Guide d'installation

Novell®
Sentinel 6.1 Rapid Deployment

SP2

Avril 2011

www.novell.com

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 produits livrables. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes noires 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 autorisations d'exportation nécessaires.

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

Documentation en ligne : pour accéder à la documentation en ligne la plus récente de ce produit et des autres produits Novell ou pour obtenir des mises à jour, reportez-vous au site 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.

Table des matières

À propos de ce Guide

Ce Guide présente Novell Sentinel 6.1 Rapid Deployment Service Pack 2 et décrit les procédures d'installation.

Public

Cette documentation est destinée aux professionnels de la sécurité des informations.

Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce Guide et les autres documentations fournies avec ce produit. Utilisez les commentaires des utilisateurs situés au bas de chaque page de la documentation en ligne, puis saisissez vos commentaires à cet endroit.

Documentation complémentaire

La documentation technique de Sentinel comporte les volumes suivants :

- *Guide d'installation de Novell Sentinel Rapid Deployment* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html)
- *Guide de l'utilisateur de Novell Sentinel Rapid Deployment* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html)
- *Guide de référence de Novell Sentinel Rapid Deployment* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/bookinfo.html)
- *Guide d'installation de Novell Sentinel* (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/)
- *Guide de l'utilisateur de Novell Sentinel* (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/)
- *Guide de référence de Novell Sentinel* (http://www.novell.com/documentation/sentinel61/s61_reference/?page=/documentation/sentinel61/s61_reference/data/)

- *Sentinel SDK* (http://www.novell.com/developer/develop_to_sentinel.html)

  Le site Web Sentinel SDK décrit le développement des collecteurs (propriétaires ou JavaScript) et les opérations de corrélation JavaScript.

Contacter Novell

- *Site Web de Novell* (http://www.novell.com)
- *Support technique de Novell* (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- *Apprentissage Novell* (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- *Site de téléchargement des correctifs* (http://download.novell.com/index.jsp)
- *Support Novell 24 heures sur 24, 7 jours sur 7* (http://www.novell.com/company/contact.html)
- *Sentinel TIDS* (http://support.novell.com/products/sentinel)
- Forums de support de la communauté Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Site Web de Sentinel Plug-in (http://support.novell.com/products/sentinel/secure/sentinelplugins.html)
- Liste des e-mails de notification : connectez-vous au site Web de Sentinel Plug-in.

Présentation du produit

1

Sentinel 6.1 Rapid Deployment est une version simplifiée de Novell Sentinel qui tire parti des composants Open Source PostgreSQL, ActiveMQ et JasperReports.

Les sections suivantes vous aident à comprendre et à installer les principaux composants du système Sentinel 6.1 Rapid Deployment. Ce *Guide d'installation de Sentinel Rapid Deployment* fournit des informations détaillées sur les procédures d'installation et de configuration. Le *Guide de l'utilisateur de Sentinel Rapid Deployment* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) contient une description détaillée de l'architecture et des procédures d'administration et d'utilisation du produit.

1.1 Présentation de Sentinel 6.1 Rapid Deployment

En tant que solution de gestion des événements et des informations de sécurité, Sentinel reçoit des données de nombreuses sources réparties dans l'entreprise, les normalise, 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 collecte de journaux pour garantir l'efficacité des contrôles informatiques tant en matière de détection des menaces que de satisfaction aux exigences d'audit. Sentinel remplace ces processus manuels laborieux par une surveillance automatisée et permanente des événements de sécurité et de conformité et des contrôles informatiques.

Par ailleurs, il collecte et met en corrélation les informations, relatives ou non à la sécurité, à partir de l'infrastructure réseau d'une organisation, d'applications, de périphériques et de systèmes tiers. Sentinel présente les données ainsi collectées dans une interface graphique utilisateur, identifie les problèmes de sécurité ou de conformité et assure le suivi des opérations de traitement afin de rationaliser les processus sources d'erreurs et de mettre en place un programme de gestion rigoureux et 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.

Les Solution Packs facilitent la distribution et l'importation des règles de corrélation, listes dynamiques, assignations, rapports Sentinel et processus de travail iTRAC au niveau des contrôles. Ces contrôles permettent de répondre aux exigences réglementaires spécifiques, telles que la norme

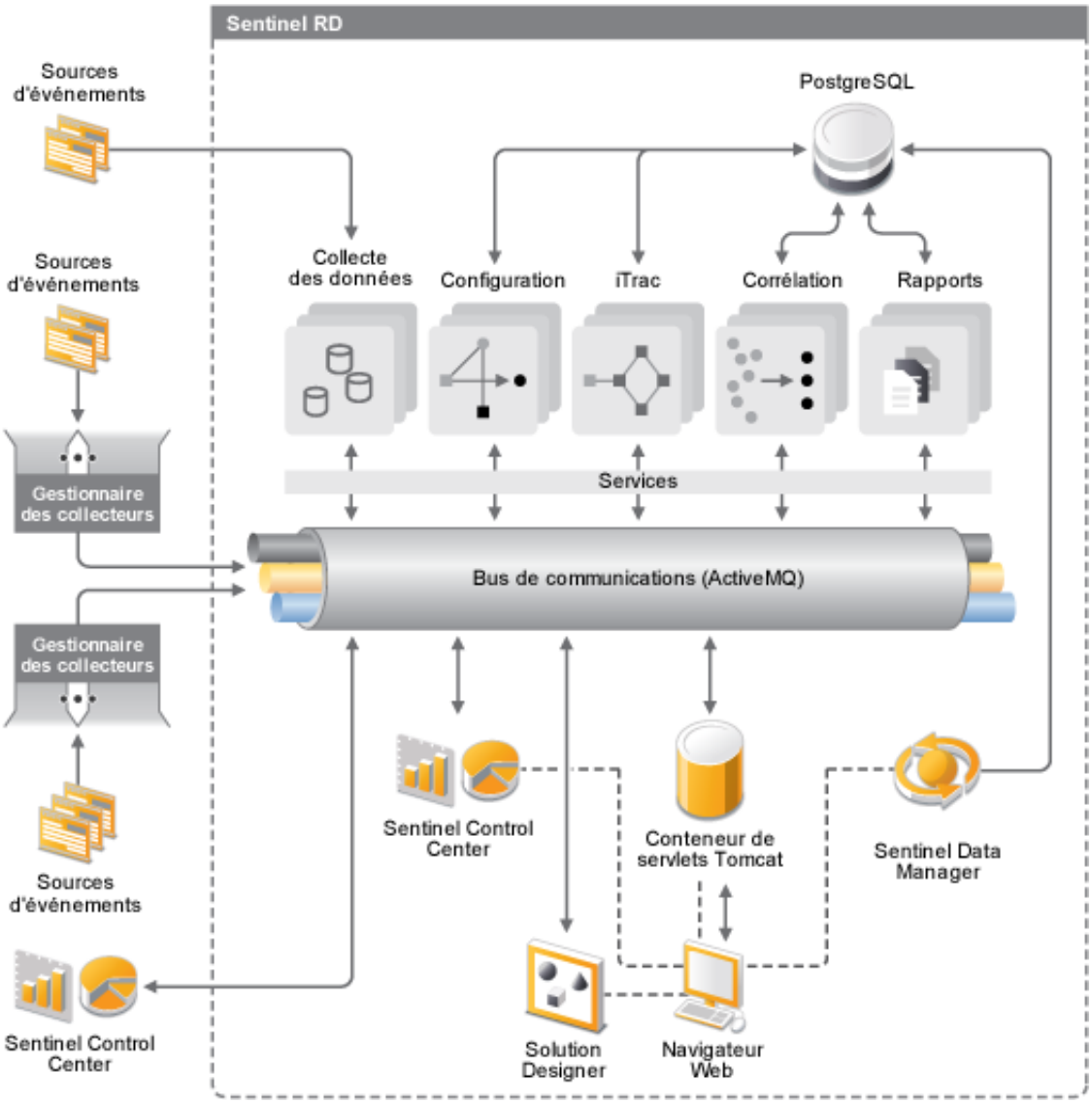
PCI-DSS (Payment Card Industry Data Security Standard, norme de sécurité informatique des données de l'industrie des cartes de paiement). Ils peuvent également être liés à une source de données spécifique, telle que les événements d'authentification des utilisateurs d'une base de données.

Avec Sentinel Rapid Deployment, vous bénéficiez des avantages suivants :

- Une gestion en temps réel et automatisée ainsi qu'une surveillance de la conformité intégrées pour tous les systèmes et réseaux.
- Une structure qui permet aux stratégies commerciales de l'entreprise de gérer les actions et les stratégies informatiques.
- Des fonctions de création de rapports et de documentation automatiques portant sur la sécurité, les systèmes et les accès dans l'entreprise.
- Une gestion des incidents et une remédiation intégrées.
- La capacité de démontrer et de surveiller votre conformité avec les stratégies internes et les législations gouvernementales, notamment Sarbanes-Oxley, HIPAA, GLBA et FISMA. Le contenu requis pour mettre en œuvre ces contrôles est distribué et implémenté à l'aide des Solution Packs.

Voici un aperçu de l'architecture conceptuelle de Sentinel Rapid Deployment qui illustre les différents composants de la gestion de la sécurité et de la conformité.

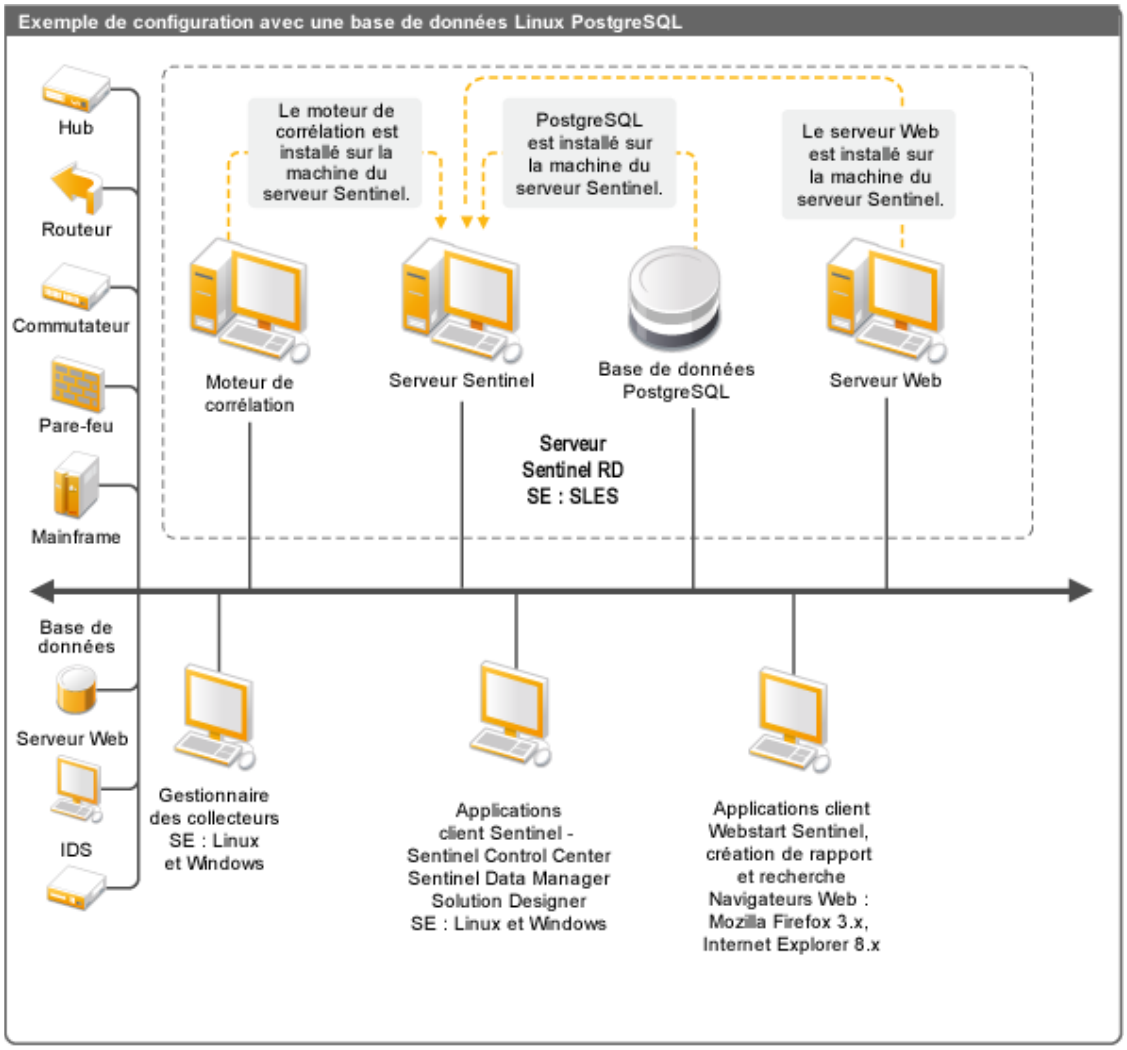
Figure 1-1 *Architecture conceptuelle de Sentinel*



1.2 Configuration de Sentinel 6.1 Rapid Deployment

Le schéma ci-après illustre la configuration de Sentinel 6.1 Rapid Deployment.

Figure 1-2 *Configuration de Sentinel 6.1 Rapid Deployment*



1.3 Interfaces utilisateur de Sentinel Rapid Deployment

Sentinel comprend les interfaces utilisateur conviviales suivantes :

- Interface Web de Sentinel 6.1 Rapid Deployment
- Sentinel Control Center
- Gestionnaire de données Sentinel
- Sentinel Solution Designer
- Sentinel Plug-in SDK

1.3.1 Interface Web de Sentinel 6.1 Rapid Deployment

L'interface Web de Novell Sentinel 6.1 Rapid Deployment permet de gérer des rapports et de démarrer Sentinel Control Center (SCC), Sentinel Data Manager et Solution Designer. Vous pouvez également télécharger le programme d'installation du gestionnaire des collecteurs et des clients à partir de la page *Applications* de l'interface Web de Sentinel 6.1 Rapid Deployment.

Pour plus d'informations, reportez-vous à la section « Gestion de Sentinel Rapid Deployment via l'interface Web » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.3.2 Sentinel Control Center

Sentinel Control Center fournit un tableau de bord intégré de gestion de la sécurité qui permet aux analystes d'identifier rapidement les nouvelles tendances ou menaces, de manipuler l'information graphique et d'interagir en temps réel avec ces données et de réagir en cas d'incidents.

Vous pouvez démarrer Sentinel Control Center en tant que programme client ou à l'aide de Java Webstart.

Principales fonctionnalités de Sentinel Control Center :

- **Vues actives (Active Views) :** diagnostics et visualisation en temps réel
- **Analyse:** exécution et enregistrement des requêtes hors ligne
- **Incidents :** création et gestion des incidents
- **Corrélation :** définition et gestion des règles de corrélation
- **iTRAC :** gestion de la documentation, de l'application et du suivi des processus de résolution d'incidents
- **Création de rapports :** rapports et métriques historiques
- **Gestion de source d'événements :** déploiement et surveillance des collecteurs
- **Solution Manager :** installation, mise en œuvre et test du contenu des Solution Packs

Pour plus d'informations, reportez-vous à la section « Sentinel Control Center » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.3.3 Gestionnaire de données Sentinel

Le gestionnaire de données Sentinel permet de gérer la base de données Sentinel. Vous pouvez exécuter les tâches suivantes dans le gestionnaire de données Sentinel :

- Surveiller l'espace utilisé par la base de données
- Afficher et gérer les partitions de base de données
- Gérer les archives de base de données
- Réimporter les données archivées dans la base de données

Pour plus d'informations, reportez-vous à la section « Gestionnaire de données Sentinel » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.3.4 Sentinel Solution Designer

Sentinel Solution Designer sert à créer et à modifier des Solution Packs, c'est-à-dire des ensembles de contenu Sentinel (règles de corrélation, actions, processus de travail iTRAC, rapports, etc.).

Le contenu Sentinel est la fonctionnalité étendue du système Sentinel. Ce contenu inclut les opérations Sentinel, les intégrateurs et les plug-ins Sentinel tels que les collecteurs, les connecteurs et les Solution Packs qui peuvent eux-mêmes comporter plusieurs types de plug-ins. Ces composants modulaires permettent d'intégrer l'application à des systèmes tiers, d'installer une solution de sécurité complète basée sur le contrôle et de fournir un correctif automatisé pour les incidents détectés.

Pour plus d'informations, reportez-vous à la section « Solution Packs » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.3.5 Sentinel Plug-in SDK

Sentinel Plug-in SDK comprend des bibliothèques et du code développé par Novell Engineering, ainsi que le modèle et le code exemple que vous pouvez utiliser pour développer vos propres projets. Pour plus d'informations, reportez-vous à la section Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html).

1.4 Composants du serveur Sentinel

Sentinel est constitué des composants suivants :

1.4.1 Data Access Service

Sentinel Data Access Service est le principal composant utilisé pour communiquer avec la base de données Sentinel. Le composant DAS et d'autres composants serveur fonctionnent conjointement pour recevoir les événements envoyés par les gestionnaires des collecteurs, les stocker dans la base de données, filtrer les données, traiter les affichages Active Views, exécuter les requêtes de base de données et en analyser les résultats, ainsi que gérer les tâches administratives telles que l'authentification et les autorisations des utilisateurs. Pour plus d'informations, reportez-vous à la section « Data Access Service » du *Guide de référence de Sentinel Rapid Deployment.*

1.4.2 Bus de messages

Sentinel 6.1 Rapid Deployment utilise un courtier de messages Open Source intitulé Apache ActiveMQ. Le bus de messages peut déplacer, en une seule seconde, des milliers de paquets de messages entre les différents composants de Sentinel. L'architecture d'Apache ActiveMQ s'articule autour de l'intergiciel Java orienté message (JMOM - Java Message Oriented Middleware) qui prend en charge les appels synchrones entre les programmes clients et les applications serveur. Les files d'attente de messages constituent une zone de stockage temporaire lorsque le programme cible est occupé ou n'est pas connecté. Pour plus d'informations, reportez-vous à la section « Serveur de communication » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.4.3 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. Sentinel 6.1 Rapid Deployment prend en charge le système PostgreSQL. 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. Pour plus d'informations, reportez-vous à la section « Gestionnaire de données Sentinel » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.4.4 Gestionnaire des collecteurs Sentinel

Le gestionnaire des collecteurs Sentinel gère la collecte des données, surveille les messages d'état du système et filtre les événements selon les besoins. Il permet notamment de transformer des événements, de les rendre pertinents pour l'entreprise en utilisant la taxonomie, de leur appliquer un filtre global, de les acheminer et d'envoyer des messages d'état de santé au serveur Sentinel. Le gestionnaire des collecteurs Sentinel se connecte directement au bus de messages. Pour plus d'informations, reportez-vous à la section « Gestionnaire des collecteurs » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.4.5 Moteur de corrélation

Le moteur 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. Pour plus d'informations, reportez-vous à la section « Onglet de corrélation » du *Guide de l'utilisateur de Sentinel Rapid Deployment.*

1.4.6 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. Pour plus d'informations, reportez-vous à la section « Processus de travail iTRAC » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.4.7 Sentinel Advisor et Exploit Detection

Sentinel Advisor est un service facultatif par abonnement qui fournit des informations sur les attaques, les vulnérabilités et les traitements connus. Ces données, associées aux vulnérabilités connues et à la détection d'intrusion en temps réel ou aux informations de prévention issues de votre environnement, permettent une détection proactive des exploits et une action immédiate en cas d'attaque contre un système vulnérable.

Un instantané des données Advisor est installé par défaut avec Sentinel 6.1 Rapid Deployment. Vous devez disposer d'une licence Advisor pour vous abonner aux mises à jour régulières des données Advisor. Pour plus d'informations, reportez-vous à la section « Utilisation et maintenance d'Advisor » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.4.8 Serveur Web

Sentinel Rapid Deployment utilise Apache Tomcat en tant que serveur Web pour assurer la connexion à l'interface Web de Sentinel Rapid Deployment.

1.5 Plug-ins Sentinel

Sentinel prend en charge un large éventail de plug-ins qui permet de développer et d'améliorer le fonctionnement de votre système. Certains plug-ins sont préinstallés. Des plug-ins supplémentaires (et des mises à jour) peuvent être téléchargés sur le site Web de Sentinel 6.1 Plug-ins (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Le téléchargement de certains plug-ins, tels que l'intégrateur Remedy, le connecteur d'ordinateurs centraux IBM et le connecteur pour SAP XAL, nécessite une licence supplémentaire.

1.5.1 Collecteurs

Sentinel collecte les données de périphériques sources et fournit un flux d'événements plus riche en intégrant une taxonomie, une détection d'exploits et des informations pertinentes sur le plan professionnel au flux de données avant que les événements ne soient corrélés, analysés et envoyés à la base de données. Un flux d'événements plus riche signifie que les données sont reliées au contexte d'entreprise requis afin de permettre l'identification et le traitement des menaces et violations de stratégie internes ou externes.

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

◆ systèmes de détection d'intrusion (hôte)	◆ système de détection des virus
◆ systèmes de détection d'intrusion (réseau)	◆ serveurs Web
◆ pare-feux	◆ bases de données
◆ systèmes d'exploitation	◆ gros système
◆ surveillance de stratégie	◆ systèmes d'évaluation des vulnérabilités
◆ authentification	◆ services d'annuaire
◆ routeurs et commutateurs	◆ systèmes de gestion réseau
◆ réseaux VPN	◆ systèmes propriétaires

Vous pouvez écrire et exécuter les collecteurs JavaScript à l'aide d'outils de développement JavaScript standard et du Collector SDK (Software Development Kit).

1.5.2 Connecteurs et intégrateurs

Les connecteurs permettent de lier le gestionnaire des collecteurs à des sources d'événements à l'aide de protocoles standard tels que JDBC et Syslog. Les événements sont transmis du connecteur au collecteur à des fins d'analyse.

