :
     - Afficher serveurs
     - Controler serveurs
   - Depuis l'onglet Admin, ouvrez un vue de serveur pour voir tous les processus du serveur Sentinel.
   - Cliquez avec le bouton droit sur le processus DAS_Binary et sélectionnez Redémarrer.
   - Le nombre de démarrages pour ce processus augmentera d'une unité si le processus a bien redémarré.

10.9 Augmentation de la limite de rafraîchissement des enregistrements pour les rapports de Crystal Enterprise Server

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 d'enregistrements, vous devez reconfigurer Crystal Page Server.

Pour reconfigurer Crystal Page Server :

1. Ouvrez un navigateur Web et entrez l'URL suivant :
   `http://`
   `<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/`
   `businessobjects/enterprise11/adminlaunch`
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.

10.10 Configuration de Sentinel Control Center pour l'intégration avec Crystal Enterprise Server.

Sentinel Control Center peut être configuré pour une intégration avec Crystal Enterprise Server, ce qui permet de consulter Crystal Reports depuis Sentinel Control Center.

Pour activer l'intégration de Sentinel Control Center avec Crystal Enterprise Server, suivez les instructions ci-dessous.

Remarque : cette configuration doit être effectuée uniquement après l'installation de Crystal Enterprise Server et la publication de Crystal Reports sur ce dernier.

Pour configurer Sentinel en vue de son intégration avec 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://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   esec-script/
   GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
   ```

   Remarque : <nom_hôte_ou_IP_du_serveur_Web> doit être remplacé par le nom d'hôte ou l'adresse IP de Crystal Enterprise Server.

   Remarque : l'URL ci-dessus ne marche pas correctement si l'APS est configuré à l'adresse IP. Il doit être le nom d'hôte.

   Remarque : <port_serveur_Web_défaut_8080> doit être remplacé par le port sur lequel le serveur Crystal Web écoute.

   ---
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://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   esec-script/
   GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
   ```

Remarque : <nom_hôte_ou_IP_du_serveur_Web> doit être remplacé par le nom d'hôte ou l'adresse IP de Crystal Enterprise Server.

Remarque : l'URL ci-dessus ne marche pas correctement si l'APS est configuré à l'adresse IP. Il doit être le nom d'hôte.

Remarque : <port_serveur_Web_défaut_8080> doit être remplacé par le port sur lequel le serveur Crystal Web écoute.

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.

10.11 Utilitaires et dépannage

10.11.1 Démarrage de MySQL

Pour vous assurer que MySQL est en cours d'exécution :

1. Loguez-vous comme utilisateur crystal.
2. cd /opt/crystal_xi/bobje
3. ./mysqlstartup.sh

10.11.2 Démarrage de Tomcat

Pour vous assurer que Tomcat est en exécution :

1. Loguez-vous comme utilisateur crystal
2. cd /opt/crystal_xi/bobje
3. ./tomcatstartup.sh

10.11.3 Démarrage de serveurs Crystal server

Pour vous assurer que les serveurs Crystal server sont en exécution :

1. Loguez-vous comme utilisateur crystal
2. cd /opt/crystal_xi/bobje
3. ./startservers

10.11.4 Erreur de nom d'hôte Crystal

Pour résoudre une erreur de nom d'hôte :

1. Si l'erreur suivant s'affiche :

   ```
   Warning: ORB::BOA_init: hostname lookup returned `localhost'
   (127.0.0.1)
   Use the -OAhost option to select some other hostname
   ```

   Assurez-vous que votre IP et votre nom d'hôte sont dans le fichier /etc/hosts. Exemple :

   ```
   192.0.2.46linuxCE02
   ```

10.11.5 Impossible de connecter à CMS

Si le système rapport qu'il ne peut pas se connecter à CMS, essayez l'exécution des commandes suivantes.

Pour remédier à un échec de connexion CMS :

1. Si la commande « netstat –an | grep 6400 » ne renvoie aucun résultat, procédez comme suit.
   - Réinsérez les informations de connexion MySQL
     a. Loguez-vous comme utilisateur crystal
     b. cd /opt/crystal_xi/bobje
     c. ./cmsdbsetup.sh
     d. Appuyez sur Entrée lorsque [<nom_hôte>.cms] s'affiche
     e. Choisissez Sélectionner et entrez de nouveau toutes les informations de la base de données MySQL qui ont été spécifiées lors de l'installation. Pour plus d'informations, reportez-vous aux instructions d'installation.
     f. À l'accomplissement, quitter cmsdbsetup.sh
     g. ./stopservers
     h. ./startservers
   - Redémarrez la base de données MySQL
     a. Loguez-vous comme utilisateur crystal
     b. cd /opt/crystal_xi/bobje
     c. ./cmsdbsetup.sh
     d. Appuyez sur Entrée lorsque [<nom_hôte>.cms] s'affiche
     e. Choisissez de réinitialiser et suivez les instructions.
     f. À l'accomplissement, quitter cmsdbsetup.sh
     g. ./stopservers
     h. ./startservers
2. Assurez-vous que tous les serveurs CCM sont activés :
   2a Loguez-vous comme utilisateur crystal
   2b cd /opt/crystal_xi/bobje

2c ./ccm.sh -enable all

Désinstallation de Sentinel 11

Rubriques traitées dans ce chapitre :

Pour supprimer une installation Sentinel, vous disposez de programmes de désinstallation pour Linux, Solaris et Windows. Plusieurs fichiers, y compris des fichiers journaux, sont conservés et peuvent être supprimés manuellement, le cas échéant. En outre, il est vivement recommandé d'effectuer chacune des opérations suivantes pour éviter que des fichiers ou des paramètres système d'une ancienne installation subsistent et nuisent à une nouvelle installation.

Avertissement : ces instructions impliquent la modification de fichiers et de paramètres du système d'exploitation. Si vous n'avez pas l'habitude de ce type d'intervention, contactez votre administrateur système.

11.1 Désinstallation de Sentinel

11.1.1 Procédure de désinstallation pour Solaris et Linux

Pour démarrer le programme de désinstallation de Sentinel pour Solaris :

1. Loguez-vous comme utilisateur root.
2. Arrêtez le serveur Sentinel.
3. Instructions d'installation:
   `$ESEC_HOME/_uninst`
4. Entrez :
   `./uninstall.bin`
5. Sélectionnez une langue et cliquez sur OK.
6. L'Assistant Sentinel Install Shield Wizard s'affiche. Cliquez sur Suivant.
7. Sélectionnez les composants à désinstaller, puis cliquez sur Suivant.

   Remarque : Sentinel affiche un avertissement demandant de fermer toutes les applications Sentinel ouvertes.

   ---

8. Vous devez alors choisir entre deux options :
   - Supprimer l'intégralité de l'instance de la base de données
   - Supprimer uniquement les objets de la base de données

Sélectionnez l'une des options et cliquez sur Suivant.

9 Cliquez sur Uninstall.

11.1.2 Procédure de désinstallation sous Windows

Pour utiliser le programme de désinstallation de Sentinel sous Windows :

1 Loguez-vous comme administrateur.

2 Arrêtez le serveur Sentinel.

3 Sélectionnez Démarrer > Tous les programmes > Sentinel > Désinstaller Sentinel.

4 Sélectionnez une langue et cliquez sur OK.

5 L'Assistant Sentinel Install Shield Wizard s'affiche. Cliquez sur Suivant.

6 Sélectionnez les composants à désinstaller, puis cliquez sur Suivant.

Remarque : Sentinel affiche un avertissement demandant de fermer toutes les applications Sentinel ouvertes.

---

7 Vous devez alors choisir entre deux options :

- Supprimer l'intégralité de l'instance de la base de données
- Supprimer uniquement les objets de la base de données

Sélectionnez l'une des options et cliquez sur Suivant.

8 Spécifiez les informations d'authentification, sélectionnez l'authentification Windows ou SQL, et entrez les références de login si elles vous sont demandées. Cliquez sur Suivant.

9 Le résumé des éléments sélectionnés pour la désinstallation s'affiche. Cliquez sur Uninstall.

10 Choisissez de redémarrer le système et cliquez sur Terminer.

11.1.3 Désinstallation à l'aide du Panneau de configuration

Pour désinstaller des applications Sentinel sous Windows :

1 Cliquez sur Démarrer > Panneau de configuration > Ajouter ou supprimer des programmes > Sentinel > Modifier/Supprimer.

2 Sélectionnez une langue et cliquez sur OK.

3 L'Assistant Sentinel Install Shield Wizard s'affiche. Cliquez sur Suivant.

4 Sélectionnez les composants à désinstaller, puis cliquez sur Suivant.

Remarque : Sentinel affiche un avertissement demandant de fermer toutes les applications Sentinel ouvertes.

---

5 Vous devez alors choisir entre deux options :

- Supprimer l'intégralité de l'instance de la base de données
- Supprimer uniquement les objets de la base de données

Sélectionnez l'une des options et cliquez sur Suivant.

6 Spécifiez les informations d'authentification, sélectionnez l'authentification Windows ou SQL, et entrez les références de login si elles vous sont demandées. Cliquez sur Suivant

7 Le résumé des éléments sélectionnés pour la désinstallation s'affiche. Cliquez sur Uninstall.

8 Choisissez de redémarrer le système et cliquez sur Terminer.

11.2 Tâches de post-désinstallation

11.2.1 Fichiers de données Sentinel

Afin de préserver des informations potentiellement importantes après la désinstallation de Sentinel, divers fichiers sont conservés. Si ces informations ne sont plus utiles, vous pouvez supprimer manuellement les fichiers et dossiers suivants.