Les intégrateurs permettent d'appliquer des opérations de traitement aux systèmes externes à Sentinel. Par exemple, une opération de corrélation peut utiliser l'intégrateur SOAP afin d'initier un processus de travail Novell Identity Manager.

L'intégrateur Remedy AR facultatif permet de créer un ticket Remedy à partir d'événements ou d'incidents Sentinel. Pour plus d'informations, reportez-vous à la section « Gestionnaire des opérations et intégrateur » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.5.3 Règles et opérations de corrélation

Les règles de corrélation identifient des modèles pertinents dans le flux d'événements. Le déclenchement d'une règle de corrélation entraîne l'exécution d'opérations de corrélation, telles que l'envoi d'un message électronique de notification, l'activation d'un processus de travail iTRAC ou l'exécution d'une opération à l'aide d'un intégrateur. Pour plus d'informations, reportez-vous à la section « Onglet de corrélation » du *Guide de l'utilisateur de Sentinel Rapid Deployment.*

1.5.4 Rapports

Vous pouvez exécuter un large éventail de tableaux de bord et de rapports opérationnels à partir de l'interface Web de Sentinel Rapid Deployment à l'aide de JasperReports. Les rapports sont généralement distribués par le biais de Solution Packs.

1.5.5 Processus de travail iTRAC

Les processus de travail iTRAC fournissent des processus cohérents et reproductibles pour gérer les incidents. Les modèles de processus de travail sont généralement distribués par le biais de Solution Packs. iTRAC est fourni avec un ensemble de modèles par défaut que vous pouvez modifier selon vos besoins. Pour plus d'informations, reportez-vous à la section « Processus de travail iTRAC » du *Guide de l'utilisateur de Sentinel Rapid Deployment.*

1.5.6 Solution Packs

Les Solution Packs sont des ensembles de contenu Sentinel, tels que des règles de corrélation, des opérations, des processus de travail iTRAC et des rapports. Novell inclut des Solution Packs qui répondent aux besoins spécifiques des entreprises, comme le Solution Pack PCI-DSS, qui répond aux besoins de conformité à la norme de sécurité informatique des données de l'industrie des cartes de paiement. De plus, Novell crée des Collector Packs dont le contenu s'applique à une source d'événements spécifique, telle que Windows Active Directory. Pour plus d'informations, reportez-vous à la section « Solution Packs » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

1.6 Prise en charge linguistique

Les composants Sentinel sont disponibles dans les langues suivantes :

- Tchèque
- Anglais
- Français
- Allemand
- Italien
- Japonais
- Néerlandais
- Polonais
- Portugais
- Chinois simplifié
- Espagnol
- Chinois traditionnel

Configuration système requise 2

Pour bénéficier de performances et d'une fiabilité optimales, vous devez installer les composants Sentinel Rapid Deployment sur des logiciels et du matériel approuvés, répertoriés dans cette section, qui ont été entièrement testés et certifiés.

2.1 Plates-formes prises en charge

Tableau 2-1 répertorie les combinaisons de logiciels et de systèmes d'exploitation certifiées ou prises en charge par Novell. Les combinaisons certifiées ont été testées à l'aide de la suite de tests complets Novell Engineering Test Suite. Les combinaisons prises en charge doivent être entièrement fonctionnelles.

2.1.1 Systèmes d'exploitation pris en charge

Novell prend en charge l'exécution de Sentinel Rapid Deployment sur les versions des systèmes d'exploitation ci-après. Novell prend également en charge l'exécution du logiciel sur les systèmes présentant des mises à jour mineures vers ces systèmes d'exploitation, comme l'installation de correctifs de sécurité ou de hotfixes. En revanche, l'exécution de Sentinel Rapid Deployment sur ces systèmes d'exploitation avec mises à jour majeures ou mineures n'est pas prise en charge tant que Novell n'a pas testé et certifié ces mises à jour.

Les composants du serveur Sentinel Rapid Deployment incluent le serveur de communication, le moteur de corrélation, le service DAS, le serveur Web et le service d'abonnement aux données Advisor.

Les programmes clients Sentinel comportent Sentinel Control Center, le gestionnaire de données Sentinel et Sentinel Solution Designer (SSD).

Le gestionnaire des collecteurs présente une configuration de plate-forme spécifique.

Tableau 2-1 *Systèmes d'exploitation pris en charge et certifiés*

Plates-formes	Composants du serveur	Programmes clients Sentinel	Gestionnaire des collecteurs
SUSE Linux Enterprise Server (SLES) 11 SP1 (64 bits)	Certifié	Certifié	Certifié
SUSE Linux Enterprise Server (SLES) 11 SP1 (32 bits)	Non pris en charge	Pris en charge	Pris en charge

Plates-formes	Composants du serveur	Programmes clients Sentinel	Gestionnaire des collecteurs
SUSE Linux Enterprise Server (SLES) 10 SP3 (64 bits)	Certifié	Pris en charge	Pris en charge
SUSE Linux Enterprise Server (SLES) 10 SP3 (32 bits)	Pris en charge	Pris en charge	Pris en charge
Windows Server 2008 R2 (64 bits)	Non pris en charge	Certifié	Certifié
Windows Server 2003 R2 (64 bits)	Non pris en charge	Pris en charge	Pris en charge
Windows Server 2003 R2 (32 bits)	Non pris en charge	Pris en charge	Pris en charge
Windows XP SP3 (32 bits)	Non pris en charge	Pris en charge	Non pris en charge
Windows Vista SP2 (32 bits)	Non pris en charge	Pris en charge	Non pris en charge
Windows 7	Non pris en charge	Certifié	Non pris en charge

Suivez les instructions ci-après pour bénéficier de performances, d'une stabilité et d'une fiabilité optimales :

- Pour SLES, le système d'exploitation du serveur Sentinel Rapid Deployment doit inclure au moins les composants Base Server et X Window de SLES.
- Pour le serveur Sentinel Rapid Deployment, utilisez le système de fichiers ext3. Pour plus d'informations sur les systèmes de fichiers, reportez-vous à la section Présentation des systèmes de fichiers sous Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) du *Guide d'administration de stockage*.

Remarque :

- Sentinel Rapid Deployment n'est pas pris en charge sur les installations Open Enterprise Server de SLES.
- La version de démonstration 32 bits du serveur Sentinel 6.1 Rapid Deployment est conçue pour des environnements de démonstration et de test limités en utilisant des systèmes matériels et d'exploitation 32 bits. Les clients ou partenaires disposant d'une prise en charge contractuelle de Sentinel 6.1 Rapid Deployment peuvent bénéficier d'une prise en charge limitée sur cette plate-forme par le support technique de Novell pour les problèmes pouvant se reproduire sur la plate-forme de production 64 bits. En raison des limitations inhérentes au matériel 32 bits, le support technique de Novell n'intervient pas en cas de problème de performances ou d'évolutivité de la version de démo 32 bits. Les versions de démo 32 bits ne sont pas prises en charge dans les environnements de production.

2.2 Configuration matérielle requise

Les composants du serveur Sentinel Rapid Deployment s'exécutent sur du matériel x86-64 (64 bits), avec quelques exceptions au niveau du système d'exploitation, comme indiqué dans la Section 2.1.1, « Systèmes d'exploitation pris en charge », page 19. Sentinel est certifié avec le matériel AMD Opteron et Intel Xeon. Les serveurs Itanium ne sont pas pris en charge.

Cette section inclut des recommandations matérielles générales destinées à vous aider à concevoir un système Sentinel. 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 (Events Per Second, événements par seconde).
- La taille moyenne des événements est de 1 ko.
- 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 quatre-vingt-dix 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 Tableau 2-2 page 22 et Tableau 2-3 page 22.
- Le serveur Sentinel dispose d'un espace disque par défaut de 5 Go pour la mise en cache temporaire des données d'événements dont l'insertion immédiate dans la base de données n'est pas possible.
- Le serveur Sentinel dispose également d'un espace disque par défaut de 5 Go pour les événements qui ne peuvent pas être insérés immédiatement dans les fichiers d'événements de regroupement.
- L'abonnement facultatif à Advisor requiert un espace disque supplémentaire de 1 Go sur le serveur.

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 ou un partenaire Novell Sentinel avant de finaliser l'architecture Sentinel. Les recommandations suivantes peuvent servir de lignes directrices.

En version SLES, la base de données est intégrée au serveur Sentinel Rapid Deployment et est installée sur la même machine que le serveur.

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

Tableau 2-2 *Configuration machine unique (jusqu'à 2 000 EPS)*

Composants	RAM	Espace	UC
Machine 1 : serveur Sentinel Rapid Deployment ◆ Base de données PostgreSQL intégrée (3 Go) ◆ Gestionnaire des collecteurs (1200 Mo) ◆ DAS_Core (1579 Mo) ◆ DAS_Binary (1404 Mo) ◆ Moteur de corrélation (1073 Mo) ◆ 4 collecteurs (général, Cisco, Snort et IBM, générant chacun 500 EPS) ◆ 10 règles de corrélation déployées ◆ 10 Active Views uniques ◆ 3 utilisateurs simultanés ◆ 2 assignations déployées	16 Go	Disque(s) dur(s) SAS (15 000 tpm), 1 To Pile RAID 10	Dell PowerEdge 2900,2 x Quad-Core Intel Xeon E5310 (1,6 GHz) avec carte réseau Gigabit Ethernet

Tableau 2-3 *Configuration trois machines (jusqu'à 5 000 EPS)*

Composants	RAM	Espace	UC
Machine 1 : serveur Sentinel Rapid Deployment ◆ Base de données PostgreSQL intégrée (3 Go) ◆ Gestionnaire des collecteurs (1200 Mo) ◆ DAS_Core (1579 Mo) ◆ DAS_Binary (1404 Mo) ◆ Moteur de corrélation (1073 Mo) ◆ 4 collecteurs (générant chacun 500 EPS, 1 500 EPS pour le gestionnaire des collecteurs à distance 1 et 1 500 EPS pour le gestionnaire des collecteurs à distance 2)	16 Go	Disque(s) dur(s) SAS (15 000 tpm), 1 To Pile RAID 10	Dell PowerEdge 2900,2 x Quad-Core Intel Xeon E5310 (1,6 GHz) avec carte réseau Gigabit Ethernet
Machine 2 : gestionnaire des collecteurs ◆ Gestionnaire des collecteurs/ Collecteurs ◆ 3 collecteurs (générant chacun 500 EPS)	4 Go	Disque dur 300 Go, SATA (3 Gbits/s)	Intel Core 2 Duo E6750 (2,66 GHz) avec carte réseau Gigabit Ethernet

Composants	RAM	Espace	UC
Machine 3 : gestionnaire des collecteurs ◆ Gestionnaire des collecteurs/ Collecteurs ◆ 3 collecteurs (générant chacun 500 EPS)	4 Go	Disque dur 300 Go, SATA (3 Gbits/s)	Intel Core 2 Duo E6750 (2,66 GHz) avec carte réseau Gigabit Ethernet

2.3 Navigateurs pris en charge

- Mozilla Firefox 3.*x*
- Internet Explorer 8.*x*

2.4 Environnement virtuel

Sentinel Rapid Deployment a été entièrement testé sur VMWare ESX Server et Novell prend intégralement en charge Sentinel Rapid Deployment dans ce type d'environnements. Pour obtenir des performances comparables aux résultats des tests effectués sur la machine physique sur ESX ou dans tout autre environnement virtuel, les caractéristiques de mémoire, de processeur, d'espace disque et d'E/S de l'environnement doivent être conformes aux recommandations de la machine physique.

Pour plus d'informations sur les recommandations de la machine physique pour un système SLES, reportez-vous à la Section 2.2, « Configuration matérielle requise », page 20.

2.5 Limites recommandées

Les limites mentionnées dans cette section sont des recommandations basées sur les tests de performances exécutés sur les sites Novell ou sur les sites de ses clients. Il n'y pas de limite matérielle. Les recommandations sont approximatives. Sur les systèmes hautement dynamiques, il est recommandé de créer des tampons et de prévoir de l'espace en vue de répondre aux besoins de croissance éventuels du système.

2.5.1 Limites du gestionnaire des collecteurs

Sauf indication contraire, le gestionnaire des collecteurs suppose l'exécution de 4 cœurs de processeur de 2,2 GHz chacun avec 4 Go de RAM sur SLES 11.

Tableau 2-4 *Performances du gestionnaire des collecteurs*

Attribut	Limite	Commentaires
Nombre maximum de gestionnaires de collecteurs	20	Cette limite suppose que chaque gestionnaire de collecteurs s'exécute suivant un faible taux d'EPS (inférieur à 100). La limite diminue à mesure que le nombre d'événements par seconde augmente.
Nombre maximum de connecteurs (utilisation optimale) sur un gestionnaire des collecteurs	1 par cœur de processeur, avec au moins 1 cœur de processeur réservé pour le système d'exploitation et tout autre traitement	Un connecteur utilisé de façon optimale s'exécute avec le taux d'EPS le plus élevé possible pour ce type de connecteur.
Nombre maximum de collecteurs (utilisation optimale) sur un gestionnaire des collecteurs	1 par cœur de processeur, avec au moins 1 cœur de processeur réservé pour le système d'exploitation et tout autre traitement	Un collecteur utilisé de façon optimale s'exécute avec le taux d'EPS le plus élevé possible pour ce type de collecteur.
Nombre maximum de périphériques sur un gestionnaire des collecteurs unique	2 000	La limite du serveur Sentinel Rapid Deployment est aussi de 2 000. Si 2 000 périphériques se trouvent sur un gestionnaire des collecteurs, le nombre maximum de périphériques pour l'ensemble du système Sentinel a été atteint.
Nombre maximum de périphériques sur le serveur Sentinel Rapid Deployment	2 000	La limite de périphériques sur le serveur Sentinel Rapid Deployment est de 2 000.

2.5.2 Limites des rapports

Tableau 2-5 *Performances des rapports*

Attribut	Limite	Commentaires
Nombre maximum de rapports enregistrés	200	Cette limite peut augmenter ou diminuer en fonction de la taille des rapports et de l'espace disque disponible sur le serveur qui n'est pas utilisé par le reste du système.
Nombre maximum de rapports pouvant être exécutés simultanément	3	La limite suppose que le serveur n'est pas déjà utilisé de façon optimale pour l'exécution d'une collecte de données ou d'autres tâches.

2.6 Résultats des tests

Sentinel Rapid Deployment permet de créer différentes configurations en fonction de votre environnement. Les informations de test de performance suivantes sont issues du test exécuté par Novell pour les configurations spécifiques répertoriées dans les tableaux ci-dessous.

Les recommandations matérielles pour une mise en œuvre Sentinel sont susceptibles de varier en fonction de chaque mise en œuvre. Nous vous conseillons donc de consulter les services Novell Consulting ou un partenaire Novell Sentinel avant de finaliser l'architecture Sentinel. Les informations de test suivantes peuvent servir de lignes directrices.

Linux Le test Linux a été exécuté pour le taux d'EPS le plus élevé avec un nombre différent de périphériques et le nombre maximum de périphériques pour un taux d'EPS spécifique. La configuration matérielle suivante a été utilisée :

- **Nombre de cœurs de processeur :** 4
- **Modèle de processeur :** Processeur Intel Xeon X5770 à 2,93 GHz
- **Mémoire vive :** 16 Go
- **Capacité du disque dur (type +RAID et nombre de disques RAID) :** 1,7 To (RAID 5, 6 disques)

Remarque : tous les tests ont été réalisés avec des sources d'événements basées sur Syslog. Les performances peuvent être différentes si d'autres connecteurs sont utilisés.

Le tableau suivant indique le taux maximum d'EPS qui peut être pris en charge avec un nombre spécifique de périphériques sur un système SLES :

Tableau 2-6 *Taux maximum d'EPS sur un système SLES*

Configuration système	Périphériques	Taux maximum d'EPS
4 gestionnaires de collecteurs (un local et trois distants) avec 10 collecteurs, générant chacun 500 EPS	25	5 000
4 gestionnaires de collecteurs (un local et trois distants) avec 10 collecteurs, générant chacun 500 EPS	100	5 000
4 gestionnaires de collecteurs (un local et trois distants) avec 10 collecteurs, générant chacun 500 EPS	1 000	5 000

Le tableau suivant indique le nombre maximum de périphériques pouvant être pris en charge avec un taux d'EPS spécifique sur un système SLES :

Tableau 2-7 *Nombre maximum de périphériques sur un système SLES*

Configuration système	EPS	Nombre maximum de périphériques
1 gestionnaire de collecteurs avec 1 collecteur, générant 500 EPS	500	2 000

Configuration système	EPS	Nombre maximum de périphériques
1 gestionnaire de collecteurs avec 2 collecteurs, générant chacun 500 EPS	1 000	2 000
1 gestionnaire de collecteurs avec 3 collecteurs, générant chacun 500 EPS	1 500	2 000

Remarque :

- Si vous souhaitez prendre en charge davantage d'événements par seconde ou de périphériques, installez d'autres gestionnaires de collecteurs.
- Le nombre maximum de périphériques n'est pas une limite rigide. Il s'agit plutôt de recommandations basées sur les tests de performances réalisés par Novell. Ces tests prennent en compte un taux moyen d'événements par seconde et par périphérique peu élevé (moins de 3 EPS). Des taux d'EPS plus élevés entraînent un nombre maximum inférieur de périphériques durables. Vous pouvez utiliser l'équation (nombre maximum de périphériques) x (moyenne d'EPS par périphérique) = taux d'événements maximum pour obtenir les limites approximatives de votre taux d'EPS moyen ou nombre de périphériques spécifique, pour autant que le nombre maximum de périphériques ne dépasse pas la limite indiquée ci-dessus.

Installation

3

Cette section fournit des informations sur l'installation des composants de Sentinel Rapid Deployment et des clients.

3.1 Présentation

Le paquetage d'installation de Sentinel fournit un programme d'installation simplifié pour machine serveur unique qui permet d'installer tous les éléments nécessaires à l'exécution de Sentinel Rapid Deployment. Le programme d'installation du serveur Sentinel Rapid Deployment installe les composants suivants :

3.1.1 Composants du serveur

Tableau 3-1 *Applications et composants du serveur Sentinel*

Composant	Description
	La base de données Sentinel stocke les données de configuration et d'événements.
Bus de messages	Un bus de messages JMS gère la communication entre les différents composants du système Sentinel.
Moteur de corrélation	Le moteur de corrélation analyse les événements en temps réel.
Advisor	Advisor met en corrélation en temps réel les attaques IDS détectées et les résultats de l'analyse de vulnérabilité afin d'indiquer immédiatement toute augmentation des risques pour une organisation.
Data Access Service	Comprend des composants de stockage, d'interrogation, d'affichage et de traitement des données.
Serveur Web	Prend en charge l'interface Web de Sentinel Rapid Deployment.

Composant	Description
Gestionnaire des collecteurs	Service de gestion des connexions à des sources d'événements, des analyses des données, des assignations, etc. Le gestionnaire des collecteurs peut être distribué à d'autres emplacements, d'autres machines et d'autres systèmes d'exploitation par l'intermédiaire du programme d'installation du gestionnaire des collecteurs disponible via l'interface Web de Sentinel Rapid Deployment. Par exemple, vous pouvez installer un gestionnaire des collecteurs supplémentaire sur une machine Windows pour collecter les événements Windows.
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.

3.1.2 Programmes clients

Les programmes clients (Sentinel Control Center, le gestionnaire de données Sentinel et Solution Designer) sont installés par défaut sur le serveur Sentinel Rapid Deployment. Vous pouvez lancer les programmes clients en utilisant l'une des méthodes suivantes :

- Via l'interface Web de Sentinel Rapid Deployment. Les systèmes clients doivent disposer de Java 1.6.0_20 ou version ultérieure et le chemin JRE doit être configuré de manière à lancer les programmes Sentinel via Webstart.

  Définissez la variable d'environnement `JAVA_HOME` en spécifiant l'emplacement du dossier `JRE 6`. Définissez le chemin d'exportation vers le dossier `bin` sous l'emplacement JRE 6.

- Via `<répertoire_installation>/bin` en tant qu'utilisateur disposant des fichiers d'installation de Sentinel Rapid Deployment. Par exemple :

  `./bin/<client_application>.sh`

Tableau 3-2 *Programmes clients Sentinel*

Composant	Description
Sentinel Control Center	Principale console destinée aux analystes de sécurité ou de conformité.
Gestionnaire de données Sentinel	Utilitaire de gestion de base de données.
Solution Designer	Application de création de Solution Packs.
Gestionnaire des collecteurs Sentinel	Service de gestion des connexions à des sources d'événements, des analyses des données, des assignations, etc. Un gestionnaire des collecteurs est installé sur le serveur Sentinel, mais d'autres gestionnaires peuvent être installés sur des machines distantes Windows ou Linux à l'aide d'un programme d'installation téléchargeable.

3.2 L'installation est basée sur SUSE Linux Enterprise Server

3.2.1 Conditions préalables

Vérifiez que les conditions préalables sont respectées avant d'installer Sentinel Rapid Deployment. Pour plus d'informations sur les conditions préalables (notamment la liste des plates-formes certifiées), reportez-vous au Chapitre 2, « Configuration système requise », page 19.

Important : les installations Sentinel Rapid Deployment qui utilisent le programme d'installation complet doivent toujours être effectuées sur un système « propre ». Si d'autres versions de Sentinel, comme Sentinel Classic ou Sentinel Log Manager, sont déjà installées sur l'une des machines, vous devez d'abord les désinstaller. Pour plus d'informations sur la désinstallation des versions antérieures de Sentinel, reportez-vous aux Guides d'installation appropriés :

- Pour désinstaller Sentinel Classic, reportez-vous au chapitre « Désinstallation de Sentinel » du Guide d'installation de Sentinel (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html).
- Pour désinstaller Sentinel Log Manager, reportez-vous au chapitre « Désinstallation de Sentinel Log Manager » du Guide d'installation de Sentinel Log Manager 1.1 (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html).