- Tiers
  - SonicMQ
    - Docs7.0
    - InstallLogs7.0
    - MQ7.0
    - Installateur
    - mq_documentation_7.0.htm
    - sonicsw.properties
    - uninstall.sh
    - wizard.jar
- Bin
  - control_center.ja
  - sdm_gui.jac
- Config
  - .proxyServerKeystore
  - .primary_key
  - .keystore
- Données
  - .cache
  - .sessionState
  - .uuid
  - .uuidlock
  - DatabaseManager.log
  - agent-84EBED40-9AB1-1029-9C3F-0003BAC9707D.lck
  - collector_mgr.cache
  - eventfiles
  - map_data
  - portcfg_84EBED40-9AB1-1029-9C3F-0003BAC9707D.dat

- uuid.dat
- Install_log
  - CreateAdminUserSimpleErr.txt
  - CreateAdminUserSimpleOut.txt
  - PostInstallSetup2Err.log
  - PostInstallSetup2Out.log
  - PostInstallSetupErr.log
  - PostInstallSetupOut.log
  - advcronjoberr.txt
  - advcronjobout.txt
  - configupdateerr.txt
  - configupdateout.txt
  - containerFileUpdate.log
  - cronjoberr.txt
  - cronjobout.txt
  - db
  - dbupdateerr.txt
  - dbupdateout.txt
  - extractJre64_err.log
  - extractJre64_out.log
  - key_generation.log
  - sentinelInstall.log
  - sentinelUninstall.log
  - shutdown_database_err.log
  - shutdown_database_out.log
  - sonic_silent_install_err.log
  - sonic_silent_install_out.log
  - sonic_silent_uninstall_err.log
  - sonic_silent_uninstall_out.log
  - stopAM_err.txt
  - stopAM_out.txt
  - stopSentinel_err.txt
  - stopSentinel_out.txt
  - uninstallDB_err.log
  - uninstallDB_out.log
  - Tous ces fichiers se trouvent dans le répertoire $ESEC_HOME ou %ESEC_HOME% et ses sous-répertoires.
  - Pour Advisor, les dossiers relatifs aux attaques et aux alertes utilisés pour les fichiers de données Advisor sont conservés.

11.2.2 Paramètres Sentinel

Après la désinstallation de Sentinel, certains paramètres système subsistent et peuvent être supprimés manuellement. Ils doivent d'ailleurs être supprimés avant de procéder à une nouvelle installation de Sentinel, surtout si le programme de désinstallation de Sentinel a rencontré des erreurs.

Remarque : sous Solaris et Linux, la désinstallation de Sentinel Server ne supprime pas l'administrateur Sentinel du système d'exploitation. Si vous le souhaitez, supprimez-le manuellement.

Suppression des paramètres système Sentinel sous Linux avec Oracle

Pour nettoyer Sentinel manuellement sous Linux :

1. Loguez-vous comme utilisateur root.
2. Assurez-vous que tous les processus Sentinel sont arrêtés.
3. Supprimez le contenu du répertoire /opt/sentinelXX (ou de tout autre emplacement dans lequel le logiciel Sentinel a été installé et nommé).
4. Supprimez le fichier S98sentinel du répertoire /etc/rc.d/rc5.d.
5. Supprimez le fichier S98sentinel du répertoire /etc/rc.d/rc3.d.
6. Supprimez le fichier K02sentinel du répertoire /etc/rc.d/rc0.d.
7. Supprimez le fichier sentinel du répertoire /etc/init.d.
8. Supprimez le répertoire /root/Install Shield.
9. Supprimez le fichier /root/vpd.properties.
10. Assurez-vous que personne n'est logué en tant qu'administrateur Sentinel (par défaut, esecadm), puis supprimez cet utilisateur (ainsi que son répertoire privé) et le groupe esec.
    - Exécutez : userdel -r esecadm
    - Exécutez : groupdel esec
11. Si le fichier .login existe, supprimez la section Install Shield du fichier /etc/profile, /etc/.login
12. Supprimez la base de données Oracle Sentinel. Pour plus d'informations, reportez-vous à « Pour nettoyer manuellement la base de données Oracle Sentinel sous Linux : » page 157.
13. Redémarrez le système d'exploitation.

Pour nettoyer manuellement la base de données Oracle Sentinel sous Linux :

Remarque : assurez-vous qu'aucune autre application n'utilise la base de données avant de la supprimer.