Serveur

- Vérifiez que chaque machine serveur satisfait à la configuration système minimale requise. Pour plus d'informations sur la configuration système requise, reportez-vous à la section Chapitre 2, « Configuration système requise », page 19.
- Configurez le système d'exploitation de façon à ce que la commande `hostname -f` renvoie un nom d'hôte valide.
- Installez et configurez un serveur SMTP pour pouvoir envoyer des notifications par message électronique à partir du système Sentinel.

Client

- Vérifiez que chaque machine cliente satisfait à la configuration système minimale requise. Pour plus d'informations sur ces conditions préalables, reportez-vous au Chapitre 2, « Configuration système requise », page 19.
- Créez un répertoire dont le nom ne comporte que des caractères ASCII (aucun caractère spécial) à partir duquel vous pourrez exécuter le programme d'installation.

- Lorsque vous installez le gestionnaire des collecteurs ou des programmes clients sur des machines Linux, veillez à ce qu'aucune restriction n'ait été définie au niveau du dossier `/tmp` de l'utilisateur Admin.
- Octroyez des privilèges avec pouvoir à l'utilisateur de domaine pour le gestionnaire des collecteurs sous Windows car les droits utilisateur normaux sont insuffisants pour l'installation du gestionnaire.
- Si vous installez le gestionnaire des collecteurs sur une machine 64 bits, assurez-vous que les bibliothèques 32 bits sont disponibles. Les bibliothèques 32 bits sont requises lors de l'exécution d'un collecteur écrit dans la langue du collecteur propriétaire (qui inclut la plupart des collecteurs écrits avant juin 2008), ainsi que lors de l'exécution de certains collecteurs (par exemple, un connecteur LEA). Les collecteurs JavaScript et les autres composants de Sentinel fonctionnent en mode 64 bits. Il est particulièrement important de vérifier que ces bibliothèques sont disponibles sur les plates-formes Linux, sur lesquelles elles ne sont peut-être pas incluses par défaut.

Advisor

Pour installer Advisor, vous devez acheter la fonctionnalité de détection d'exploits Sentinel et souscrire à l'abonnement aux données Advisor. Après avoir souscrit à l'abonnement, utilisez votre eLogin Novell pour télécharger et mettre à jour les données Advisor. Pour plus d'informations, reportez-vous au chapitre « Utilisation et maintenance d'Advisor » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

3.2.2 Installation de Sentinel Rapid Deployment

Le serveur Sentinel Rapid Deployment peut être installé de plusieurs manières :

- « Installation à script unique avec privilèges root » page 30
- « Installation non-root » page 33

Le script du programme d'installation de Sentinel Rapid Deployment propose les options suivantes au cours de l'installation :

- **-all :** Vous devez être l'utilisateur `root` pour utiliser cette option. Cette option crée un utilisateur (par défaut : `novell`), un groupe d'utilisateurs (par défaut : `novell`), puis installe le serveur Sentinel Rapid Deployment. Elle permet également d'exécuter automatiquement les services Sentinel Rapid Deployment au démarrage du système.
- **-install :** Cette option installe uniquement le serveur Sentinel Rapid Deployment.
- **-createuser :** Vous devez être l'utilisateur `root` pour utiliser cette option. Cette option crée uniquement l'utilisateur (par défaut : `novell`) et le groupe d'utilisateurs (par défaut : `novell`).
- **-createservice :** Vous devez être l'utilisateur `root` pour utiliser cette option. Cette option permet uniquement d'exécuter automatiquement les services Sentinel Rapid Deployment au démarrage du système.
- **-help :** Cette option affiche l'aide sur l'utilisation des options de script d'installation.

Installation à script unique avec privilèges root

1 `Loguez-vous en tant qu'utilisateur root.`

L'utilisateur qui exécute l'installation doit disposer d'un accès en écriture au répertoire temporaire à partir duquel les fichiers du programme d'installation seront téléchargés.

2 Téléchargez le programme d'installation `sentinel6_rd_linux_x86-64.tar.gz` sur le site de téléchargement Novell (http://download.novell.com/) dans un répertoire temporaire.

3 Extrayez le programme d'installation :

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

4 Accédez au répertoire à partir duquel vous avez extrait le programme d'installation :

```
cd sentinel6_rd_linux_x86-64
```

5 Exécutez le script `install.sh` avec l'option `-all` :

```
./install.sh -all
```

Le script d'installation vérifie d'abord si la mémoire et l'espace disque sont suffisants. Si moins de 1 Go de mémoire est disponible, le script stoppe automatiquement l'installation. Si la mémoire disponible est supérieure à 1 Go mais inférieure à 4 Go, le script affiche un message vous recommandant de libérer de la mémoire. Ce message vous demande également si vous souhaitez poursuivre l'installation. Entrez `y` si vous souhaitez poursuivre l'installation ou `n` dans le cas contraire.

6 Spécifiez le nom d'utilisateur ou appuyez sur Entrée pour sélectionner le nom d'utilisateur par défaut. Le nom d'utilisateur par défaut est `novell`.

Si le nom d'utilisateur spécifié existe déjà, le programme d'installation affiche un message indiquant que l'utilisateur existe, ainsi que le groupe d'utilisateurs. Passez à la Étape 8.

Si le nom d'utilisateur spécifié n'existe pas, le programme d'installation le crée. Passez à la Étape 7.

7 Spécifiez le nom du groupe ou appuyez sur Entrée pour sélectionner le nom du groupe par défaut. Le nom du groupe par défaut est `novell`.

Si le nom du groupe spécifié existe déjà, le programme d'installation poursuit l'installation. Dans le cas contraire, il crée le groupe et affiche un message indiquant que le nom d'utilisateur spécifié est créé sous le groupe spécifié.

L'utilisateur et le groupe spécifiés sont les propriétaires de l'installation et des processus d'exécution de Sentinel.

8 Spécifiez le chemin d'installation ou appuyez sur Entrée pour sélectionner le chemin par défaut. Le chemin d'accès par défaut est `/opt/novell`.

Le chemin d'installation que vous spécifiez ne doit pas comporter d'espace. Si un espace est inséré, le script d'installation vous invite à le supprimer.

9 Choisissez l'une des langues suivantes en saisissant le numéro correspondant:

Numéro de série	Langue
1	Tchèque
2	Anglais
3	Français
4	Allemand
5	Italien
6	Japonais
7	Néerlandais

Numéro de série	Langue
8	Polonais
9	Portugais
10	Chinois simplifié
11	Espagnol
12	Chinois traditionnel

L'accord de licence utilisateur final s'affiche dans la langue sélectionnée.

10 Après avoir lu l'accord de licence utilisateur final, entrez `1` si vous en acceptez les termes et souhaitez continuer l'installation. Entrez `2` pour stopper l'installation.

Le programme d'installation commence ensuite à extraire les fichiers et vous invite à renseigner la clé de licence.

11 Entrez `1` pour utiliser la clé de licence d'évaluation de 90 jours ou `2` pour utiliser la clé de licence valide.

Si vous entrez `2`, le programme d'installation vous invite à entrer la clé de licence Sentinel RD valide. Si la clé de licence que vous spécifiez n'est pas valide, le programme d'installation vous invite à la saisir de nouveau. Si elle n'est toujours pas valide, la clé de licence d'évaluation de 90 jours s'affiche automatiquement. Vous pouvez entrer la clé de licence valide ultérieurement.

Le script charge ensuite la licence d'évaluation ou la licence valide.

12 Indiquez un mot de passe pour l'utilisateur `dbauser` et confirmez-le en le saisissant de nouveau.

Les références `dbauser` sont utilisées pour la création de tables et de partitions dans la base de données PostgreSQL.

13 Indiquez un mot de passe pour l'utilisateur `admin` et confirmez-le en le saisissant de nouveau.

Lorsque vous spécifiez les mots de passe pour les utilisateurs `admin` et `dbauser`, n'utilisez pas de barre oblique inverse (\) ni d'apostrophe (‘) car ces caractères ne sont pas pris en charge par la base de données PostgreSQL.

Le script d'installation installe la base de données PostgreSQL, crée les tables et les partitions, puis installe le serveur Sentinel Rapid Deployment.

Une fois l'installation terminée, vous pouvez procéder comme suit :

- Démarrez l'interface Web de Sentinel Rapid Deployment en accédant au site `https://<ADRESSE_IP_SERVEUR>:8443/sentinel`. <*ADRESSE_IP_SERVEUR*> correspond à l'adresse IP de la machine sur laquelle le serveur Sentinel Rapid Deployment est installé.
- Démarrez Sentinel Control Center en exécutant le fichier `<répertoire_installation>/bin/control_center.sh` avec les références de l'utilisateur créé à l'Étape 6.

Installation non-root

Si la stratégie organisationnelle empêche l'exécution de l'ensemble du processus d'installation en tant que `root`, l'installation peut être réalisée en deux étapes. La première doit être effectuée avec un accès au niveau `root`, tandis que la deuxième s'opère en tant qu'administrateur Sentinel (créé au cours de la première étape).

1. Loguez-vous au serveur sur lequel vous souhaitez installer Sentinel Rapid Deployment.

   L'utilisateur qui exécute l'installation doit disposer d'un accès en écriture au répertoire temporaire à partir duquel les fichiers du programme d'installation seront téléchargés.

2. Téléchargez le programme d'installation `sentinel6_rd_linux_x86-64.tar.gz` sur le site de téléchargement Novell (http://download.novell.com/) dans un répertoire temporaire.

3. Extrayez le programme d'installation :

   ```
   tar zxvf sentinel6_rd_linux_x86-64.tar.gz
   ```

4. `Loguez-vous en tant qu'utilisateur root.`

5. Accédez au répertoire à partir duquel vous avez extrait le programme d'installation :

   ```
   cd sentinel6_rd_linux_x86-64
   ```

6. Exécutez le script `install.sh` avec l'option `-createuser` :

   ```
   ./install.sh -createuser
   ```

7. Spécifiez le nom d'utilisateur ou appuyez sur Entrée pour sélectionner le nom d'utilisateur par défaut. Le nom d'utilisateur par défaut est `novell`.

   Si le nom d'utilisateur spécifié existe déjà, le programme d'installation affiche un message indiquant que l'utilisateur existe, ainsi que le groupe d'utilisateurs. Passez à l'Étape 9.

   Si le nom d'utilisateur spécifié n'existe pas, le programme d'installation le crée. Passez à l'Étape 8.

8. Spécifiez le nom du groupe ou appuyez sur Entrée pour sélectionner le nom du groupe par défaut. Le nom du groupe par défaut est `novell`.

   Si le nom du groupe spécifié existe déjà, le programme d'installation poursuit l'installation. Dans le cas contraire, il crée le groupe et affiche un message indiquant que le nom d'utilisateur spécifié est créé sous le groupe spécifié.

   L'utilisateur et le groupe spécifiés sont les propriétaires de l'installation et des processus d'exécution de Sentinel.

9. Spécifiez le chemin d'installation ou appuyez sur Entrée pour sélectionner le chemin par défaut. Le chemin d'accès par défaut est `/opt/novell`.

   Le chemin d'installation que vous spécifiez ne doit pas comporter d'espace. Si un espace est inséré, le script d'installation vous invite à le supprimer.

10. Loguez-vous en tant qu'utilisateur non-root. Par exemple.

    ```
    su - novell
    ```

11. Exécutez le script d'installation avec l'option `-install` :

    ```
    ./install.sh -install
    ```

    Le script d'installation vérifie d'abord si la mémoire et l'espace disque sont suffisants. Si moins de 1 Go de mémoire est disponible, le script stoppe automatiquement l'installation. Si la mémoire disponible est supérieure à 1 Go mais inférieure à 4 Go, le script affiche un message

vous recommandant de libérer de la mémoire. Ce message vous demande également si vous souhaitez poursuivre l'installation. Entrez `y` si vous souhaitez poursuivre l'installation ou `n` dans le cas contraire.

12 Spécifiez le chemin d'installation ou appuyez sur Entrée pour sélectionner le chemin par défaut. Le chemin d'accès par défaut est `/opt/novell`.

Le chemin d'installation que vous spécifiez ne doit pas comporter d'espace. Si un espace est inséré, le script d'installation vous invite à le supprimer.

13 Choisissez l'une des langues suivantes en saisissant le numéro correspondant:

Numéro de série	Langue
1	Tchèque
2	Anglais
3	Français
4	Allemand
5	Italien
6	Japonais
7	Néerlandais
8	Polonais
9	Portugais
10	Chinois simplifié
11	Espagnol
12	Chinois traditionnel

L'accord de licence utilisateur final s'affiche dans la langue sélectionnée.

14 Après avoir lu l'accord de licence utilisateur final, entrez `1` si vous en acceptez les termes et souhaitez continuer l'installation. Entrez `2` pour stopper l'installation.

Le programme d'installation commence ensuite à extraire les fichiers et vous invite à renseigner la clé de licence.

15 Entrez `1` pour utiliser la clé de licence d'évaluation de 90 jours ou `2` pour utiliser la clé de licence valide.

Si vous entrez `2`, le programme d'installation vous invite à entrer la clé de licence Sentinel RD valide. Si la clé de licence que vous spécifiez n'est pas valide, le programme d'installation vous invite à la saisir de nouveau. Si elle n'est toujours pas valide, la clé de licence d'évaluation de 90 jours s'affiche automatiquement. Vous pouvez entrer la clé de licence valide ultérieurement.

Le script charge ensuite la licence d'évaluation ou la licence valide.

16 Indiquez un mot de passe pour l'utilisateur `dbauser` et confirmez-le en le saisissant de nouveau.

Les références `dbauser` sont utilisées pour la création de tables et de partitions dans la base de données PostgreSQL.

17 Indiquez un mot de passe pour l'utilisateur `admin` et confirmez-le en le saisissant de nouveau.

Lorsque vous spécifiez les mots de passe pour les utilisateurs `admin` et `dbauser`, n'utilisez pas de barre oblique inverse (\) ni d'apostrophe (‘) car ces caractères ne sont pas pris en charge par la base de données PostgreSQL.

18 (Facultatif) Une fois l'installation terminée, si vous souhaitez exécuter automatiquement les services Sentinel Rapid Deployment au démarrage du système, exécutez le script `install.sh` avec l'option `-createservice` en tant qu'utilisateur `root` :

```
./install.sh -createservice
```

Une fois l'installation terminée, vous pouvez procéder comme suit :

- Démarrez l'interface Web de Sentinel Rapid Deployment en accédant au site `https://<ADRESSE_IP_SERVEUR>:8443/sentinel`. *<ADRESSE_IP_SERVEUR>* correspond à l'adresse IP de la machine sur laquelle Sentinel Rapid Deployment est installé.
- Lancez Sentinel Control Center en exécutant le fichier `<répertoire_installation>/bin/control_center.sh` avec les références de l'utilisateur créé à l'Étape 7 ci-dessus.

3.3 Installation du gestionnaire des collecteurs et des programmes clients

Utilisez l'interface Web de Novell Sentinel Rapid Deployment pour télécharger les programmes d'installation du gestionnaire des collecteurs et des clients.

3.3.1 Téléchargement des programmes d'installation

1 Entrez l'URL suivante dans un navigateur Web :

`https://<svrname.example.com>:8443/sentinel`

Remplacez `<nom_serveur.exemple.com>` par le nom DNS réel ou l'adresse IP du serveur sur lequel Sentinel est en cours d'exécution. L'URL respecte la casse.

2 Si vous êtes invité à vérifier les certificats, vérifiez-en les informations, puis cliquez sur *Oui* si elles sont valides.

3 Indiquez le nom d'utilisateur et le mot de passe permettant d'accéder au compte Sentinel.

4 Sélectionnez une langue dans la liste déroulante *Langues*.

Il s'agit de la même langue que le code de langue utilisé pour le serveur Sentinel Rapid Deployment et votre ordinateur local. Veillez à ce que le paramètre de langues de votre navigateur soit configuré pour prendre en charge la langue souhaitée.

5 Cliquez sur *Se connecter*.

6 Sélectionnez *Applications*.

Vous pouvez télécharger les programmes d'installation suivants :

Options	Description	Opération
Programme d'installation du gestionnaire des collecteurs	Le programme d'installation du gestionnaire des collecteurs vous permet d'installer le gestionnaire des collecteurs Sentinel sur les plates-formes Windows et Linux.	Cliquez sur *Télécharger le programme d'installation* sous Programme d'installation du gestionnaire des collecteurs et suivez les instructions à l'écran.
Programme d'installation du client	Le programme d'installation des clients permet d'installer Sentinel Control Center, Sentinel Solution Designer et le gestionnaire de données Sentinel sur les plates-formes prises en charge.	Cliquez sur *Télécharger le programme d'installation* sous Programme d'installation du client et suivez les instructions à l'écran.

Pour plus d'informations sur l'installation du gestionnaire des collecteurs, reportez-vous à la Section 3.3.4, « Installation du gestionnaire des collecteurs Sentinel sur SLES ou Windows », page 39. Pour plus d'informations sur l'installation du programme d'installation des clients, reportez-vous à la Section 3.3.3, « Installation des programmes clients Sentinel », page 36.

3.3.2 Numéros de ports des composants des clients Sentinel Rapid Deployment

Utilisez les ports suivants pour configurer votre pare-feu de façon à autoriser l'accès entre le serveur Sentinel Rapid Deployment et les composants du client.

Tableau 3-3 *Numéros de ports compatibles pour les composants Sentinel Rapid Deployment*

Numéro de port	Description
61616	Les gestionnaires des collecteurs distants utilisent ce numéro de port pour se connecter au serveur Sentinel Rapid Deployment via ActiveMQ.
10013	Sentinel Control Center utilise ce numéro de port pour se connecter au serveur Sentinel Rapid Deployment via un proxy.
5432	Le gestionnaire de données Sentinel utilise ce numéro de port pour se connecter à la base de données PostgreSQL.
8443	Les clients Web utilisent ce numéro de port pour se connecter au serveur Sentinel Rapid Deployment.

3.3.3 Installation des programmes clients Sentinel

Vous pouvez installer le programme client Sentinel sur un système Linux ou Windows. Pour installer les programmes clients, procédez comme suit :

1. Recherchez le dossier dans lequel vous avez téléchargé le programme d'installation du client.
2. Extrayez le script d'installation du fichier :

Plate-forme	Opération
Windows	Dézippez le fichier `client_installer.zip`. Les fichiers sont dézippés dans un répertoire intitulé `disk1`.
Linux	Exécutez la commande suivante en utilisant des privilèges root : `unzip client_installer.zip` Les fichiers sont dézippés dans un répertoire intitulé `disk1`.

3 Accédez au répertoire d'installation et démarrez l'installation :

Plate-forme	Opération
Windows	Exécutez `disk1\setup.bat`. **Remarque :** sur une machine Windows Vista, démarrez l'invite de commande en sélectionnant *Exécuter en tant qu'administrateur* dans le menu contextuel (accessible en cliquant sur le bouton droit).
Linux	◆ **Mode GUI :** `<répertoire_installation>/disk1/setup.sh` ◆ **Mode console :** `<répertoire_installation>/disk1/setup.sh -console`

Les étapes ci-dessous doivent uniquement être exécutées en mode GUI.

4 Cliquez sur la flèche vers le bas et sélectionnez l'une des langues.

5 Dans l'écran de bienvenue, cliquez sur *Suivant*.

6 Lisez et acceptez le contrat de licence utilisateur final. Cliquez sur *Suivant*.

7 Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* pour en spécifier un autre. Cliquez sur *Suivant*.

Important : vous ne pouvez pas procéder à l'installation dans un répertoire dont le nom comporte des caractères spéciaux ou des caractères non-ASCII. Par exemple, lors de l'installation de Sentinel Rapid Deployment sous Windows x86-64, le chemin par défaut est `C:\\Program Files (x86)`. Vous devez modifier le chemin par défaut pour éviter les caractères spéciaux, comme des parenthèses sous Windows x86, et poursuivre l'installation.

8 Sélectionnez les programmes Sentinel à installer.

Les options disponibles sont les suivantes :

Composant	Description
Sentinel Control Center	Principale console destinée aux analystes de sécurité ou de conformité.
Gestionnaire de données Sentinel	Destiné aux activités de gestion manuelle des bases de données.
Solution Designer	Permet de créer des Solution Packs.

9 Si vous choisissez d'installer Sentinel Control Center, le programme d'installation vous demande de spécifier l'espace mémoire maximal qui lui sera alloué. Spécifiez la taille maximale du tas JVM (Mo) qui ne sera utilisé que par Sentinel Control Center.

   La plage autorisée est comprise entre 64 et 1024 Mo.

   Cette option n'est pas disponible si des applications Sentinel sont déjà installées.

10 Spécifiez le nom d'utilisateur ou appuyez sur Entrée pour sélectionner le nom d'utilisateur par défaut. Le nom d'utilisateur par défaut est `esecadm`.

   Il s'agit du nom d'utilisateur du propriétaire du produit Sentinel installé. Si l'utilisateur n'existe pas, il est créé, de même que son répertoire privé, dans le répertoire indiqué.

11 Spécifiez le répertoire privé de l'utilisateur ou appuyez sur Entrée pour sélectionner le répertoire par défaut. Le répertoire par défaut est `/export/home`.

   Si le nom d'utilisateur est `esecadm`, le répertoire privé correspondant est `/export/home/esecadm`.

12 Spécifiez le mot de passe utilisateur que ce dernier utilise pour se loguer en tant qu'utilisateur `esecadm` si vous avez sélectionné le nom d'utilisateur par défaut à l'Étape 10. Sinon, définissez le mot de passe utilisateur que vous avez créé à l'Étape 10.

13 Indiquez les informations suivantes :

   - **Port du bus de messages :** port sur lequel le serveur de communication écoute. Il est utilisé par les composants qui se connectent directement au serveur de communication. Le numéro de port par défaut est 61616.
   - **Port proxy de Sentinel Control Center :** port sur lequel le serveur proxy SSL (proxy DAS) écoute et accepte le nom d'utilisateur et le mot de passe. Le serveur proxy SSL accepte les références en fonction des connexions authentifiées. Sentinel Control Center utilise ce port pour se connecter au serveur Sentinel. Le numéro de port par défaut est `10013`.
   - **Nom d'hôte du serveur de communication :** adresse IP ou nom d'hôte de la machine sur laquelle le serveur Sentinel Rapid Deployment est installé.