---

1. Loguez-vous comme oracle.
2. Arrêtez le processus d'écoute Oracle :
    - Exécutez : lsnrctl stop

3. Arrêtez la base de données Sentinel.
   - Définissez la variable d'environnement ORACLE_SID sur le nom de votre instance de base de données Sentinel (généralement ESEC).
   - Exécutez : sqlplus '/ as sysdba'
   - À l'invite sqlplus, exécutez : shutdown immediate
4. Supprimez l'entrée pour la base de données Sentinel dans le fichier /etc/oratab
5. Supprimez le fichier init<nom_instance>.ora (généralement initESEC.ora) du répertoire $ORACLE_HOME/dbs.
6. Supprimez les entrées pour votre base de données Sentinel des fichiers suivants situés dans le répertoire $ORACLE_HOME/network/admin :
   - tnsnames.ora
   - listener.ora
7. Supprimez les fichiers de données de la base de données situés à l'emplacement choisi pour leur installation.

Suppression des paramètres système Sentinel sous Solaris avec Oracle

Pour nettoyer Sentinel manuellement sous Solaris :

Remarque : Le nettoyage manuel est généralement pratiqué lorsque le programme de désinstallation de Sentinel rencontre une erreur.

---

1. Loguez-vous comme utilisateur root.
2. Assurez-vous qu'aucun processus Sentinel n'est en cours d'exécution.
3. Supprimez le contenu du répertoire /opt/sentinelXX (ou de tout autre emplacement dans lequel le logiciel Sentinel a été installé).
4. Supprimez le fichier S98sentinel du répertoire /etc/rc3.d.
5. Supprimez le fichier K02sentinel du répertoire /etc/rc0.d.
6. Supprimez le fichier sentinel du répertoire /etc/init.d.
7. Nettoyez les références install shield dans /var/sadm/pkg. Supprimez les fichiers suivants du répertoire /var/sadm/pkg :
   - tous les fichiers commençant par IS (IS* dans la ligne de commande) ;
   - tous les fichiers commençant par ES (ES* dans la ligne de commande) ;
   - tous les fichiers commençant par MISCwp (MISCwp* dans la ligne de commande) ;
8. Assurez-vous que personne n'est logué en tant qu'administrateur Sentinel, puis supprimez cet utilisateur (ainsi que son répertoire privé) et le groupe esec.
   - Exécutez : userdel -r esecadm
   - Exécutez : groupdel esec
9. Si le fichier .login existe, supprimez la section Install Shield de /etc/profile, /etc/.login
10. Supprimez le répertoire /Install Shield s'il en existe un.

11 Redémarrez le système d'exploitation.

Pour nettoyer manuellement la base de données Oracle Sentinel sous Solaris :

Remarque : assurez-vous qu'aucune autre application n'utilise la base de données avant de la supprimer.

---

1 Loguez-vous comme oracle.

2 Arrêtez le processus d'écoute Oracle :

- Exécutez : lsnrctl stop

3 Arrêtez la base de données Sentinel :

- Définissez la variable d'environnement ORACLE_SID sur le nom de votre instance de base de données Sentinel (généralement ESEC).
- Exécutez : sqlplus '/ as sysdba'
- À l'invite sqlplus, exécutez : shutdown immediate

4 Supprimez l'entrée pour la base de données Sentinel dans le fichier /var/opt/oracle/oratab

5 Supprimez le fichier init<nom_instance>.ora (généralement initESEC.ora) du répertoire $ORACLE_HOME/dbs.

6 Supprimez les entrées pour votre base de données Sentinel des fichiers suivants situés dans le répertoire $ORACLE_HOME/network/admin :

- tnsnames.ora
- listener.ora

7 Supprimez les fichiers de données de la base de données situés à l'emplacement choisi pour leur installation.

Suppression des paramètres système Sentinel sous Windows avec SQL Server

Pour nettoyer Sentinel manuellement sous Windows :

1 Supprimez le dossier %CommonProgramFiles%\InstallShield\Universal et l'ensemble de son contenu.

2 Supprimez le dossier %ESEC_HOME% (par défaut : C:\Program Files\novell\sentinel6).

3 Cliquez avec le bouton droit sur Poste de travail > Propriétés > Onglet Avancé.

4 Cliquez sur le bouton Variables d'environnement.

5 Si elles existent, supprimez les variables suivantes :

- ESEC_HOME
- ESEC_VERSION
- ESEC_JAVA_HOME
- ESEC_CONF_FILE
- WORKBENCH_HOME

6 Supprimez toutes les entrées dans la variable d'environnement PATH qui pointent vers l'installation Sentinel.

Avertissement : ne supprimez pas les chemins pointant vers autre chose que l'ancienne installation Sentinel, faute de quoi votre système risque de ne pas fonctionner correctement.

7 Supprimez tous les raccourcis Sentinel du Bureau.

8 Supprimez le dossier de raccourcis Démarrer > Tous les programmes > Sentinel.

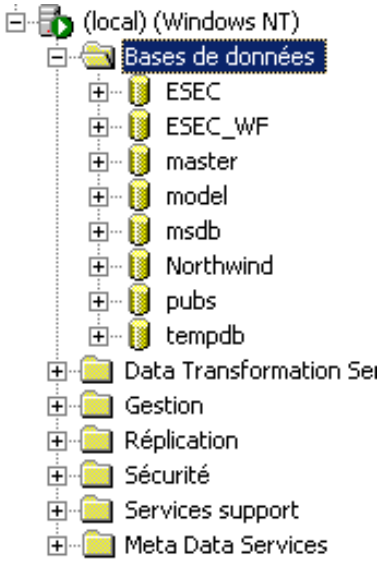
9 Redémarrez le système d'exploitation.

Pour nettoyer manuellement la base de données Sentinel Microsoft SQL Server sous Windows :

Remarque : assurez-vous qu'aucune autre application n'utilise la base de données avant de la supprimer.

1 Ouvrez Microsoft SQL Server Management Studio et connectez-vous à l'instance SQL Server sur laquelle la base de données Sentinel est installée.

2 Agrandissez l'arborescence Base de données et localisez votre base de données Sentinel.



3 Vous devriez trouver une base de données relative aux données Sentinel (généralement appelée ESEC) et une autre relative aux processus de travail (généralement appelée ESEC_WF). Cliquez avec le bouton droit sur chacune et sélectionnez Supprimer.

4 À l'invite, sélectionnez Oui pour supprimer la base de données.

Questionnaire de préinstallation

A

Questions de préinstallation

1 Dans quel but souhaitez-vous utiliser Novell Sentinel ?

1a Conformité

1b Gestion des événements de sécurité (SEM)

1c Autre_____

2 Quel matériel est prévu pour l'installation de Sentinel ? Satisfait-il aux conditions matérielles spécifiées dans le Guide d'installation de Sentinel ?

3 Avez-vous vérifié si votre configuration répond aux exigences Sentinel logicielles et matérielles décrites dans le Guide d'installation de Sentinel ?

- Niveaux de correctif du système d'exploitation
- Correctifs de service
- Hot Fix, etc.

4 Votre machine DAS présente-t-elle la configuration matérielle et logicielle requise ?

5 Quelle est l'architecture réseau pour les périphériques sources concernant le segment de sécurité dans lequel le matériel Sentinel et Collector doit se situer ?

Remarque : ceci est important afin de comprendre la hiérarchie de la collecte de données par le collecteur et d'identifier les pare-feux pouvant être franchis pour permettre la communication de Collector vers Sentinel ou de Sentinel ou Crystal Server vers la base de données.

Entrez ci-dessous des informations (texte et/ou dessin) ou des liens vers ces dernières.

6 Quels rapports le système doit-il générer ? Cette information est importante pour garantir que les collecteurs recueillent les données appropriées à transmettre à la base de données Sentinel.

6a _____

6b _____

6c _____

6d _____

6e _____

6f _____

7 À partir de quels périphériques sources voulez-vous collecter des données (IDS, HIDS, routeurs, pare-feu, etc.) ? Spécifiez les taux d'événements (EPS – événements par seconde), les versions, les méthodes de connexion, les plates-formes et les correctifs.

Périphérique (fabricant/ modèle)	Taux d'événements (EPS)	Version	Méthode de connexion	Plate-forme	Correctifs

Pouvez-vous fournir des exemples de données de ce que les collecteurs Sentinel doivent collecter et analyser ? Sentinel peut être configuré pour donner les résultats souhaités en fonction des informations spécifiées ici.

8 Quels sont les modèles/normes de sécurité en vigueur sur votre site ?

- Que pensez-vous des comptes locaux par rapport à l'authentification de domaine ?
  - Sous Windows avec l'authentification de domaine, des paramètres de compte de domaine adéquats doivent être créés pour permettre l'installation de Sentinel.
  - Pour une installation sous Solaris, ce n'est pas le cas. Toutefois, Sentinel ne prend pas en charge NIS.

9 Pendant combien de jours les données doivent-elles être conservées ?

10 Selon le délai de conservation des données et le taux d'événements, quelle taille de disque allez-vous utiliser ? Pour évaluer la taille, prévoyez 500 à 800 octets par événement.

Fiche d'installation de Sentinel sous Linux avec Oracle

B

Cette liste de contrôle est valable pour les installations distribuées comptant jusqu'à trois instances Collector Manager et Correlation Engine.

Reportez-vous au Guide d'installation pour prendre connaissance des exigences matérielles et logicielles ainsi que de la procédure d'installation.