   Pour que les communications soient actives, veillez à ce que les numéros de ports soient les mêmes que dans le fichier `<répertoire_installation>/config/configuration.xml`, sur le serveur Sentinel Rapid Deployment. Conservez ces informations pour les installations futures sur d'autres machines. Pour plus d'informations sur les numéros de ports, reportez-vous à la Section 3.3.2, « Numéros de ports des composants des clients Sentinel Rapid Deployment », page 36.

14 Cliquez sur *Suivant*.

   Le résumé de l'installation est affiché.

15 Cliquez sur *Installer*.

16 Cliquez sur *Terminer* pour quitter le processus d'installation.

Remarque : lorsque vous vous reloguez, utilisez le nom d'utilisateur que vous avez indiqué dans Étape 10.

Si vous avez oublié le nom d'utilisateur que vous avez défini, ouvrez une console de terminal et saisissez la commande suivante en tant qu'utilisateur `root` :

```
env | grep ESEC_USER
```

Cette commande renvoie le nom d'utilisateur si l'utilisateur est déjà créé et les variables d'environnement déjà définies.

3.3.4 Installation du gestionnaire des collecteurs Sentinel sur SLES ou Windows

Le gestionnaire des collecteurs Sentinel peut être téléchargé depuis la page Applications de l'interface Web de Sentinel Rapid Deployment. Pour installer le gestionnaire des collecteurs, procédez comme suit :

1. Accédez au dossier dans lequel vous avez téléchargé le programme d'installation du gestionnaire des collecteurs.
2. Extrayez le script d'installation du fichier :

Plate-forme	Opération
Windows	Dézippez le fichier `scm_installer.zip`. Les fichiers sont dézippés dans un répertoire intitulé `disk1`.
Linux	Exécutez la commande suivante en utilisant des privilèges root : `unzip scm_installer.zip` Les fichiers sont dézippés dans un répertoire intitulé `disk1`.

3. Accédez au répertoire `disk1` et démarrez l'installation :

Plate-forme	Opération
Windows	Exécutez la commande suivante : `disk1\setup.bat`
Linux	◆ **Mode GUI :** `<répertoire_installation>/disk1/setup.sh` ◆ **Mode console :** `<répertoire_installation>/disk1/setup.sh –console`

4. Sélectionnez une langue pour poursuivre l'installation.
5. Après avoir lu l'écran d'accueil, cliquez sur *Suivant*.
6. Lisez et acceptez le contrat de licence utilisateur final. Cliquez sur *Suivant*.
7. Acceptez le répertoire d'installation par défaut ou cliquez sur *Parcourir* pour en spécifier un autre, puis cliquez sur *Suivant*.

Important : vous ne pouvez pas procéder à l'installation dans un répertoire dont le nom comporte des caractères spéciaux ou des caractères non-ASCII. Par exemple, lors de l'installation de Sentinel sous Windows x86-64, le chemin par défaut est `C:\\Program Files (x86)`. Vous devez modifier le chemin par défaut pour éviter les caractères spéciaux, comme des parenthèses sous Windows x86, et poursuivre l'installation.

8 Indiquez le nom d'utilisateur de l'administrateur Sentinel, ainsi que le chemin du répertoire privé correspondant.

Cette option n'est pas disponible si des applications Sentinel sont déjà installées.

- **Nom d'utilisateur de l'administrateur Sentinel de l'OS :** le nom par défaut est `esecadm`.

  Il s'agit du nom d'utilisateur du propriétaire du produit Sentinel installé. Si l'utilisateur n'existe pas, il est créé, de même que son répertoire privé, dans le répertoire indiqué.
- **Répertoire privé de l'administrateur Sentinel de l'OS :** par défaut, `/export/home`. Si `esecadm` est le nom d'utilisateur, le répertoire privé correspondant est `/export/home/esecadm`.

Pour vous loguer en tant qu'utilisateur `esecadm`, vous devez d'abord définir le mot de passe.

9 Indiquez les informations suivantes :

- **Port du bus de messages :** port sur lequel le serveur de communication écoute. Il est utilisé par les composants qui se connectent directement au serveur de communication. Le numéro de port par défaut est 61616.
- **Nom d'hôte du serveur de communication :** adresse IP ou nom d'hôte de la machine sur laquelle le serveur Sentinel Rapid Deployment est installé.

Pour que les communications soient actives, veillez à ce que les numéros de port soient identiques sur chaque machine du système Sentinel. Conservez ces informations pour les installations futures sur d'autres machines.

10 Cliquez sur *Suivant*.

11 Indiquez les informations suivantes :

- **Configuration de mémoire automatique :** sélectionnez la quantité totale de mémoire à allouer au gestionnaire des collecteurs. Le programme d'installation détermine automatiquement la distribution optimale de la mémoire entre les différents composants en prenant en compte la surcharge d'information estimée du système d'exploitation et de la base de données.

  Important : vous pouvez modifier la valeur -Xmx du fichier `configuration.xml` afin de changer la quantité de mémoire RAM attribuée au processus du gestionnaire des collecteurs. Le fichier `configuration.xml` est situé dans le répertoire `<répertoire_installation>/config` sous Linux ou dans le répertoire `<répertoire_installation>\config` sous Windows.

- **Configuration de mémoire personnalisée :** cliquez sur le bouton *Configurer* pour régler précisément les allocations de mémoire. Cette option n'est disponible que si la machine dispose d'une mémoire suffisante.

12 Cliquez sur *Suivant*.

L'écran récapitulatif des fonctionnalités sélectionnées pour l'installation s'affiche.

13 Cliquez sur *Installer*.

14 Une fois l'installation terminée, vous êtes invité à entrer le nom d'utilisateur et le mot de passe utilisés par la stratégie ActiveMQ JMS pour vous connecter au courtier.

Utilisez le nom d'utilisateur `collectormanager` et le mot de passe correspondant, disponible dans le fichier `<répertoire_installation>/config/activemqusers.properties` sur le serveur Sentinel.

Exemple de références disponibles dans le fichier `activemqusers.properties` :

`collectormanager=cefc76062c58e2835aa3d777778f9295`

`collectormanager` est le nom d'utilisateur et `cefc76062c58e2835aa3d777778f9295`, le mot de passe correspondant.

Vous devez vous loguer en tant qu'utilisateur collectormanager avec le mot de passe correspondant pendant l'installation du service Gestionnaire des collecteurs. Dans ce cas, l'utilisateur `collectormanager` dispose de droits d'accès uniquement aux canaux de communication requis pour les opérations du gestionnaire des collecteurs.

Une fois l'installation terminée, vous êtes invité à redémarrer les services Sentinel ou à vous reloguer et à les démarrer manuellement.

15 Cliquez sur *Terminer* pour redémarrer votre système.

16 Lorsque vous vous reloguez, utilisez le nom d'utilisateur que vous avez spécifié à l'Étape 8.

Si vous avez oublié le nom d'utilisateur, ouvrez une console de terminal et saisissez la commande suivante avec les références `root`.

```
env | grep ESEC_USER
```

Cette commande renvoie le nom d'utilisateur si l'utilisateur est déjà créé et les variables d'environnement déjà définies.

Remarque : l'installation du gestionnaire des collecteurs présente plusieurs problèmes sur la plate-forme Windows 2008, ainsi que sur les images de gestionnaires des collecteurs. Pour obtenir des informations sur la résolution de ces problèmes, reportez-vous à l'Annexe B, « Conseils de dépannage », page 91.

3.4 Démarrage et arrêt manuels des services Sentinel

Pour démarrer les services Sentinel manuellement, utilisez l'une des commandes suivantes :

Plate-forme	Commande
Linux	`<install_directory>/bin/sentinel.sh start`
Windows	`<install_directory>/bin/sentinel.bat start`

Pour arrêter les services Sentinel manuellement, utilisez l'une des commandes suivantes :

Plate-forme	Commande
Linux	`<install_directory>/bin/sentinel.sh stop`
Windows	`<install_directory>/bin/sentinel.bat stop`

Vous pouvez également utiliser la commande ci-après pour démarrer ou arrêter les services Sentinel.

```
/etc/init.d/sentinel.sh stop|start
```

3.5 Mise à niveau manuelle de Java

La version Java 1.6.0_24 est intégrée au programme d'installation du serveur Sentinel Rapid Deployment et s'installe en même temps que le serveur Sentinel Rapid Deployment. Cependant, si vous mettez à niveau Java vers la dernière version sur le serveur, vous devez procéder comme suit afin que Sentinel Rapid Deployment utilise la dernière version :

1. Téléchargez les ensembles jre selon le système d'exploitation sur lequel le serveur Sentinel Rapid Deployment est installé.

   L'utilisateur qui effectue la mise à niveau doit disposer d'un accès en écriture au répertoire d'installation de Sentinel Rapid Deployment et au répertoire dans lequel les fichiers de mise à niveau seront téléchargés.

   - Si vous avez installé Sentinel Rapid Deployment sur SUSE Linux Enterprise Server, téléchargez les ensembles jre 32 bits et 64 bits sur le site de téléchargement Java (http://www.java.com/en/download/manual.jsp).

2. Renommez les dossiers `jre` et `jre64` dans le répertoire d'installation de Sentinel Rapid Deployment en `jre_old` et `jre64_old` respectivement.

   ```
   cd <install_path>/sentinel_rd
   mv jre jre_old
   mv jre64 jre64_old
   ```

   Remarque : il est nécessaire de renommer les dossiers pour pouvoir revenir aux anciennes versions si la mise à niveau de Java ne fonctionne pas correctement. Vous pouvez supprimer les dossiers renommés si Java fonctionne correctement après la mise à niveau.

   ---

3. Procédez à l'extraction des ensembles jre téléchargés.
4. Renommez le dossier 32 bits en `jre` et le répertoire 64 bits en `jre64`.
5. Copiez les dossiers renommés `jre` et `jre64` dans le répertoire d'installation de Sentinel Rapid Deployment.

   ```
   copy jre <install_path>/sentinel_rd/
   copy jre64 <install_path>/sentinel_rd/
   ```

6. (Sous condition) Assurez-vous que vous avez conféré les droits et autorisations nécessaires pour les dossiers `jre` et `jre64` à l'utilisateur exécutant le serveur Sentinel Rapid Deployment.
7. Redémarrez le serveur Sentinel Rapid Deployment, redémarrez le navigateur et vérifiez que Java est correctement installé.

3.6 Configuration de post-installation

Cette section décrit la configuration de post-installation des services Sentinel Rapid Deployment.

- Section 3.6.1, « Modifications des paramètres de date et d'heure », page 43
- Section 3.6.2, « Configuration d'un intégrateur SMTP pour l'envoi de notifications Sentinel », page 43
- Section 3.6.3, « Services du gestionnaire des collecteurs », page 43
- Section 3.6.4, « Gestion du temps », page 44

3.6.1 Modifications des paramètres de date et d'heure

Le format par défaut de date et d'heure de Sentinel Control Center peut être modifié. Pour plus d'informations sur la personnalisation du format de date et d'heure par rapport à votre fuseau horaire, consultez le site Web de Java (http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html).

1. Modifiez le fichier `SentinelPreferences.properties`.

   `<install_directory>/config/SentinelPreferences.properties`

2. Supprimez le contenu de la ligne suivante et personnalisez le format de date et d'heure dans les champs appropriés des événements de Sentinel Control Center :

   ```
   com.eSecurity.Sentinel.event.datetimeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
   ```

3.6.2 Configuration d'un intégrateur SMTP pour l'envoi de notifications Sentinel

Dans Sentinel Rapid Deployment, une opération Envoyer un message électronique fonctionne avec un intégrateur SMTP pour envoyer des messages aux destinataires à partir de divers contextes de l'interface Sentinel. L'intégrateur SMTP doit être configuré sur la base d'informations de connexion valides avant de pouvoir fonctionner. Pour plus d'informations, reportez-vous à la section « Envoi d'un e-mail » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

Une instance d'opération unique du plug-in d'opération Envoyer un message électronique est automatiquement créée dans chaque installation de Sentinel. Aucune configuration n'est nécessaire pour l'opération Envoyer un message électronique, si ce n'est que les destinataires et le contenu du message doivent être configurés dans les paramètres de l'opération.

Sentinel utilise cette opération en interne pour envoyer des messages dans les situations suivantes :

- Une règle de corrélation déployée avec une opération Envoyer un message électronique est déclenchée. Cette opération désigne l'opération signalée par l'icône d'engrenage, qui est uniquement valide pour la corrélation (contrairement à l'opération Envoyer un message électronique JavaScript, indiquée par l'icône JS JavaScript).
- Le processus de travail inclut une activité ou une étape de message configurée pour envoyer un message électronique.
- L'utilisateur ouvre un incident et choisit d'exécuter une activité configurée pour envoyer un message électronique.
- L'utilisateur clique avec le bouton droit de la souris sur un événement et sélectionne *Courrier électronique*.
- L'utilisateur ouvre un incident et sélectionne *Incident de message électronique*.

3.6.3 Services du gestionnaire des collecteurs

- « Installation de gestionnaires des collecteurs supplémentaires » page 44
- « Utilisation du collecteur général » page 44

Installation de gestionnaires des collecteurs supplémentaires

Les gestionnaires des collecteurs gèrent tous les processus de collecte et d'analyse des données. Il peut parfois s'avérer nécessaire d'ajouter un noeud de gestionnaire des collecteurs Sentinel supplémentaire à un environnement Sentinel afin de répartir la charge entre toutes les machines. Les gestionnaires des collecteurs distants présentent plusieurs avantages :

- Analyse et traitement des événements distribués afin d'améliorer les performances système.
- Filtrage, codage et compression des données au niveau du système source via la colocalisation avec les sources d'événements. Ceci réduit les exigences de bande passante réseau et renforce la sécurité des données.
- Installation sur des systèmes d'exploitation supplémentaires. Par exemple, l'installation d'un nœud de gestionnaire des collecteurs sous Microsoft Windows permet la collecte des données via l'utilisation du protocole WMI.
- Caching des fichiers permettant au gestionnaire des collecteurs à distance de mettre en cache de grandes quantités de données pendant que le serveur est momentanément occupé à archiver des événements ou à traiter un pic d'événements. Cet avantage est particulièrement intéressant pour les protocoles, tels que Syslog qui ne prennent normalement pas en charge le caching d'événements.

La charge des composants du gestionnaire des collecteurs peut être équilibrée en installant des instances de ces composants sur des machines supplémentaires. Vous pouvez installer des gestionnaires des collecteurs supplémentaires en exécutant le programme d'installation sur une nouvelle machine. Pour plus d'informations sur l'installation du gestionnaire des collecteurs, reportez-vous à laSection 3.3.4, « Installation du gestionnaire des collecteurs Sentinel sur SLES ou Windows », page 39.

Utilisation du collecteur général

Lors de l'installation du serveur Sentinel Rapid Deployment , un collecteur nommé Collecteur général est configuré. Par défaut, il crée des événements à un rythme de 5 événements par seconde (EPS).

Vous pouvez télécharger des collecteurs supplémentaires pour votre système sur le site Web de Novell (http://support.novell.com/products/sentinel/collectors.html).

3.6.4 Gestion du temps

Vous devez connecter le serveur Sentinel à un serveur NTP (Network Time Protocol) ou à un autre type de serveur horaire. Si l'heure système des machines n'est pas synchronisée, le moteur de corrélation Sentinel et la fonctionnalité Active Views ne fonctionnent pas correctement. Les événements des gestionnaires des collecteurs ne sont pas considérés comme étant en temps réel. Par conséquent, ils ne sont pas envoyés directement à la base de données Sentinel, mais passent par les centres Sentinel Control Center et les moteurs de corrélation.

Par défaut, le seuil pour les données en temps réel est de 120 secondes. Vous pouvez le modifier en changeant la valeur de `security.router.event.realtime.expiration` dans le fichier `event-router.properties`. L'heure de l'événement Sentinel est renseignée sur la base de l'heure du périphérique approuvé ou du gestionnaire des collecteurs. Vous pouvez sélectionner l'heure du périphérique approuvé lors de la configuration d'un collecteur. Cette heure correspond à l'heure de génération du journal par le périphérique. L'heure du gestionnaire des collecteurs correspond à l'heure locale du système du gestionnaire des collecteurs.

3.7 Authentification LDAP

En plus de l'authentification de base de données, Sentinel Rapid Deployment prend en charge l'authentification LDAP. Vous pouvez autoriser les utilisateurs à se loguer à Sentinel Rapid Deployment avec leurs références Novell eDirectory ou Microsoft Active Directory en configurant un serveur Sentinel Rapid Deployment pour l'authentification LDAP.

3.7.1 Présentation

Vous pouvez configurer le serveur Sentinel Rapid Deployment pour l'authentification LDAP sur une connexion SSL sécurisée avec ou sans utilisation de recherches anonymes dans l'annuaire LDAP.

Remarque : si la recherche anonyme est désactivée dans l'annuaire LDAP, vous ne devez pas configurer le serveur Sentinel Rapid Deployment pour qu'il utilise la recherche anonyme.

- **Recherche anonyme :** lorsque vous créez des comptes utilisateur Sentinel Rapid Deployment LDAP, vous devez spécifier le nom de l'utilisateur du répertoire, mais pas son nom distinctif.

  Lorsque l'utilisateur LDAP se logue au serveur Sentinel Rapid Deployment, celui-ci exécute une recherche anonyme dans l'annuaire LDAP basée sur le nom d'utilisateur spécifié, trouve le nom distinctif correspondant et authentifie le login de l'utilisateur par rapport à l'annuaire LDAP en utilisant le nom distinctif.

- **Recherche non anonyme :** lorsque vous créez des comptes utilisateur Sentinel Rapid Deployment LDAP, vous devez spécifier à la fois le nom de l'utilisateur du répertoire et son nom distinctif.

  Lorsqu'un utilisateur LDAP se logue au serveur Sentinel Rapid Deployment, celui-ci authentifie le login de l'utilisateur par rapport à l'annuaire LDAP en utilisant son nom distinctif et n'exécute pas de recherche anonyme dans l'annuaire LDAP.

  Il existe une autre approche qui s'applique uniquement à Active Directory. Pour plus d'informations, reportez-vous à la section Authentification LDAP non anonyme avec l'attribut UserPrincipalName dans Active Directory.

3.7.2 Conditions préalables

Exportation du certificat CA du serveur LDAP

La connexion SSL sécurisée au serveur LDAP nécessite un certificat CA du serveur LDAP que vous devez exporter vers un fichier au format de codage Base64.

- **eDirectory:** reportez-vous à la section Exportation d'un certificat CA organisationnel auto-signé (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html).

  Pour exporter un certificat CA eDirectory dans iManager, les plug-ins du serveur de certificats Novell pour iManager doivent être installés.
- **Active Directory:** reportez-vous à la section Activation du protocole LDAP sur SSL avec une autorité de certification tierce (http://support.microsoft.com/kb/321051).

Activation de la recherche anonyme dans l'annuaire LDAP

Pour procéder à l'authentification LDAP via la fonction de recherche anonyme, vous devez activer cette dernière dans l'annuaire LDAP. Par défaut, la recherche anonyme est activée dans eDirectory et désactivée dans Active Directory.

Pour activer la recherche anonyme dans l'annuaire LDAP, reportez-vous aux instructions ci-après :

- **eDirectory:** reportez-vous à l'attribut ldapBindRestrictions dans la section Attributs de l'objet Serveur LDAP (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html).
- **Active Directory:** l'objet Utilisateur ANONYMOUS LOGON doit disposer d'une autorisation appropriée et d'un accès en lecture aux attributs `sAMAccountName` et `objectclass`. Pour plus d'informations, reportez-vous à la section Configuration d'Active Directory pour autoriser les requêtes anonymes (http://support.microsoft.com/kb/320528).

  Pour Windows Server 2003, vous devez exécuter une configuration supplémentaire. Pour plus d'informations, reportez-vous à la section Configuration d'Active Directory sous Windows Server 2003 (http://support.microsoft.com/kb/326690/en-us).

3.7.3 Configuration du serveur Sentinel pour l'authentification LDAP

1. Vérifiez que votre système respecte la configuration requise, indiquée à la Section 3.7.2, « Conditions préalables », page 45.
2. Loguez-vous au serveur Sentinel Rapid Deployment en tant qu'utilisateur `root`.
3. Copiez le fichier exporté du certificat CA du serveur LDAP dans le répertoire `<répertoire_installation>/config`.
4. Définissez la propriété et les autorisations du fichier de certificat de la manière suivante :

   ```
   chown novell:novell <répertoire_installation>/config/<fichier-cert>
   chmod 700 <répertoire_installation>/config/<fichier-cert>
   ```
5. Passez à l'utilisateur `novell` :

   ```
   su - novell
   ```
6. Accédez au répertoire `<répertoire_installation>/bin`.
7. Exécutez le script de configuration de l'authentification LDAP :

```
./ldap_auth_config.sh
```

Le script crée une sauvegarde des fichiers de configuration `auth.login` et `configuration.xml` dans le répertoire `config` comme `auth.login.sav` et `configuration.xml.sav` avant de les modifier en vue de l'authentification LDAP.

8 Indiquez les informations suivantes :

Appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez une autre valeur pour la remplacer.

- **Emplacement d'installation de Sentinel :** répertoire d'installation sur le serveur Sentinel.
- **Nom d'hôte ou adresse IP du serveur LDAP :** nom d'hôte ou adresse IP de la machine sur laquelle le serveur LDAP est installé La valeur par défaut est localhost. Toutefois, vous ne devez pas installer le serveur LDAP sur la même machine que le serveur Sentinel
- **Port du serveur LDAP :** numéro de port garantissant une connexion LDAP sécurisée. Le numéro de port par défaut est 636.
- **Recherches anonymes dans l'annuaire LDAP :** spécifiez `y` si vous souhaitez activer les recherches anonymes. Sinon, spécifiez `n`. La valeur par défaut est `y`.

  Si vous indiquez `n`, procédez à la configuration LDAP et suivez les étapes présentées à la section « Authentification LDAP sans recherche anonyme » page 48.
- **Annuaire LDAP utilisé :** ce paramètre s'affiche uniquement si vous avez spécifié « y » pour les recherches anonymes. Spécifiez 1 pour Novell eDirectory ou 2 pour Active Directory. La valeur par défaut est 1.
- **Sous-arborescence LDAP pour rechercher les utilisateurs :** ce paramètre s'affiche uniquement si vous avez spécifié « y » pour les recherches anonymes. La sous-arborescence du répertoire contient les objets Utilisateur. Exemples de spécification de sous-arborescence dans eDirectory et Active Directory :
  - eDirectory:

    ```
    ou=users,o=novell
    ```

    Remarque : si aucune sous-arborescence n'est spécifiée pour eDirectory, la recherche s'exécute sur l'ensemble du répertoire.
  - Active Directory:

    ```
    CN=users,DC=TESTAD,DC=provo, DC=novell,DC=com
    ```

    Remarque : la sous-arborescence ne peut pas être vide pour Active Directory.
- **Nom du fichier du certificat du serveur LDAP :** nom du fichier du certificat CA eDirectory/Active Directory que vous avez copié à l'Étape 3.

9 Entrez l'une des commandes suivantes :

- `y` pour accepter les valeurs entrées
- `n` pour entrer des nouvelles valeurs
- `q` pour quitter la configuration

En cas de configuration exécutée avec succès :

- Le certificat du serveur LDAP est ajouté à un keystore intitulé `<répertoire_installation>/config/ldap_server.keystore`.
- Les fichiers de configuration `auth.login` et `configuration.xml` du répertoire `<répertoire_installation>/config` sont mis à jour pour permettre l'authentification LDAP.

10 Entrez `y` pour redémarrer le service Sentinel.

Important : en cas d'erreur, revenez à l'étape des modifications apportées aux fichiers de configuration `auth.login` et `configuration.xml` du répertoire `config` :

```
cp -p auth.login.sav auth.login
cp -p configuration.xml.sav configuration.xml
```

---

11 (Sous condition) Si vous avez spécifié `n` pour Recherches anonymes dans l'annuaire LDAP :, continuez avec « Authentification LDAP sans recherche anonyme » page 48.

Authentification LDAP sans recherche anonyme

Si vous avez spécifié n pour les recherches anonymes dans l'annuaire LDAP lors de la configuration de Sentinel Rapid Deployment pour l'authentification LDAP, aucune recherche anonyme ne sera exécutée.

Lorsque vous créez le compte utilisateur LDAP à l'aide de Sentinel Control Center, veillez à spécifier *le nom distinctif de l'utilisateur LDAP* pour l'authentification LDAP non anonyme. Vous pouvez utiliser cette approche pour eDirectory et Active Directory.

Pour plus d'informations, reportez-vous à la section « Création d'un compte utilisateur LDAP pour Sentinel » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

Pour Active Directory, il existe une autre approche permettant de procéder à l'authentification LDAP sans recherches anonymes. Pour plus d'informations, reportez-vous à Authentification LDAP non anonyme avec l'attribut UserPrincipalName dans Active Directory.

Authentification LDAP non anonyme avec l'attribut UserPrincipalName dans Active Directory

Pour Active Directory, vous pouvez également exécuter une authentification LDAP sans recherche anonyme via l'attribut UserPrincipalName :

1 Assurez-vous que l'attribut UserPrincipalName est défini sur <*nomComptesAM@domaine*> pour l'utilisateur Active Directory.

Pour plus d'informations, reportez-vous à la section Attribut UserPrincipalName (http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx).

2 Vérifiez que vous avez suivi la procédure depuis l'Étape 1 page 46 jusqu'à l'Étape 10 page 48 et spécifié `n` pour « Recherches anonymes dans l'annuaire LDAP : » page 47.

3 Sur le serveur Sentinel, modifiez la section `LdapLogin` du fichier `<Répertoire d'installation>/config/auth.login` :

```
LdapLogin {
 com.sun.security.auth.module.LdapLoginModule required
 userProvider="ldap://LDAP server IP:636/DN of the Container that contains
the user objects"
 authIdentity="{USERNAME}@Domain Name"
 userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
 useSSL=true;
 };
```

Par exemple :

```
LdapLogin {
 com.sun.security.auth.module.LdapLoginModule required
 userProvider="ldap://137.65.151.12:636/DC=Test-
AD,DC=provo,DC=novell,DC=com"
 authIdentity="{USERNAME}@Test-AD.provo.novell.com"
 userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
 useSSL=true;
 };
```

4 Redémarrez le service Sentinel :

```
/etc/init.d/sentinel stop
```

```
/etc/init.d/sentinel start
```

3.7.4 Configuration de plusieurs serveurs LDAP en vue d'une reprise après échec

Pour configurer un ou plusieurs serveurs LDAP en tant que serveurs de reprise après échec en vue de l'authentification LDAP, procédez comme suit :

1 Assurez-vous que vous avez suivi la procédure depuis l'Étape 2 page 46 jusqu'à l'Étape 10 page 48 pour configurer le serveur Sentinel en vue de l'authentification LDAP au niveau du serveur LDAP principal.

2 Loguez-vous au serveur Sentinel en tant qu'utilisateur `novell`.

3 Arrêtez le service Sentinel.

```
/etc/init.d/sentinel stop
```

4 Accédez au répertoire `<répertoire_installation>/config` :

```
cd <install_directory>/config
```

5 Ouvrez le fichier `auth.login` pour le modifier.

```
vi auth.login
```

6 Mettez à jour l'option `userProvider` dans la section LdapLogin pour spécifier plusieurs URL LDAP. Séparez chaque URL par un espace.

Par exemple :

```
userProvider="ldap://ldap-url1 ldap://ldap-url2"
```

Pour Active Directory, assurez-vous que la sous-arborescence de l'URL LDAP n'est pas vide.

Pour plus d'informations sur la spécification de plusieurs URL LDAP, reportez-vous à la description de l'option `userProvider` dans le module Class LdapLogin Module (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

7 Enregistrez les modifications apportées.

8. Exportez le certificat de chaque serveur LDAP de reprise après échec et copiez le fichier de certificat dans le répertoire <*répertoire_installation*>/config du serveur Sentinel.

   Pour plus d'informations, reportez-vous à la section « Exportation du certificat CA du serveur LDAP » page 46.

9. Assurez-vous que vous avez défini les droits et autorisations nécessaires concernant le fichier de certificat pour chaque serveur LDAP de basculement.

   ```
   chown novell:novell <install_directory>/config/<cert-file>
   chmod 700 <install_directory>/config/<cert-file>
   ```

10. Ajoutez chaque certificat de serveur LDAP de basculement au keystore ldap_server.keystore créé à l'Étape 8 de la section « Configuration du serveur Sentinel pour l'authentification LDAP » page 46.

    ```
    <install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
    -file <certificate-file> -alias <alias_name> -keystore
    ldap_server.keystore -storepass sentinel
    ```

    Remplacez <*fichier-certificat*> par le nom du fichier de certificat au format de codage Base64 et remplacez <*nom_alias*> par le nom de l'alias du certificat à importer.

    Important : n'oubliez pas de spécifier l'alias. Si aucun alias n'a été spécifié, le keytool utilise mykey en tant qu'alias par défaut. Lorsque vous importez plusieurs certificats dans le keystore sans spécifier d'alias, le keytool signale que l'alias existe déjà.

    ---

11. Démarrez le service Sentinel.

    ```
    /etc/init.d/sentinel start
    ```

Il est possible que le service ne se connecte pas au serveur LDAP de reprise après échec si un timeout survient au niveau du serveur Sentinel avant que celui-ci ne détecte l'arrêt du serveur LDAP principal. Pour vous assurer que le serveur Sentinel se connecte au serveur LDAP de reprise après échec sans que survienne un timeout, procédez comme suit :

1. Loguez-vous au serveur Sentinel en tant qu'utilisateur root.
2. Ouvrez le fichier sysct1.conf pour le modifier :

   ```
   vi /etc/sysctl.conf
   ```

3. Vérifiez que la valeur net.ipv4.tcp_syn_retries est définie sur 3. Si l'entrée n'existe pas, ajoutez-la. Enregistrez le fichier :

   ```
   net.ipv4.tcp_syn_retries = 3
   ```

4. Exécutez la commande pour appliquer les modifications :

   ```
   /sbin/sysctl -p
   /sbin/sysctl -w net.ipv4.route.flush=1
   ```

5. Définissez la valeur de timeout du serveur Sentinel en ajoutant le paramètre -Desecurity.remote.timeout=60 dans les fichiers control_center.sh et solution_designer.sh du répertoire <*répertoire_installation*>/bin :

   control_center.sh :

```
"<install_directory>/jre/bin/java" $MEMORY -
Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
Desecurity.cache.directory="<install_directory>/data/
control_center.cache" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
control_center_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Dice.pilots.html4.baseFontFamily="Arial Unicode MS" -
Desecurity.remote.timeout=60 -jar ../lib/console.jar
```

solution_designer.sh :

```
"<install_directory>/jre/bin/java" -classpath $LOCAL_CLASSPATH $MEMORY -
Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
Dsentinel.installer.jar.location="<install_directory>/lib/
contentinstaller.jar" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
solution_designer_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -Desecurity.cache.directory=../
data/solution_designer.cache -Desecurity.remote.timeout=60
com.esecurity.content.exportUI.ContentPackBuilder
```

3.7.5 Configuration de l'authentification LDAP pour plusieurs domaines Active Directory

Si les utilisateurs LDAP à authentifier appartiennent à des domaines Active Directory différents, vous pouvez configurer le serveur Sentinel Rapid Deployment pour l'authentification LDAP en procédant comme suit :

1. Assurez-vous que vous avez suivi la procédure de l'Étape 2 page 46 à l'Étape 10 page 48 pour configurer le serveur Sentinel pour l'authentification LDAP par rapport au contrôleur de domaine Active Directory du premier domaine : Vérifiez également que vous avez indiqué `n` pour « Recherches anonymes dans l'annuaire LDAP : » page 47.
2. Loguez-vous au serveur Sentinel en tant qu'utilisateur `novell`.
3. Arrêtez le service Sentinel.

   ```
   /etc/init.d/sentinel stop
   ```
4. Accédez au répertoire `<répertoire_installation>/config` :

   ```
   cd <install_directory>/config
   ```
5. Ouvrez le fichier `auth.login` pour le modifier.

   ```
   vi auth.login
   ```
6. Modifiez la section `LdapLogin` pour spécifier plusieurs URL LDAP en séparant chaque URL par un espace.

   Par exemple :

```
LdapLogin {
        com.sun.security.auth.module.LdapLoginModule required
        userProvider="ldap://<IP of the domain 1 domain controller>:636
ldap://<IP of the domain 2 domain controller>:636"
        authIdentity="{USERNAME}"
        useSSL=true;
};
```

Pour plus d'informations sur la spécification de plusieurs URL LDAP, reportez-vous à la description de l'option `userProvider` dans le module Class LdapLogin Module (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

7 Enregistrez les modifications apportées.

8 Exportez le certificat du contrôleur de domaine de chaque domaine et copiez les fichiers de certificat dans le répertoire `<répertoire_installation>/config`sur le serveur Sentinel.

Pour plus d'informations, reportez-vous à « Exportation du certificat CA du serveur LDAP » page 46.

9 Assurez-vous que vous avez défini les droits et autorisations nécessaires pour les fichiers de certificat.

```
chown novell:novell <install_directory>/config/<cert-file>
chmod 700 <install_directory>/config/<cert-file>
```

10 Ajoutez chaque certificat au keystore `ldap_server.keystore` créé à l'Étape 8 de la section « Configuration du serveur Sentinel pour l'authentification LDAP » page 46.

```
<install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
-file <certificate-file> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

Remplacez `<fichier-certificat>` par le nom du fichier de certificat au format de codage Base64 et remplacez `<nom_alias>` par le nom de l'alias du certificat à importer.

Important : n'oubliez pas de spécifier l'alias. Si aucun alias n'a été spécifié, le keytool utilise `mykey` en tant qu'alias par défaut. Lorsque vous importez plusieurs certificats dans le keystore sans spécifier d'alias, le keytool signale que l'alias existe déjà.

---

11 Démarrez le service Sentinel.

```
/etc/init.d/sentinel start
```

3.7.6 Connexion à l'aide des références utilisateur LDAP

Après avoir configuré avec succès le serveur Sentinel en vue de l'authentification LDAP, vous pouvez créer des comptes utilisateur LDAP Sentinel dans Sentinel Control Center. Pour plus d'informations sur la création de comptes utilisateur LDAP, reportez-vous à la section « Création d'un compte utilisateur LDAP pour Sentinel » du *Guide de l'utilisateur de Sentinel Rapid Deployment.*

Après avoir créé le compte utilisateur LDAP, vous pouvez vous loguer à l'interface Web utilisateur de Sentinel Rapid Deployment, à Sentinel Control Center et à Sentinel Solution Designer à l'aide de votre nom d'utilisateur et de votre mot de passe LDAP.

Remarque : pour modifier une configuration LDAP existante, exécutez de nouveau le script `ldap_auth_config` et spécifiez les nouvelles valeurs des paramètres.

3.8 Mise à jour de la clé de licence d'évaluation vers une clé de licence de production

Si vous achetez le produit après évaluation, suivez la procédure ci-dessous pour mettre à jour la clé de licence afin d'éviter la réinstallation :

1. Loguez-vous à la machine sur laquelle Sentinel Rapid Deployment est installé en tant qu'administrateur Sentinel (l'utilisateur par défaut est `novell`).
2. À l'invite de commande, remplacez le répertoire par `<répertoire_installation>/bin`.
3. Saisissez la commande suivante :

   ```
   ./softwarekey.sh
   ```

4. Spécifiez 1 pour définir la clé principale. Appuyez sur Entrée.
5. Entrez la nouvelle clé de licence valide et suivez les instructions qui s'affichent à l'écran pour quitter le système après la mise à jour de la clé de licence.

Mise à niveau de Sentinel Rapid Deployment

4

Cette section fournit des informations sur la mise à niveau d'une version existante de Sentinel Rapid Deployment vers le dernier correctif.

Remarque : ce correctif s'applique uniquement à une installation 64 bits de Sentinel Rapid Deployment. L'application de ce correctif sur un système de démo de 32 bits entraîne le dysfonctionnement de l'installation.

4.1 Conditions préalables

- Assurez-vous que Sentinel 6.1 Rapid Deployment SP1 est déjà installé sur le système que vous mettez à niveau.
- Assurez-vous que les tâches du gestionnaire de données Sentinel sont activées de sorte que la partition en ligne active n'atteigne jamais P_MAX. Si elle atteint P_MAX et si vous ajoutez des partitions manuellement, Sentinel Control Center ne se lancera pas correctement.

4.2 Installation du correctif sur le serveur

1 Loguez-vous au serveur sur lequel vous souhaitez installer le correctif en tant qu'utilisateur `novell`.

Avant d'installer le correctif, veillez à sauvegarder la base de données Sentinel, le dossier de configuration et le dossier de données en utilisant les commandes suivantes :

Base de données Sentinel :

```
tar -cf backup.tar <install_directory>/3rdparty/postgresql/database_files
tar -cf backupdata.tar <install_directory>/3rdparty/postgresql/data
```

Dossier de configuration :

```
tar -cf backupconfig.tar <install_directory>/config
```

Dossier de données :

```
tar -cf backupdata.tar <install_directory>/data
```

Pour plus d'informations sur ces commandes, reportez-vous à la section Sauvegarde au niveau du système de fichiers (http://www.postgresql.org/docs/8.1/static/backup-file.html) sur le site Web PostgreSQL.

2 Sauvegardez la configuration Gestion de source d'événements (ESM, Event Source Management) et créez une exportation ESM.

Pour plus d'informations, reportez-vous à la section « Exportation d'une configuration » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

3 Téléchargez le programme d'installation du correctif pour Sentinel Rapid Deployment à partir de l'outil Novell Patch Finder (http://download.novell.com/patch/finder/).

4 Copiez le paquetage du programme d'installation téléchargé dans un répertoire temporaire.

5 Arrêtez les services Sentinel :

```
sentinel.sh stop
```

6 Indiquez la commande suivante pour extraire les fichiers contenus dans le paquetage du programme d'installation :

```
unzip <install_filename>
```

Remplacez <*install_filename*> par le nom effectif du fichier du programme d'installation.

7 Accédez au répertoire à partir duquel vous avez extrait les fichiers du programme d'installation :

```
cd <directory_name>
```

Remplacez <*nom_répertoire*> par le nom effectif du répertoire à partir duquel vous avez extrait les fichiers.

8 Spécifiez la commande suivante pour appliquer le correctif au serveur, puis suivez les instructions qui s'affichent à l'écran :

```
./service_pack.sh
```

Une fois l'installation terminée, les services Sentinel démarrent automatiquement.

9 Appliquez le correctif à l'ensemble des machines sur lesquelles un gestionnaire des collecteurs, des programmes clients ou les deux sont exécutés.

4.3 Mise à niveau du gestionnaire des collecteurs et des programmes clients

4.3.1 Mise à niveau du gestionnaire des collecteurs

Linux

1 Loguez-vous à la machine du gestionnaire des collecteurs Sentinel Rapid Deployment en tant qu'utilisateur `root`.

2 Téléchargez le programme d'installation du correctif pour Sentinel Rapid Deployment à partir de l'outil Novell Patch Finder (http://download.novell.com/patch/finder/).

3 Copiez le fichier d'installation téléchargé dans un répertoire temporaire.

4 Spécifiez la commande suivante pour extraire les fichiers contenus dans le paquetage zippé du programme d'installation :

```
unzip <install_filename>
```

Remplacez <*install_filename*> par le nom réel du fichier d'installation.

5 Accédez au répertoire à partir duquel vous avez extrait les fichiers du programme d'installation :

```
cd <directory_name>
```

Remplacez <*directory_name*> par le nom effectif du répertoire à partir duquel les fichiers du programme d'installation ont été extraits.

6 Arrêtez les services du gestionnaire des collecteurs.

```
<install_directory>/bin/sentinel.sh stop
```

7 Exécutez le programme d'installation du paquetage de services, puis suivez les instructions qui s'affichent à l'écran :

```
./service_pack.sh
```

Une fois l'installation terminée, les services du gestionnaire des collecteurs démarrent automatiquement.

Windows

1 Loguez-vous à la machine du gestionnaire des collecteurs Sentinel Rapid Deployment en tant qu'utilisateur admin.

2 Téléchargez le programme d'installation du correctif pour Sentinel Rapid Deployment à partir de l'outil Novell Patch Finder (http://download.novell.com/patch/finder/).

3 Copiez le fichier du programme d'installation dans un répertoire temporaire.

4 Extrayez les fichiers du paquetage du programme d'installation.

5 Arrêtez les services du gestionnaire des collecteurs.