	Variable de configuration			
1.	Version Sentinel :		Date du jour :	
2.	Valeurs Kernel UNIX pour Oracle. Ci-dessous valeurs min. Dans SLES et RHEL, vous pouvez définir des paramètres dans « etc/sysctl.conf ».			
	◆ shmmax		☐ : Oui | ☐ : Non	valeur si sup. :
	◆ shmmin		☐ : Oui | ☐ : Non	valeur si sup. :
	◆ shmseg		☐ : Oui | ☐ : Non	valeur si sup. :
	◆ shmmni		☐ : Oui | ☐ : Non	valeur si sup. :
	◆ semmns		☐ : Oui | ☐ : Non	valeur si sup. :
	◆ semmni		☐ : Oui | ☐ : Non	valeur si sup. :
	◆ semmsl		☐ : Oui | ☐ : Non	valeur si sup. :
	◆ shmopm		☐ : Oui | ☐ : Non	valeur si sup. :
	◆ shmvmx		☐ : Oui | ☐ : Non	valeur si sup. :
3.	Système de base de données			
	◆ SE correct pour composants Sentinel	☐ : Oui | ☐ : Non	◆ correctif adéquat	☐ : Oui | ☐ : Non
	◆ SE correct pour BD	☐ : Oui | ☐ : Non	◆ correctif adéquat	☐ : Oui | ☐ : Non
	◆ Version		◆ Niveau de correctif	
	◆ BD Oracle correcte avec partitionnement	☐ : Oui | ☐ : Non	◆ correctif adéquat	☐ : Oui | ☐ : Non
	◆ Version		◆ niveau de correctif	
	◆ ensemble de variables d'environnement correct pour utilisateur du SE Oracle	☐ : Oui | ☐ : Non		

	Variable de configuration			
	◆ Fichier Init.ora configuré	☐ : Oui | ☐ : Non		
4.	Machine DAS			
	◆ SE correct pour composants Sentinel	: Oui | : Non	◆ correctif adéquat	: Oui | : Non
	◆ numéro de série			
	◆ clé de licence			
5.	Installation DAS			
	◆ nom d'hôte BD ou IP			
	◆ nom base de données			Valeur par défaut : ESEC
	◆ port de base de données			Valeur par défaut : 1521
	◆ emplacement fichier JDBC			
6.	Instance base de données (SID)			
7.	Nom base de données			
8.	Composants Sentinel :			
	◆ base de données Sentinel (IP ou DNS)			SE: correctif :
	◆ journal d'installation BD			
	◆ mémoire (RAM) Oracle			
	◆ nom d'instance			
	◆ port d'écoute		Valeur par défaut : 1521	
	◆ mot de passe SYS			
	◆ mot de passe SYSTÈME			
	◆ Fichier .keystore importé lors de l'installation :			
	◆ Corrélation	☐ : Oui | ☐ : Non		
	◆ DAS	☐ : Oui | ☐ : Non		
	◆ Gestionnaire des collecteurs	☐ : Oui | ☐ : Non		
	◆ Serveur de communication	☐ : Oui | ☐ : Non		
	◆ serveur de communication (iSCALE) (IP ou DNS)	◆ IP/DNS :		SE: correctif :
	◆ DAS/Advisor (IP ou DNS) (l'Advisor est facultatif)	◆		SE: correctif :

Variable de configuration	
◆ DAS RAM	◆
◆ moteur de corrélation (IP et SE)	
	◆ IP: SE:
	◆ IP: SE:
	◆ IP: SE:
◆ générateur de collecteurs (IP ou DNS) (une seule installation recommandée)	
◆ Gestionnaire des collecteurs	Entrez les informations pour chaque gestionnaire des collecteurs que vous déployez.
◆ Gestionnaire des collecteurs	☐ : Oui | ☐ : Non
◆ IP: ◆ SE:	◆ Port du bus de message : ◆ Port proxy de Sentinel Control Center : ◆ Nom d'hôte du serveur de communication : ◆ Port d'authentification du certificat de gestionnaire des collecteurs :

9. Advisor (facultatif)

◆ Installé sur les mêmes machines que DAS ?	☐ : Oui | ☐ : Non
◆ Téléchargement d'Advisor :	☐ : Indépendant| ☐ : Directement depuis Internet
◆ emplacement fichier alimentation données	
◆ Advisor adresse expéditeur	
◆ Advisor adresse destinataire	
◆ Nom d'utilisateur	n/u :