```
<install_directory>\bin\sentinel.bat stop
```

6 Accédez au répertoire dans lequel vous avez extrait les fichiers du programme d'installation.

7 Appliquez l'une des méthodes suivantes pour exécuter le programme d'installation :

- Double-cliquez sur le fichier `service_pack.bat`, puis suivez les instructions qui s'affichent à l'écran.
- À l'invite de commande, exécutez le fichier `service_pack.bat`, puis suivez les instructions qui s'affichent à l'écran.

Une fois l'installation terminée, les services du gestionnaire des collecteurs démarrent automatiquement.

4.3.2 Mise à niveau des programmes clients

- « Linux » page 57
- « Windows » page 58

Linux

1 Loguez-vous en tant qu'utilisateur `root` à la machine exécutant les programmes clients de Novell Sentinel Rapid Deployment.

2 Téléchargez le programme d'installation du correctif pour Sentinel Rapid Deployment à partir du localisateur de correctifs Novell (http://download.novell.com/patch/finder/).

3 Copiez le paquetage du programme d'installation téléchargé dans un répertoire temporaire.

4 Indiquez la commande suivante pour extraire les fichiers contenus dans le paquetage du programme d'installation :

```
unzip <install_filename>
```

Remplacez <*install_filename*> par le nom réel du fichier d'installation.

5 Accédez au répertoire à partir duquel vous avez extrait les fichiers du programme d'installation :

```
cd <directory_name>
```

Remplacez <*nom_répertoire*> par le nom effectif du répertoire dans lequel les fichiers ont été extraits.

6 Exécutez le programme d'installation, puis suivez les instructions qui s'affichent à l'écran :

```
./service_pack.sh
```

Windows

1 Loguez-vous en tant qu'administrateur à la machine exécutant les programmes clients de Novell Sentinel Rapid Deployment.

2 Téléchargez le programme d'installation du correctif pour Sentinel Rapid Deployment à partir du localisateur de correctifs Novell (http://download.novell.com/patch/finder/).

3 Copiez le fichier d'installation téléchargé dans un répertoire temporaire.

4 Extrayez les fichiers du paquetage du programme d'installation.

5 Accédez au répertoire dans lequel vous avez extrait les fichiers du programme d'installation.

6 Appliquez l'une des méthodes suivantes pour exécuter le programme d'installation :

- Double-cliquez sur le fichier `service_pack.bat`, puis suivez les instructions qui s'affichent à l'écran.
- À l'invite de commande, exécutez le fichier `service_pack.bat`, puis suivez les instructions qui s'affichent à l'écran.

Observations sur la sécurité de Sentinel Rapid Deployment

5

Cette section fournit des instructions spécifiques sur la sécurité de l'installation, de la configuration et de la maintenance de Novell Sentinel Rapid Deployment.

5.1 Renforcement de la sécurité

5.1.1 Renforcement de la sécurité prêt à l'emploi

- Tous les ports inutiles sont désactivés.
- Si possible, un port de service écoute uniquement les connexions locales et n'autorise pas les connexions à distance.
- Les fichiers sont installés avec les derniers privilèges de manière à ce que très peu d'utilisateurs puissent les lire.
- Les mots de passe par défaut ne sont pas autorisés.
- Les rapports relatifs à la base de données ne s'exécutent que lorsqu'un utilisateur dispose des autorisations appropriées.
- Toutes les interfaces Web nécessitent le protocole HTTPS.
- L'application est soumise à une analyse des vulnérabilités et tous les problèmes de sécurité potentiels sont traités.
- Toutes les communications réseau utilisent SSL par défaut et sont configurées en vue de l'authentification.
- Les mots de passe des comptes utilisateur sont codés par défaut lorsqu'ils sont stockés dans le système de fichiers ou la base de données.

5.1.2 Sécurisation des données de Sentinel Rapid Deployment

Les données du serveur Sentinel Rapid Deployment étant extrêmement sensibles, cette machine doit être sécurisée physiquement et placée dans un endroit sûr du réseau.Pour collecter les données des sources d'événements en dehors du réseau sécurisé, utilisez un gestionnaire des collecteurs distant. Pour plus d'informations sur les gestionnaires des collecteurs distants, reportez-vous à la « Section 3.3, « Installation du gestionnaire des collecteurs et des programmes clients », page 35 ».

5.2 Sécurisation de la communication réseau

La communication entre les différents composants de Sentinel Rapid Deployment s'effectue sur le réseau, à l'aide des différents types de protocoles de communication utilisés dans le système.

5.2.1 Communication entre les processus serveur de Sentinel

Le serveur Sentinel comprend DAS Core, DAS Binary, un moteur de corrélation, un gestionnaire des collecteurs et le serveur Web. Ils communiquent entre eux à l'aide d'ActiveMQ.

La communication entre ces processus serveur s'effectue par défaut sur SSL, par l'intermédiaire du bus de messages ActiveMQ. Pour configurer SSL, indiquez les informations suivantes dans le fichier `<répertoire_installation>/configuration.xml` :

```
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
```

Pour plus d'informations sur la configuration des certificats serveur et client personnalisés, reportez-vous à la section « Processus » du *Guide de l'utilisateur Sentinel Rapid Deployment*.

5.2.2 Communication entre le serveur Sentinel et les programmes clients Sentinel

Les programmes clients Sentinel tels que Sentinel Control Center (SCC), Sentinel Data Manager (SDM) et Solution Designer utilisent la communication SSL par défaut par l'intermédiaire du serveur proxy SSL.

Pour permettre la communication entre le serveur Sentinel et SCC, SDM et Solution Designer exécutés en tant que programmes clients sur le serveur, indiquez les informations suivantes dans le fichier `<répertoire_installation>/configuration.xml` :

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory">
   <transport type="ssl">
    <ssl host="localhost" keystore="<install_directory>/config/
.proxyClientKeystore" port="10013" usecacerts="false"/>
   </transport>
  </strategy>
```

Pour activer la communication entre le serveur Sentinel et SCC, SDM et Solution Designer exécutés via Web Start, la stratégie de communication est définie sur le serveur dans le fichier `<répertoire_installation>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml` de la manière suivante :

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory" >
   <transport type="ssl">
    <ssl host="127.0.0.1" port="10013" keystore="./.novell/sentinel/
.proxyClientKeystore" />
   </transport>
  </strategy>
```

Pour plus d'informations sur la configuration des certificats serveur et client personnalisés, reportez-vous à la section « Processus » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

5.2.3 Communication entre le serveur et la base de données

Le protocole utilisé pour la communication entre le serveur et la base de données est défini par le pilote JDBC. Certains pilotes peuvent coder la communication avec la base de données.

Sentinel Rapid Deployment utilise le pilote PostgreSQL (`postgresql-<version>.jdbc3.jar`) disponible sur la page de téléchargement PostgreSQL (http://jdbc.postgresql.org/download.html) pour établir la connexion à la base de données PostgreSQL, qui est une mise en œuvre Java (Type IV). Ce pilote prend en charge le codage de la communication des données. Pour configurer le codage de la communication des données, reportez-vous aux options de codage PostgreSQL (http://www.postgresql.org/docs/8.1/static/encryption-options.html).

Remarque : l'activation du codage a des conséquences sur les performances du système. C'est pourquoi, par défaut, les communications de la base de données ne sont pas codées. Il n'y a cependant aucun problème de sécurité car les communications entre la base de données et le serveur ont lieu au niveau de l'interface réseau en boucle et ne sont pas exposées au réseau ouvert.

5.2.4 Communication entre les gestionnaires des collecteurs et les sources d'événements

Vous pouvez configurer Sentinel pour collecter en toute sécurité les données de différentes sources d'événements. Toutefois, la collecte de données sécurisée est déterminée par les protocoles spécifiques pris en charge par la source d'événements. Par exemple, Check Point LEA, Syslog et Audit Connectors peuvent être configurés pour que leur communication avec les sources d'événements soit codée.

Pour plus d'informations sur les fonctionnalités de sécurité pouvant être activées, reportez-vous à la documentation du fournisseur des connecteurs et de la source d'événements, accessible sur le site Web de Novell Sentinel Plug-ins (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

5.2.5 Communication avec les navigateurs Web

Le serveur Web est configuré par défaut pour communiquer par l'intermédiaire du protocole HTTPS. Pour plus d'informations, reportez-vous à la documentation Tomcat (http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html).

5.2.6 Communication entre la base de données et d'autres clients

Vous pouvez configurer la base de données PostgreSQL SIEM afin d'établir la connexion depuis une machine cliente à l'aide de Sentinel Data Manager ou d'une application tierce telle que Pgadmin.

Pour que Sentinel Data Manager puisse se connecter depuis une machine cliente, ajoutez la ligne suivante dans le fichier `<répertoire_installation>/3rdparty/postgresql/data/pg_hba.conf` :

```
host    all         all         0.0.0.0/0             md5
```

Si vous souhaitez limiter les connexions des clients qui sont autorisés à se connecter à la base de données par l'intermédiaire de SDM et à l'exécuter, remplacez la ligne ci-dessus par l'adresse IP de l'hôte. La ligne suivante du fichier `pg_hba.conf` est un indicateur permettant à PostgreSQL d'accepter les connexions de la machine locale, de manière à ce que le gestionnaire de données Sentinel ne puisse s'exécuter que sur le serveur.

```
host all all 127.0.0.1/32 md5
```

Pour limiter les connexions depuis les autres machines clientes, vous pouvez ajouter des entrées `host` supplémentaires.

5.3 Sécurisation des utilisateurs et des mots de passe

5.3.1 Utilisateurs du système d'exploitation

Installation des serveurs

L'installation du serveur Sentinel Rapid Deployment crée un utilisateur et un groupe système qui sont les propriétaires des fichiers installés dans le répertoire *<répertoire_installation>*. Si l'utilisateur n'existe pas, il est créé et son répertoire privé est défini sur *<répertoire_installation>*. Si un nouvel utilisateur est créé, son mot de passe n'est pas défini par défaut afin d'optimiser la sécurité. Si vous souhaitez vous loguer au système avec les références de l'utilisateur créé lors de l'installation, vous devez définir son mot de passe après l'installation.

Installation du gestionnaire des collecteurs

Le niveau de sécurité des utilisateurs peut varier en fonction du système d'exploitation sur lequel le gestionnaire des collecteurs est installé.

Linux : le programme d'installation vous invite à indiquer le nom de l'utilisateur système qui est le propriétaire des fichiers installés, ainsi que l'emplacement de création de son répertoire privé. Par défaut, l'utilisateur système est `esecadm`, mais vous pouvez le renommer. Si l'utilisateur n'existe pas, il est créé, ainsi que son répertoire privé. Si un nouvel utilisateur est créé, son mot de passe n'est pas défini lors de l'installation afin d'optimiser la sécurité. Si vous souhaitez vous loguer au système avec les références de l'utilisateur, vous devez définir son mot de passe après l'installation. Le groupe par défaut est `esec`.

Au cours de l'installation du client, si l'utilisateur existe, le programme d'installation ne redemande pas de l'indiquer. Ce comportement est semblable à celui qui se produit pendant la désinstallation et la réinstallation du logiciel. Si vous souhaitez que le programme d'installation demande de nouveau d'indiquer l'utilisateur, procédez comme suit :

1. Supprimez l'utilisateur et le groupe créés lors de la première installation.
2. Supprimez les variables d'environnement ESEC_USER à partir de `/etc/profile`.

Windows : aucun utilisateur n'est créé.

Les stratégies de mot de passe des utilisateurs système sont définies par le système d'exploitation utilisé.

5.3.2 Utilisateurs d'applications et de bases de données Sentinel

Tous les utilisateurs des applications Sentinel Rapid Deployment sont des utilisateurs des bases de données natives et leurs mots de passe sont protégés par l'utilisation de procédures, suivies de la plate-forme des bases de données natives. Ces utilisateurs n'ont qu'un accès en lecture seule à certaines tables de la base de données et peuvent interroger cette dernière.

Le programme d'installation crée et configure une base de données PostgreSQL avec les utilisateurs suivants :

- **admin :** l'utilisateur admin est l'administrateur de toutes les applications Sentinel auxquelles il se logue.
- **dbauser:** l'utilisateur dbauser est créé en tant que superutilisateur qui peut gérer la base de données. Le mot de passe de l'utilisateur dbauser est défini au moment de l'installation du serveur Sentinel Rapid Deployment. Ce mot de passe est stocké dans le fichier `<répertoire`

`privé de l'utilisateur>/.pgpass`. Le système suit les stratégies relatives aux mots de passe de bases de données PostgreSQL. Pour plus d'informations, reportez-vous à la Section 5.3.3, « Application des stratégies de mot de passe pour les utilisateurs », page 64.

- **appuser :** appuser est l'utilisateur non-superutilisateur utilisé par toutes les applications Sentinel pour établir la connexion à la base de données. Par défaut, l'utilisateur appuser utilise un mot de passe généré de façon aléatoire lors de l'installation, qui est stocké et codé dans les fichiers XML (`das_core.xml`, `das_binary.xml` et `advisor_client.xml`) dans le répertoire <*répertoire_installation*>/config. Pour changer le mot de passe de l'utilisateur appuser, employez l'utilitaire `<répertoire_installation>/bin/dbconfig`. Pour plus d'informations, reportez-vous à la section « Fichiers du conteneur DAS » du *Guide de référence de Sentinel Rapid Deployment*.

Remarque : il existe également un utilisateur de base de données PostgreSQL propriétaire de l'intégralité de la base de données, y compris des tables de la base de données système. Par défaut, l'utilisateur de la base de données PostgreSQL est défini sur NOLOGIN de manière à ce qu'aucun utilisateur ne puisse se loguer en tant qu'utilisateur PostgreSQL.

5.3.3 Application des stratégies de mot de passe pour les utilisateurs

Sentinel Rapid Deployment utilise des mécanismes basés sur des normes pour faciliter l'application des stratégies de mot de passe.

Le programme d'installation crée et configure une base de données PostgreSQL avec les utilisateurs suivants :

dbauser : propriétaire de la base de données (utilisateur administrateur de la base de données). Son mot de passe est défini lors du processus d'installation.

appuser : l'utilisateur d'applications servant à se loguer à la base de données depuis Sentinel Rapid Deployment. Le mot de passe est généré de manière aléatoire lors du processus d'installation et est réservé à une utilisation interne uniquement.

admin : les références de l'administrateur peuvent être utilisées pour se loguer à l'interface Web de Sentinel Rapid Deployment. Son mot de passe est défini lors du processus d'installation.

Par défaut, les mots de passe utilisateur sont stockés dans la base de données PostgreSQL, intégrée à Sentinel Rapid Deployment. PostgreSQL permet d'utiliser plusieurs mécanismes d'authentification basés sur des normes, tels que décrits dans la section Authentification des clients (http://www.postgresql.org/docs/8.3/static/client-authentication.html) de la documentation PostgreSQL.

L'utilisation de ces mécanismes affecte tous les comptes utilisateur de Sentinel Rapid Deployment, y compris les utilisateurs d'applications Web et les comptes utilisés uniquement par les services principaux, comme `dbauser` et `appuser`.

Il est plus simple d'utiliser un annuaire LDAP pour authentifier les utilisateurs d'applications Web. Pour activer cette option sur le serveur Sentinel Rapid Deployment, reportez-vous à la Section 3.7, « Authentification LDAP », page 45. Cette option n'affecte pas les comptes utilisés par les services principaux, qui continuent à procéder aux authentifications via PostgreSQL, sauf si vous avez modifié les paramètres de configuration de PostgreSQL.

Vous pouvez appliquer la stratégie de mot de passe de Sentinel Rapid Deployment de façon rigoureuse en utilisant à la fois ces mécanismes basés sur des normes et les mécanismes existant dans votre environnement, comme votre annuaire LDAP.

5.4 Sécurisation des données Sentinel

Important : les données du serveur Sentinel étant extrêmement sensibles, cette machine doit être sécurisée physiquement et placée dans un endroit sûr du réseau.Pour collecter les données des sources d'événements en dehors du réseau sécurisé, utilisez un gestionnaire des collecteurs distant.

Les mots de passe de certains composants doivent être stockés pour être disponibles lorsque le système doit se connecter à une ressource telle que la base de données ou une source d'événements. Dans ce cas, lorsque le mot de passe est stocké, il est d'abord codé pour empêcher tout accès non autorisé au mot de passe en texte clair.

Même si le mot de passe est codé, veillez à ce que l'accès aux données du mot de passe stocké soit protégé pour éviter toute exposition. Vous pouvez vérifier par exemple que les autorisations sur les fichiers contenant des données sensibles ne sont pas lisibles par des utilisateurs non autorisés.

Fichiers

`advisor_client.xml`

Référence de base de données

Les références de la base de données sont stockées dans le fichier *<répertoire_installation>*`/config/server.xml`.

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Références d'Advisor

```
<obj-component id="DownloadComponent">
          <class>esecurity.ccs.comp.advisor.feed.NewAdvClientDownload</class>
      <property name="advisor.downloadfrom.url">https://secure-www.novell.com/
sentinel/advisor/advisordata</property>
      <property name="username">admin</property>
      <!-- Set the password (encrypted) using the adv_change_password script -
->
      <property name="password">jqhlWIX8HD6GDHVX9FApWg==</property>
<property name="compression.enabled">true</property>
      <!--
        Set the following properties to connect through an HTTP proxy.
       Set the proxy password (encrypted) using the adv_change_password script
(make a
        copy of the script and add "-x" to the java cmd line to set the proxy
password
        instead of the advisor password.
      -->
```

```
      <!--
      <property name="proxy_host"></property>
      <property name="proxy_port"></property>
      <property name="proxy_username"></property>
      <property name="proxy_password"></property>
      -->
        </obj-component>
```

Configuration.xml

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.Ac
tiveMQStrategyFactory" name="ActiveMQ">
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
    </strategy>
```

das_binary.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

das_core.xml

```
 <class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Certaines tables de la base de données stockent des mots de passe et des certificats. Ces données sensibles sont codées et stockées dans les tables répertoriées ci-dessous. Vous devez limiter l'accès à ces tables.

- **evt_src :** données de la colonne evt_src_config
- **evt_src_collector :** colonnes : evt_src_collector_props
- **evt_src_grp (doute) :** colonnes : evt_src_default_config
- **MD_CONFIG :** colonne : données
- **integrator_config :** colonne : integrator_properties
- **md_view_config :** colonne : view_data
- **esec_content :** colonne : content_context, content_hash
- **esec_content_grp_content :** colonnes : content_hash
- **sentinel_plugin :** colonnes : content_pkg, file_hash

Sentinel Rapid Deployment stocke les données de configuration et d'événements. Ces données sont stockées dans les emplacements suivants :

Composants	Emplacement des données de configuration	Emplacement des données d'événements
Serveur Sentinel Rapid Deployment	Tables de base de données et système de fichiers (<*répertoire_installation*>/config) Ces informations de configuration comprennent la base de données code, la source d'événements, les intégrateurs et les mots de passe.	Base de données (tables EVENTS, CORRELATED_EVENTS, EVT_SMRY_ et AUDIT_RECORD) et système de fichiers aux emplacements <*répertoire_installation*>/data/eventdata et <*répertoire_installation*>/data/raw data Les données d'événements peuvent être archivées dans le système de fichiers dans le cadre de la gestion des partitions.
Moteur de corrélation	Système de fichiers (<*répertoire_installation*>/config). La seule information de configuration sensible est la paire de clés client utilisée pour établir la connexion au bus de messages.	correlation_engine.cache
DAS Core	<*répertoire_installation*>/config	das_core.cache
DAS Binary	<*répertoire_installation*>/config	Les données d'événements peuvent être mises en cache si la base de données est arrêtée. das_binary.cache
Gestionnaire des collecteurs	Système de fichiers (<*répertoire_installation*>/config). La seule information de configuration sensible est le mot de passe utilisateur du gestionnaire des collecteurs permettant d'établir la connexion au bus de messages.	Les données d'événements peuvent être mises en cache dans le système de fichiers dans des situations d'erreur : bus de messages arrêté ou débordement d'événements. Ces données d'événements sont stockées dans le répertoire <*répertoire_installation*>/data/collector_mgr.cache.

Composants	Emplacement des données de configuration	Emplacement des données d'événements
Programmes clients	Système de fichiers (*répertoire_installation*/config). Les programmes clients ne stockent pas d'informations sensibles dans les fichiers de configuration.. Par exemple, les programmes clients peuvent exporter des données ESM dans un système de fichiers local. Le fichier exporté contient des mots de passe codés s'ils sont présents dans la configuration des sources d'événements exportées. Les mots de passe sont codés, mais l'autorisation d'exportation ESM ne doit être accordée qu'aux utilisateurs approuvés et disposant de ce privilège.	Aucun

5.5 Sauvegarde des informations

- Vous devez sauvegarder les événements régulièrement. Le support de sauvegarde doit être stocké dans un lieu sécurisé, en dehors du site.
- Sauvegardez les données système. Pour plus d'informations, reportez-vous à la section sur l'« utilitaire de sauvegarde et de restauration » dans le *Guide de l'utilisateur de Sentinel Rapid Deployment*.
- Pour les données sensibles, utilisez l'une des méthodes suivantes pour coder la sauvegarde des données :
  - Codez les données proprement dites si l'application de création des données prend en charge le codage. C'est le cas notamment des produits de base de données et des outils tiers. Utilisez un logiciel de sauvegarde pouvant coder les données au moment de la sauvegarde. Cette méthode a une incidence sur les performances et la facilité d'utilisation du système, notamment en ce qui concerne la gestion des clés de codage.
  - Utilisez un applicatif pour coder le support de sauvegarde des données sensibles lors de la sauvegarde.
- Si vous transportez le support et le stockez en dehors du site, utilisez une entreprise spécialisée dans l'expédition et le stockage des supports. Veillez à ce que les bandes soient identifiées par des codes barres, qu'elles soient stockées dans des conditions respectueuses de l'environnement et gérées par une entreprise réputée pour gérer les supports correctement.
- Chargez les certificats de récupération. Le service Sentinel de Novell par défaut n'est pas configuré pour l'agent de récupération. Au cours de la configuration du serveur par l'intermédiaire du système YaST, veillez à ce que le chemin de l'agent de récupération soit configuré. Ce chemin doit contenir la liste des certificats que le service peut charger et dans laquelle les utilisateurs peut sélectionner un élément.

Pour plus d'informations, reportez-vous à « Gestion des certificats pour le serveur Sentinel 6.1 Rapid Deployment » dans le *Guide de référence de Sentinel Rapid Deployment*.

YaST contient des modules pour la gestion de base des certificats X.509, qui implique principalement la création d'autorités et de sous-autorités de certification, ainsi que de leurs certificats. Pour plus d'informations sur la gestion et la mise à jour des certificats, reportez-vous à la section Managing X.509 Certification (Gestion de la certification X.509) (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html) du manuel*SUSE Linux Enterprise Server 10 Installation and Administration Guide (Guide d'installation et d'administration du SUSE Linux Enterprise Server 10)* (http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html).

5.6 Sécurisation du système d'exploitation

- Sentinel Rapid Deployment est pris en charge par SUSE Linux Enterprise Server (SLES) 10 SP3 ou version ultérieure. Pour plus d'informations sur la sécurisation d'une machine SLES, reportez-vous à ladocumentation de SUSE Linux Enterprise Server 10 (http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html).
- Sécurisez l'accès au serveur Sentinel Rapid Deployment à l'aide d'un pare-feu. Si le serveur Sentinel est accessible à l'extérieur du réseau de l'entreprise, utilisez un pare-feu pour empêcher tout accès direct par un intrus.

  Activez les ports du pare-feu suivants :

Composants	Port
ActiveMQ	61616
PostgreSQL	5432
Tomcat	8443
Port du client proxy de Sentinel Control Center	10013
Client approuvé proxy	10014
internal_gateway_server and internal_gateway Utilisé entre le moteur et le gestionnaire	5556
internal_router_server et internal_router_client Utilisé entre le serveur et le client du routeur d'événements	5558
Port d'écoute d'événements Configuré dans `config/collector_mgr.properties` comme “`esecurity.agentmanager.event.port`”	35 000

Remarque : les ports marqués d'un astérisque peuvent être différents s'ils étaient déjà utilisés au moment de l'installation. Si c'est le cas, utilisez les numéros de port demandés lors de l'installation.

Pour plus d'informations sur l'activation d'un pare-feu sur SLES 10, reportez-vous à la section Configuring Firewalls with YaST (Configuration de pare-feu avec YaST) (http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html) du manuel *SLES 10 Administration Guide (Guide d'administration de SLES 10)*.

5.7 Affichage des événements d'audit Sentinel

Sentinel Rapid Deployment génère des événements d'audit pour de nombreuses opérations effectuées par les utilisateurs et pour des opérations réalisées en interne pour des activités système. Ces événements peuvent être affichés dans Active Views ou sont accessibles par l'intermédiaire d'une recherche ou d'un rapport. Vous devez cependant disposer des autorisations nécessaires pour afficher les événements système.

Pour plus d'informations, reportez-vous à la section consacrée aux « événements système de Sentinel » dans le *Guide de l'utilisateur de Sentinel Rapid Deployment*.

5.8 Utilisation de certificats signés par des autorités de certification

Vous pouvez remplacer le certificat auto-signé par un certificat signé par une autorité de certification réputée telle que VeriSign, Thawte ou Entrust. Vous pouvez également remplacer le certificat auto-signé par un certificat signé par une autorité de certification moins connue, telle que l'autorité de votre entreprise ou de votre organisation.