10. 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	

Variable de configuration		
◆ journal des répétitions du répertoire du membre A		
11. Taille de la base de données :		
◆ standard (20 Go)		
◆ grande (400 Go)		
◆ personnalisée (taille)		
12. Serveur SMTP		
(DNS ou IP)		
13. Mots de passe utilisateur		
◆ esecadm	MP :	
◆ répertoire privé		Valeur par défaut : /export/home
◆ esecapp	MP :	
◆ esecdba	MP :	
◆ esecrpt	MP :	
Installation de Crystal		
1. Version Crystal:		
◆ SE		
◆ Base de donnée Crystal		
◆ Crystal Server (IP ou DNS)		
◆ Serveur Web (IP ou DNS)		
2. Crystal Reports		
◆ Publication de tous les rapports	☐ : Oui | ☐ : Non	
◆ Rapports configurés sur SCC	☐ : Oui | ☐ : Non	

Fiche d'installation de Sentinel sous Solaris avec Oracle

C

Cette liste de contrôle est valable pour les installations distribuées comptant jusqu'à trois instances Collector Manager et Correlation Engine.

Pour plus d'informations, reportez-vous aux exigences matérielles et logicielles ainsi qu'à la procédure d'installation dans le Guide d'installation.

	Variable de configuration			
1.	Version Sentinel :			Date du jour :
2.	Valeurs Kernel UNIX pour Oracle. Ci-dessous valeurs min. Dans SLES et RHEL, vous pouvez définir des paramètres dans « etc/sysctl.conf ».			
	shmmax		☐ : Oui | ☐ : Non	valeur si sup. :
	shmmin		☐ : Oui | ☐ : Non	valeur si sup. :
	shmseg		☐ : Oui | ☐ : Non	valeur si sup. :
	shmmni		☐ : Oui | ☐ : Non	valeur si sup. :
	semmns		☐ : Oui | ☐ : Non	valeur si sup. :
	semmni		☐ : Oui | ☐ : Non	valeur si sup. :
	semmsl		☐ : Oui | ☐ : Non	valeur si sup. :
	shmopm		☐ : Oui | ☐ : Non	valeur si sup. :
	shmvmx		☐ : Oui | ☐ : Non	valeur si sup. :
3.	Système de base de données			
	SE correct pour composants Sentinel	☐ : Oui | ☐ : Non	correctif adéquat	☐ : Oui | ☐ : Non
	◆ 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 - note Oracle : 148673.1	☐ : Oui | ☐ : Non		
	◆ ensemble de variables d'environnement correct pour utilisateur du SE Oracle	☐ : Oui | ☐ : Non		

	Variable de configuration			
	◆ Fichier Init.ora configuré	☐ : Oui | ☐ : Non		
	◆ SE correct pour composants Sentinel	☐ : Oui | ☐ : Non	◆ correctif adéquat	☐ : Oui | ☐ : Non
4.	Machine DAS			
	◆ numéro de série			
	◆ clé de licence			
5.	Installation DAS			
	◆ nom d'hôte BD ou IP			
	◆ nom base de données			Valeur par défaut : ESEC
	◆ port de base de données			Valeur par défaut : 1521
	◆ emplacement fichier JDBC			
6.	Instance base de données (SID)			
7.	Nom base de données			
8.	Composants Sentinel :			
	◆ base de données Sentinel (IP ou DNS)			SE: correctif :
	◆ journal d'installation BD			
	◆ mémoire (RAM) Oracle			
	◆ nom d'instance			
	◆ port d'écoute		Valeur par défaut : 1521	
	◆ mot de passe SYS			
	◆ mot de passe SYSTÈME			
	◆ Fichier .keystore importé lors de l'installation :			
	◆ Corrélation	☐ : Oui | ☐ : Non		
	◆ DAS	☐ : Oui | ☐ : Non		
	◆ Gestionnaire des collecteurs	☐ : Oui | ☐ : Non		
	◆ Gestionnaire des collecteurs			
	◆ Installation de Collector Manager :	☐ : Oui | ☐ : Non	Bus de message direct | proxy	

Variable de configuration			
◆ IP: ◆ SE:	◆ Port du bus de message : ◆ Port proxy de Sentinel Control Center : ◆ Nom d'hôte du serveur de communication : ◆ Port d'authentification du certificat de gestionnaire des collecteurs :		
◆ Serveur de communication	☐ : Oui | ☐ : Non		
◆ serveur de communication (iSCALE) (IP ou DNS)	☐ : Oui | ☐ : Non		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)			
◆ MySQL pour Crystal Server	Version MySQL : Correctif MySQL : mot de passe administrateur système ou titulaire du mot de passe :		
◆ IP:	n/u :	MP :	SE:
◆ générateur de collecteurs (IP ou DNS) (une seule installation recommandée)			
◆ Gestionnaire des collecteurs			
◆ Installation de Collector Manager à l'aide de :	☐ : Oui | ☐ : Non	☐ : Proxy | ☐ : Bus de message direct	
◆ IP:	MP :		SE:
◆ IP:	MP :		SE:
◆ IP:	MP :		SE:

9. Advisor (facultatif)

Installé sur les mêmes machines que DAS ?	☐ : Oui | ☐ : Non	
◆ Téléchargement d'Advisor :	☐ : Autonome	☐ : Directement depuis Internet

Variable de configuration		
◆ emplacement fichier alimentation données		
◆ Advisor adresse expéditeur		
◆ Advisor adresse destinataire		
◆ nom d'utilisateur et mot de passe	n/u :	
10. 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		
11. Taille de la base de données :		
◆ standard (20 Go)		
◆ grande (400 Go)		
◆ personnalisée (taille)		
12. Serveur SMTP		
(DNS ou IP)		
13. Mots de passe utilisateur		
◆ esecadm	MP :	
◆ répertoire privé		Valeur par défaut : /export/home
◆ esecapp	MP :	
◆ esecdba	MP :	
◆ esecrpt	MP :	
Installation de Crystal		
1. ◆ Version Crystal:		
◆ SE		

	Variable de configuration	
	◆ Base de donnée Crystal	
	◆ Crystal Server (IP ou DNS)	
	◆ Serveur Web (IP ou DNS)	
2.	Crystal Reports	
	◆ Publication de tous les rapports	☐ : Oui | ☐ : Non
	◆ Rapports configurés sur SCC	☐ : Oui | ☐ : Non

Fiche d'installation de Sentinel sous Windows avec Microsoft SQL Server

D

Cette liste de contrôle est valable pour les installations distribuées comptant jusqu'à trois instances Collector Manager et Correlation Engine.

Pour plus d'informations, reportez-vous aux exigences matérielles et logicielles ainsi qu'à la procédure d'installation dans le Guide d'installation.

	Variable de configuration			
1.	Version Sentinel :			Date du jour :
	Système de base de données			
	◆ SE correct pour BD	☐ : Oui | ☐ : Non	◆ correctif adéquat	☐ : Oui | ☐ : Non
	◆ BD de SQL correcte	☐ : Oui | ☐ : Non	◆ correctif adéquat	☐ : Oui | ☐ : Non
	◆ Version		◆ niveau de correctif	
	◆			◆
2.	Pour l'installation DAS sous un compte de domaine Windows, assigner « se loguer comme service »	☐ : Oui | ☐ : Non		
3.	Machine DAS			
	◆ 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			Valeur par défaut : ESEC
6.	Port :			Par défaut : 1433
7.	Mode d'authentification	☐ : Mixte		
		☐ : Non-mixte		
8.	mot de passe administrateur de SQL Server ou titulaire du mot de passe :	MP :		
9.	Composants Sentinel :			

Variable de configuration		
◆ base de données Sentinel (IP ou DNS)		SE: correctif :
◆ Fichier .keystore importé lors de l'installation :		
◆ Corrélation	☐ : Oui | ☐ : Non	
◆ DAS	☐ : Oui | ☐ : Non	
◆ Service Collector Manager	☐ : Oui | ☐ : Non	
◆ Serveur de communication	☐ : Oui | ☐ : Non	
◆ serveur de communication (iSCALE) (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 :
◆ Microsoft SQL Server pour Crystal Server	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)		
◆ Gestionnaire des collecteurs	☐ : Oui | ☐ : Non ☐ Proxy | ☐ Bus de message direct	
◆ IP: ◆ SE:	◆ Port du bus de message : ◆ Port proxy de Sentinel Control Center : ◆ Nom d'hôte du serveur de communication : ◆ Port d'authentification du certificat de gestionnaire des collecteurs :	

	Variable de configuration		
10.	Advisor (facultatif)		
	Installé sur les mêmes machines que DAS ?	☐ : Oui | ☐ : Non	
	◆ Téléchargement d'Advisor :	☐ : Indépendant| ☐ : Directement depuis Internet	
	◆ emplacement fichier alimentation données		
	◆ Advisor adresse expéditeur		
	◆ Advisor adresse destinataire		
	◆ nom d'utilisateur et mot de passe	n/u :	
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 :

	Variable de configuration			
	◆ administrateur Sentinel (login)	n/u :		
	◆ utilisateur de rapports Sentinel (login)	n/u :		
	Installation de Crystal			
1.	Version Crystal:			
	SE			
	DB			
	Crystal Server (IP ou DNS)			
	Microsoft SQL (facultatif mais recommandé)	Version Microsoft SQL : Correctif Microsoft SQL : mot de passe admin.système ou titulaire ou mot de passe :		
	IP:	n/u :	MP :	SE:
2.	Crystal Reports			
	Type de rapports	☐ : SQL	☐ : Oracle	
	◆ Publication de tous les rapports	☐ : Oui | ☐ : Non		
	◆ Rapports configurés sur SCC	☐ : Oui | ☐ : Non		