Pour plus d'informations, reportez-vous à « Gestion des certificats pour le serveur Sentinel 6.1 Rapid Deployment » dans le *Guide de référence de Sentinel Rapid Deployment*.

Test des fonctionnalités de Sentinel Rapid Deployment

6

Sentinel Rapid Deployment est installé avec un collecteur générique qui permet de tester de nombreuses fonctions de base du système. Vous pouvez utiliser ce collecteur pour tester les affichages Active Views, la création d'incidents, les règles de corrélation et les rapports.

6.1 Test de l'installation de Rapid Deployment

La procédure suivante décrit les étapes à suivre pour tester le système Sentinel Rapid Deployment 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 confirmer ce qui suit :

- Les services Sentinel sont fonctionnels.
- La communication via le bus de messages est fonctionnelle.
- Des événements d'audit interne sont envoyés.
- Des événements peuvent être envoyés à partir d'un gestionnaire des collecteurs.
- Les événements sont insérés dans la base de données et peuvent être récupérés à l'aide d'un rapport.
- Il est possible de créer et de visualiser des incidents.
- Les règles sont évaluées et le moteur de corrélation déclenche les événements corrélés.
- Le gestionnaire de données Sentinel se connecte à la base de données et lit les informations de partition.

Si l'un de ces tests échoue, consultez le journal d'installation et les autres fichiers journaux et contactez le Support technique de Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup), si nécessaire.

Pour tester l'installation :

1. Loguez-vous à l'interface Web de Sentinel Rapid Deployment.

   Pour plus d'informations, reportez-vous à la section « Accès à l'interface Web de Novell Sentinel » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

2. Sélectionnez la page Rechercher, puis recherchez un événement interne. Un ou plusieurs événements doivent être renvoyés.

   Par exemple, pour rechercher des événements internes avec un niveau de gravité compris entre 3 et 5, sélectionnez *Inclure les événements système*, puis saisissez *sev:[3 TO 5]* dans le champ *Rechercher*.

Pour plus d'informations, reportez-vous à la section « Exécution d'une recherche d'événements » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

Par défaut, la fonctionnalité de recherche n'est pas activée dans SP2. Cependant, si vous souhaitez activer cette fonctionnalité, reportez-vous à la section « Activation de l'option de recherche dans l'interface utilisateur Web » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

3 Sélectionnez la page Rapports, spécifiez les paramètres, puis exécutez un rapport.

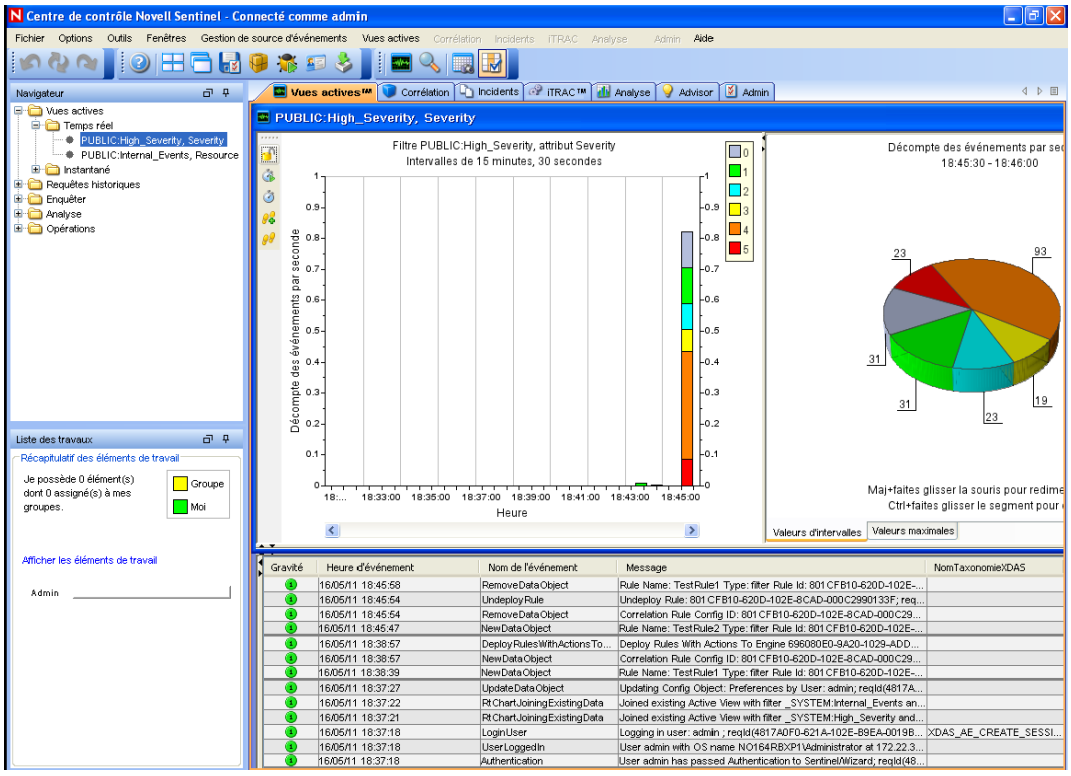
Par exemple, cliquez sur le bouton *Exécuter* en regard de Configuration d'événements Sentinel Core, spécifiez les paramètres souhaités, puis cliquez sur *Exécuter*.

Pour plus d'informations, reportez-vous à la section « Exécution de rapports » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

4 Dans la page Applications, cliquez sur *Démarrer Sentinel Control Center*.

5 Loguez-vous au système en tant qu'administrateur Sentinel spécifié durant l'installation (par défaut, admin).

Sentinel Control Center s'ouvre et affiche l'onglet *Active Views* qui présente les événements filtrés par les filtres publics *Internal_Events* et *High_Severity*.



6 Accédez au menu *Gestion de source d'événements*, puis sélectionnez *Vue en direct*.

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

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

9 Cliquez sur l'onglet *Active Views*.

Vous pouvez afficher la fenêtre active portant le titre PUBLIC: High_Severity, Severity. Vous devrez peut-être attendre un certain temps avant que le collecteur démarre et que les données apparaissent dans la fenêtre.

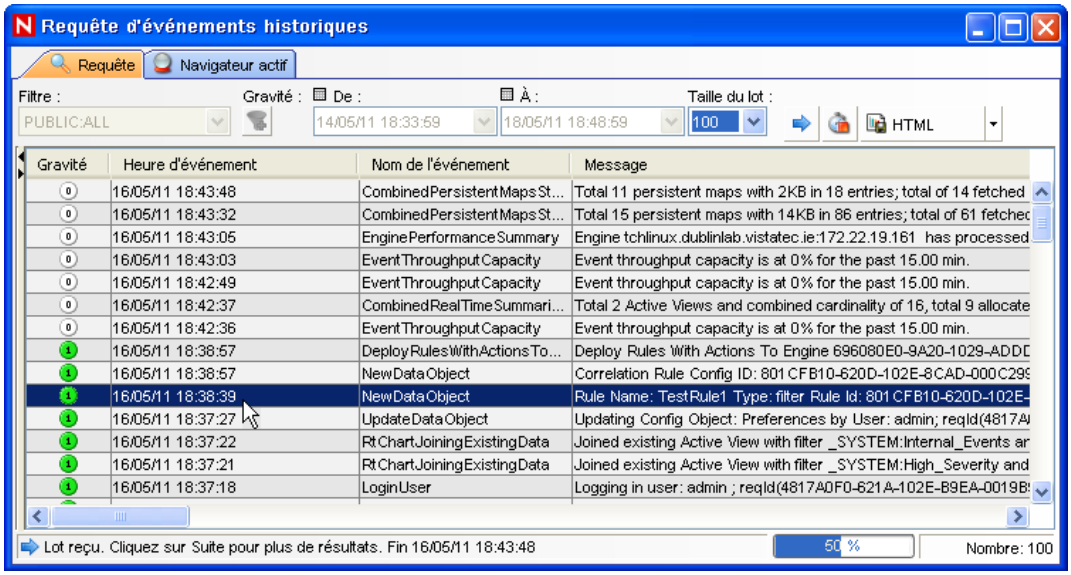
10 Cliquez sur le bouton *Requête d'événement* dans la barre d'outils. La fenêtre Requête d'événements historiques s'affiche.

11 Dans cette fenêtre, cliquez sur la flèche vers le bas *Filtre* pour sélectionner le filtre. Sélectionnez le filtre *Public: All*.

12 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*.

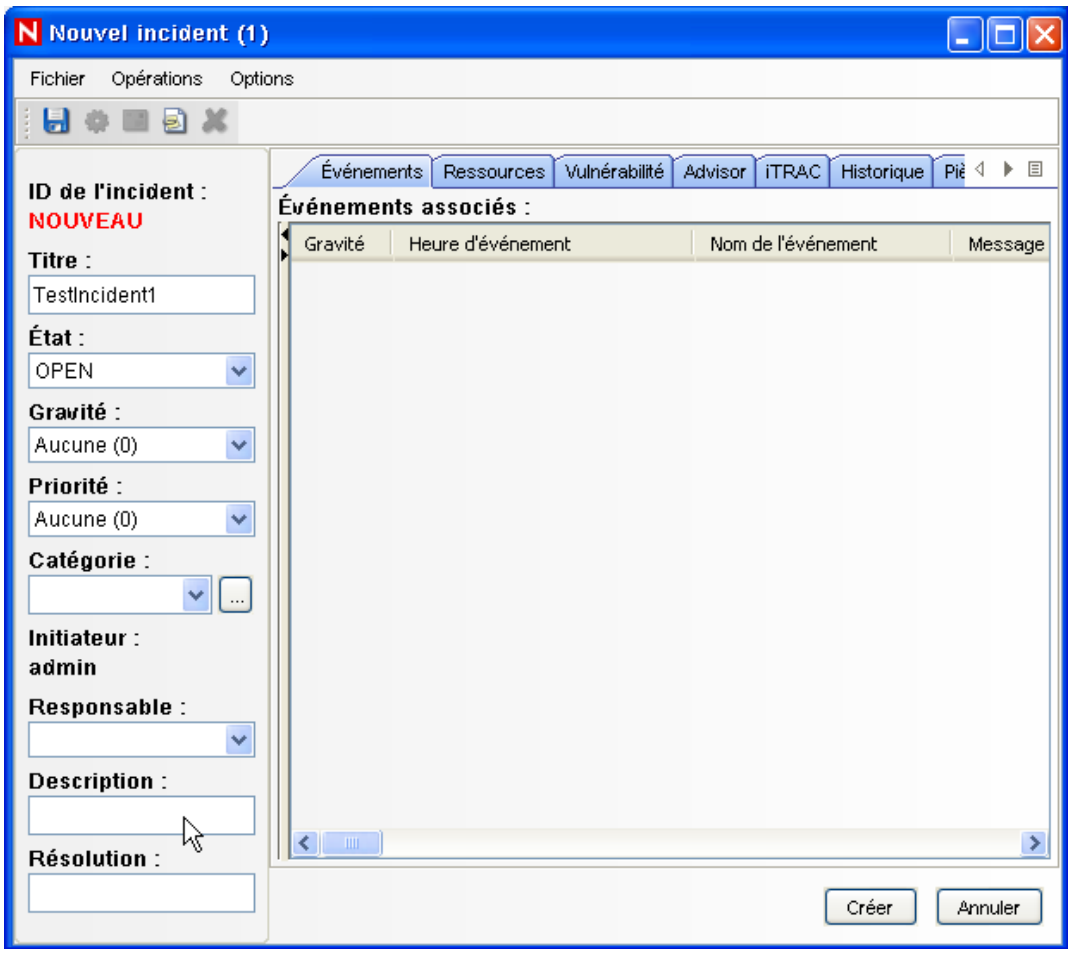
13 Sélectionnez une taille de lot.

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



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

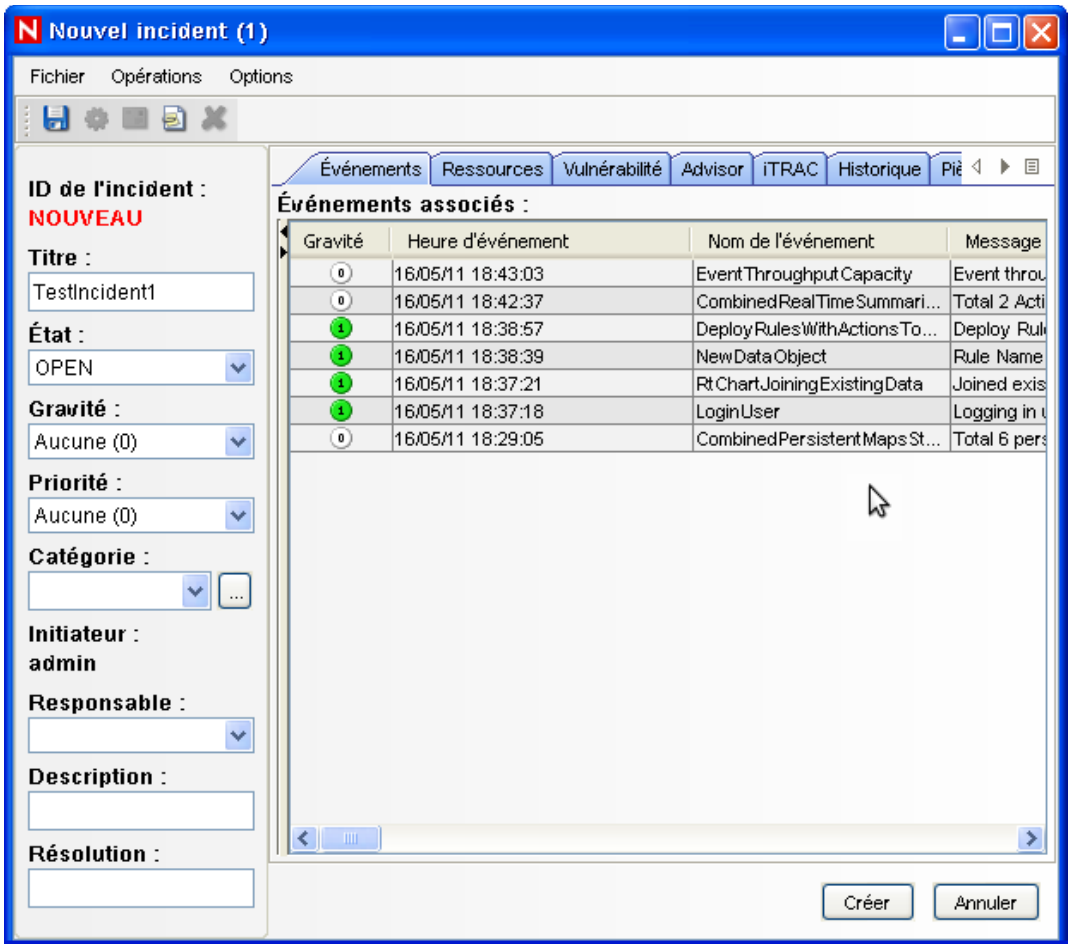
16 Cliquez avec le bouton droit dans la fenêtre, puis sélectionnez *Créer un incident* pour afficher la fenêtre Nouvel incident.



17 Nommez l'incident TestIncident1, puis cliquez sur *Créer*. Une notification de réussite s'affiche. Cliquez sur *Enregistrer*.

18 Cliquez sur l'onglet *Incidents* pour afficher l'incident que vous venez de créer dans le gestionnaire de vues d'incidents.

19 Double-cliquez sur l'incident pour afficher les événements.



20 Fermez la fenêtre Incidents.

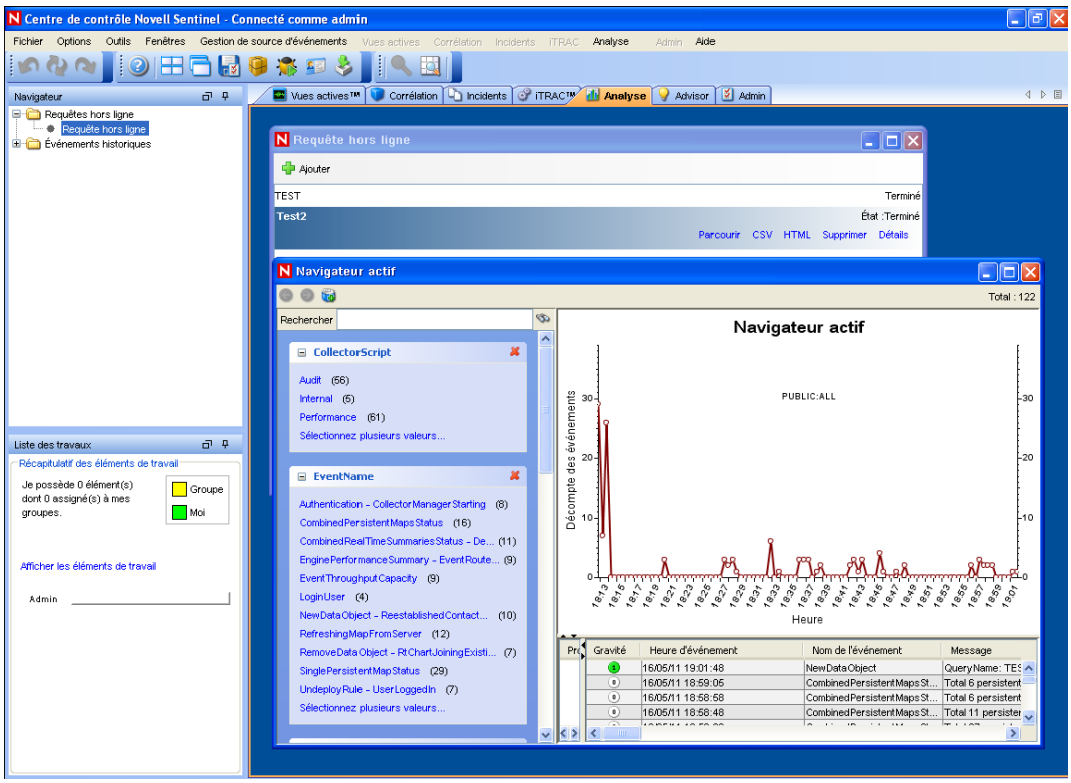
21 Cliquez sur l'onglet *Analyse*.

22 Cliquez sur *Requêtes hors ligne* dans le menu *Analyse* ou depuis le navigateur.

23 Dans la fenêtre Requêtes hors ligne, cliquez sur *Ajouter*.

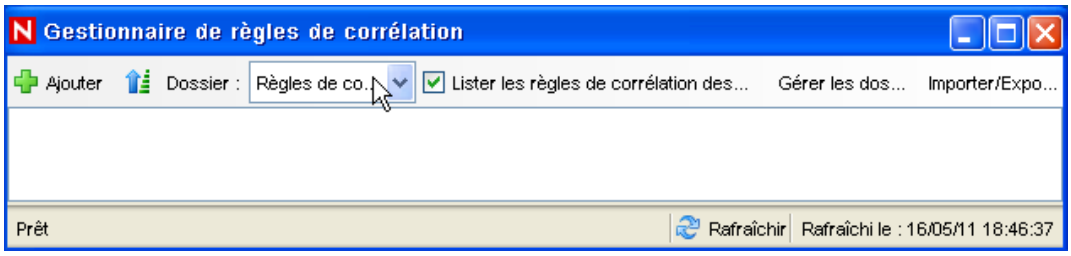
24 Spécifiez un nom, sélectionnez un filtre, sélectionnez une période et cliquez sur *OK*.

25 Cliquez sur *Parcourir* pour afficher la liste des événements et les détails associés dans la fenêtre de navigateur actif.

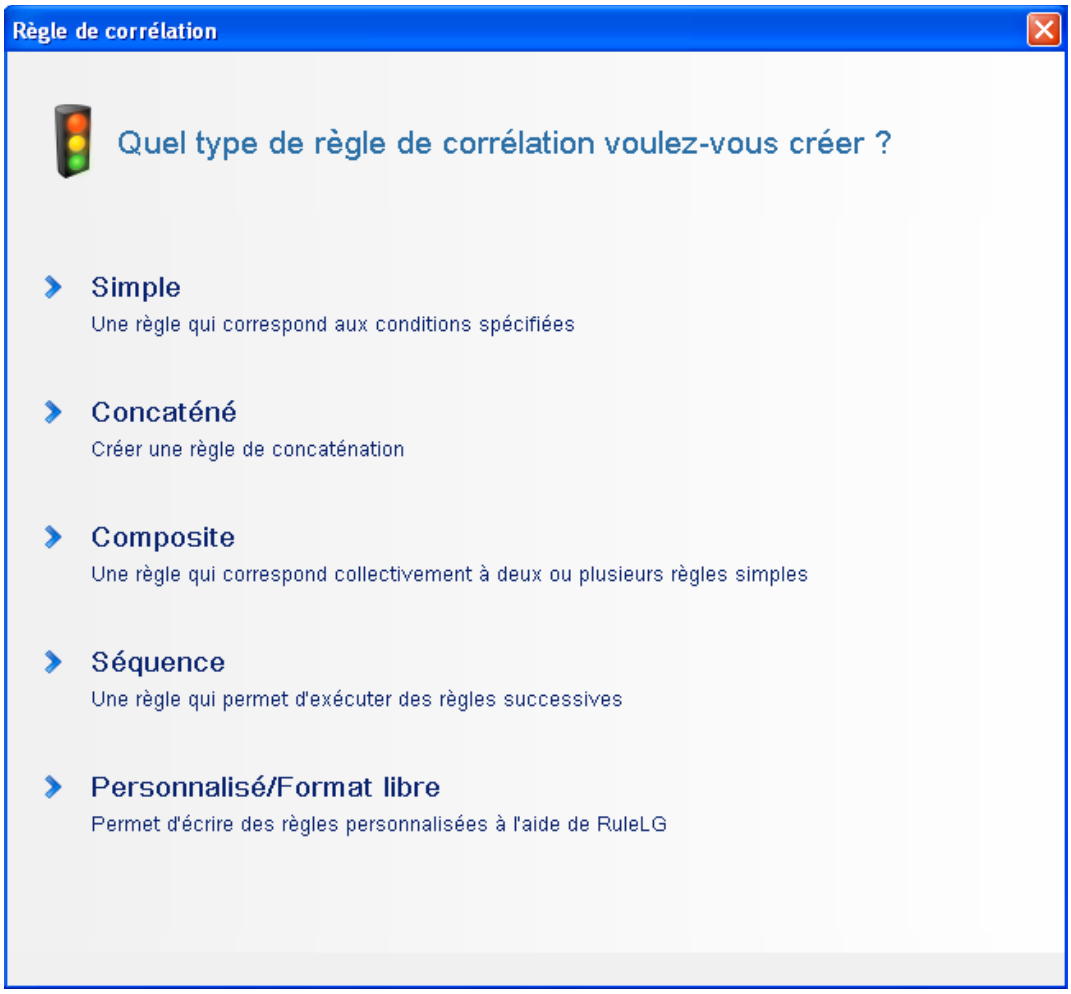


Vous pouvez afficher les détails suivants : collecteur, adresse IP cible, gravité, port de service cible et ressource.

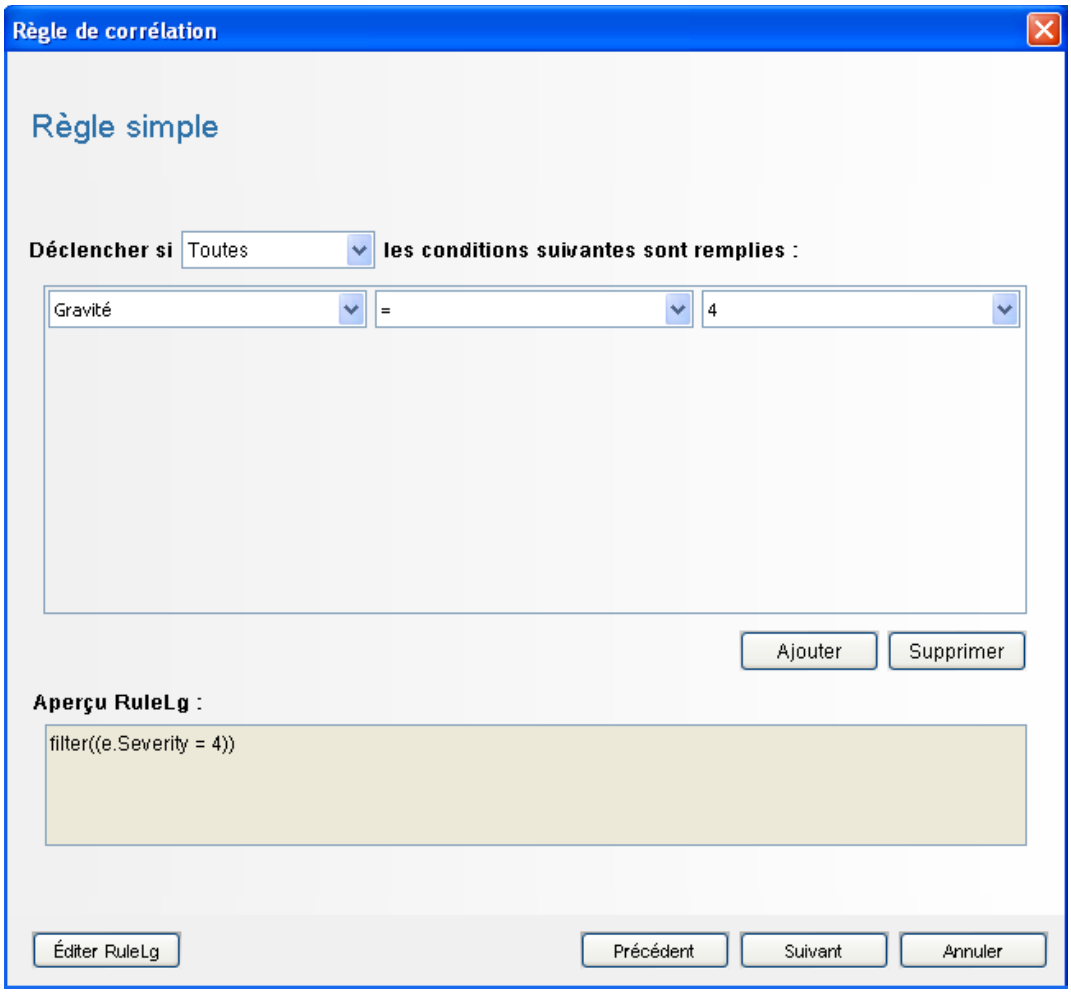
26 Sélectionnez l'onglet *Corrélation*. Le gestionnaire de règles de corrélation s'affiche.



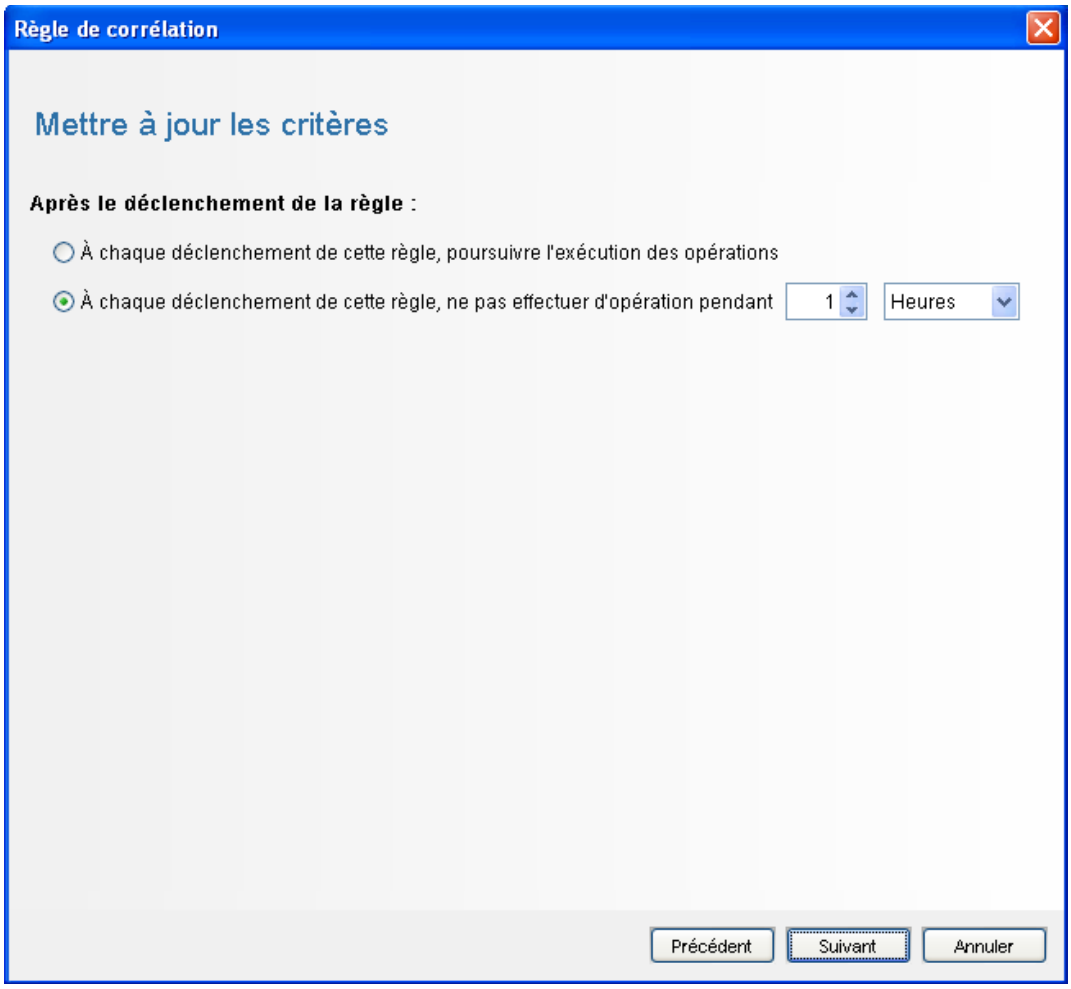
27 Cliquez sur *Ajouter*. L'Assistant de règles de corrélation s'affiche.



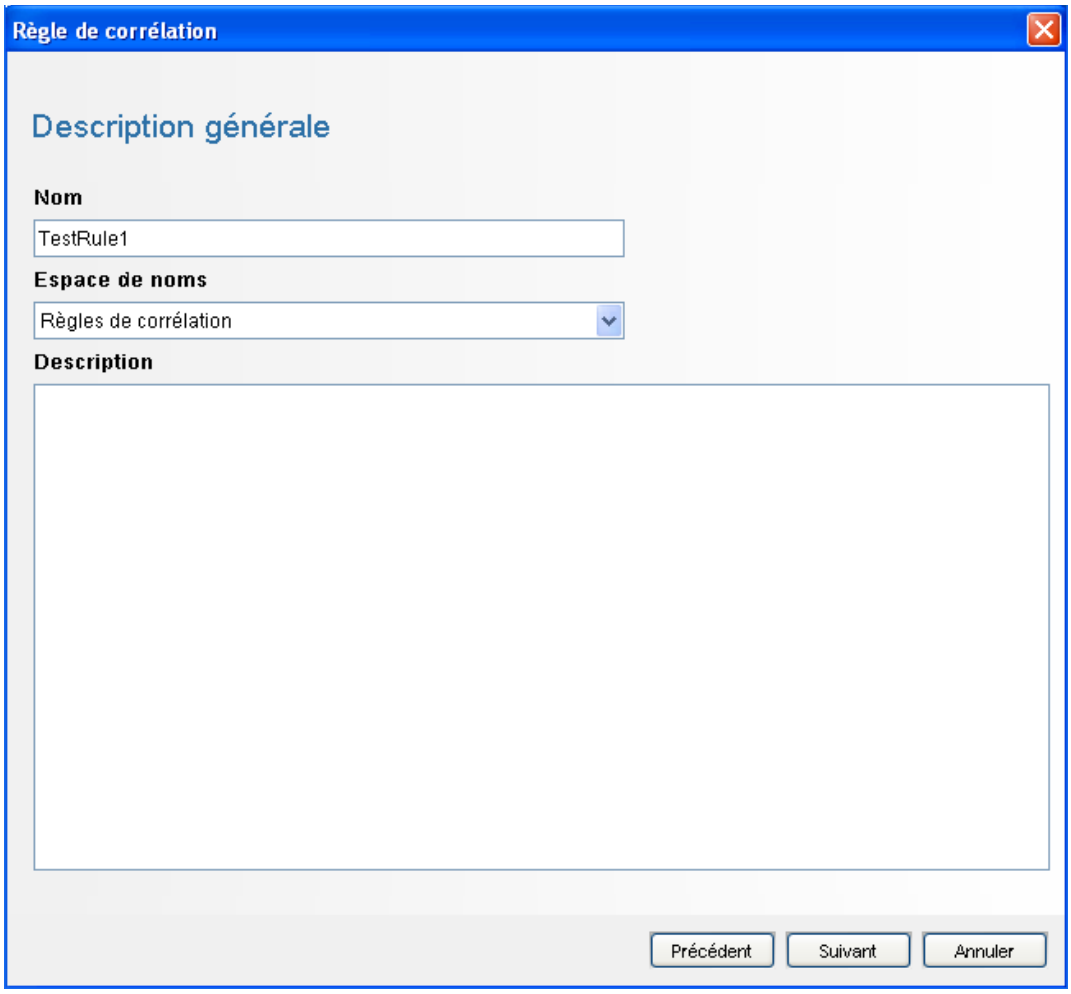
28 Cliquez sur *Simple*. La fenêtre Règle simple s'affiche.



29 Utilisez les menus déroulants pour définir le critère de gravité sur 4, puis cliquez sur *Suivant*. La fenêtre Mettre à jour les critères s'affiche.



30 Sélectionnez *Ne pas effectuer d'opération à chaque déclenchement de cette règle pendant* et définissez la période sur 1 minute à l'aide du menu déroulant, puis cliquez sur *Suivant*. La fenêtre Description générale s'affiche.



31 Nommez la règle *TestRule1*, entrez une description et cliquez sur *Suivant*.

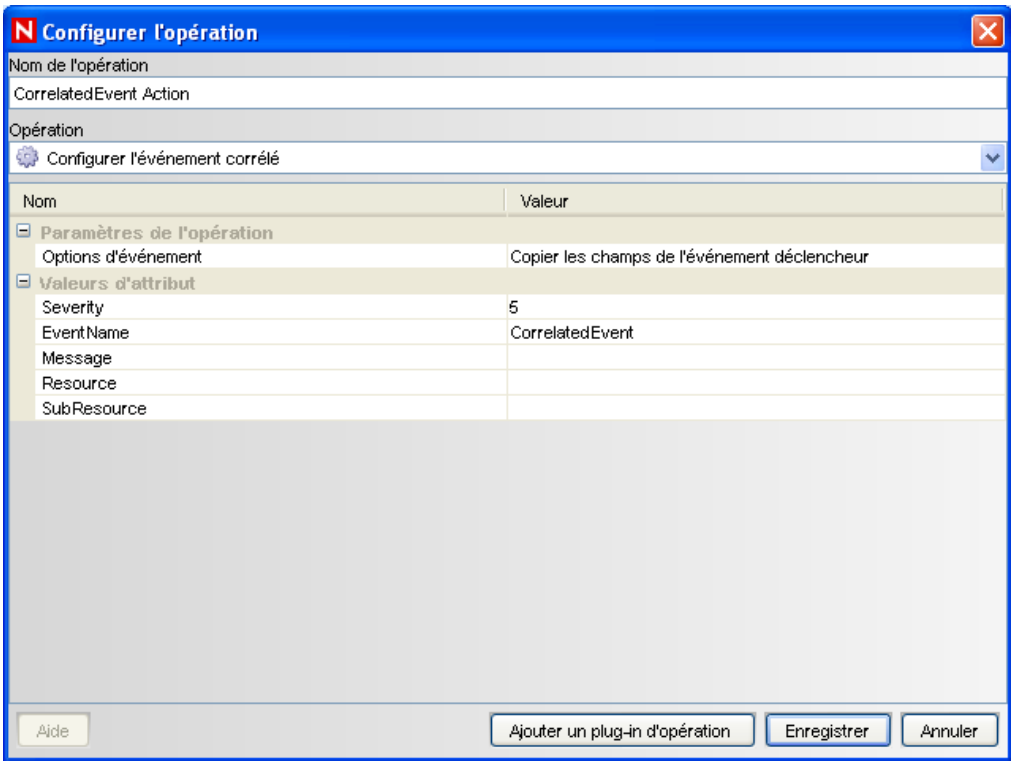
32 Sélectionnez *Non, ne pas créer d'autre règle* et cliquez sur *Suivant*.

33 Créez une opération à associer à la règle que vous avez créée.

33a Effectuez l'une des opérations suivantes :

- Sélectionnez *Outils* > *Gestionnaire d'opérations* > *Ajouter*.
- Dans la fenêtre Déployer la règle, cliquez sur *Ajouter une opération*. Pour plus d'informations, reportez-vous à l'Étape 34 à l'Étape 35 page 81.

La fenêtre Configurer une opération s'affiche.



33b Dans la fenêtre Configurer une opération, spécifiez les éléments suivants :

- Spécifiez le nom de l'opération (CorrelatedEvent, par exemple).
- Sélectionnez *Configurer un événement corrélé* dans la liste déroulante *Opération*.
- Définissez les *options d'événements*.
- Définissez le niveau de *gravité* sur 5.
- Spécifiez le *nom de l'événement* (CorrelatedEvent, par exemple).
- Spécifiez un message, le cas échéant.

Pour plus d'informations sur la création d'opérations, reportez-vous à la section « Création d'opérations » du *Guide de l'utilisateur de Sentinel Rapid Deployment*.

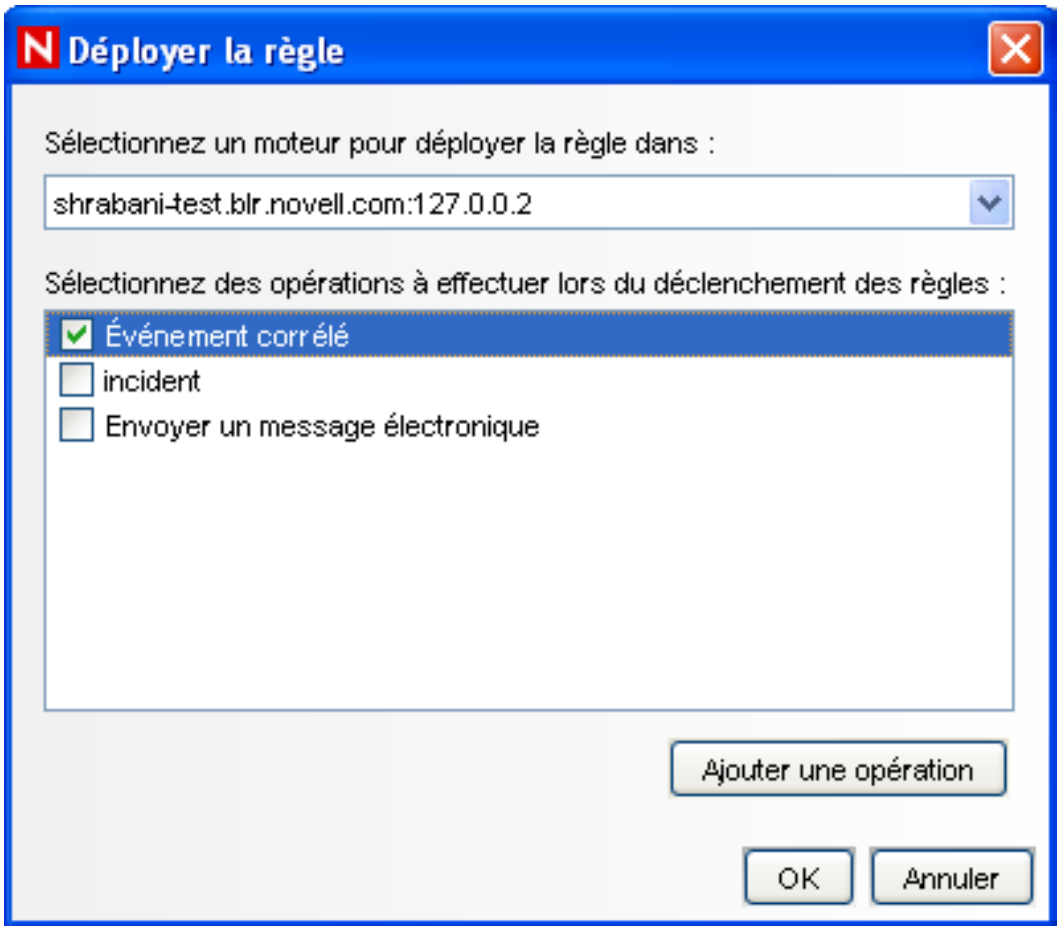
33c Cliquez sur *Enregistrer*.

34 Ouvrez la fenêtre Gestionnaire de règle de corrélation.

35 Sélectionnez une règle, puis cliquez sur le lien *Déployer les règles*. La fenêtre Déployer la règle s'affiche.

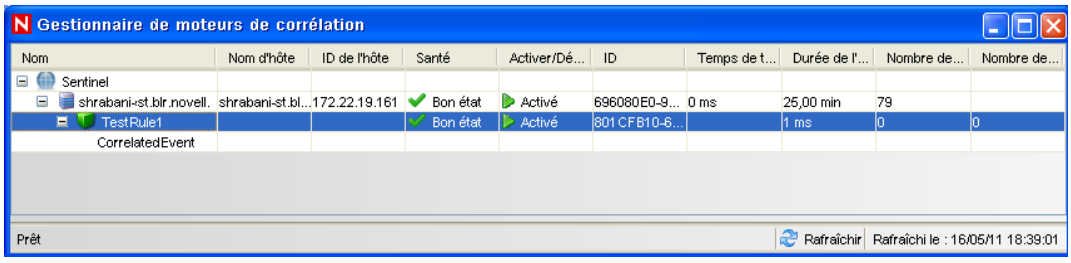
36 Dans la fenêtre Déployer la règle, sélectionnez le moteur à utiliser pour déployer la règle.

37 Sélectionnez l'opération que vous avez créée dans Étape 33 page 80 pour l'associer à la règle, puis cliquez sur *OK*.



38 Sélectionnez le *gestionnaire de moteurs de corrélation*.

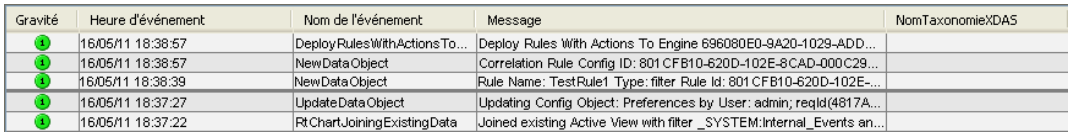
Sous le moteur de corrélation, vous pouvez voir que la règle est déployée et activée.



39 Déclenchez un événement de sécurité 4, comme une authentification échouée, pour activer la règle de corrélation déployée.

Pour générer un tel événement, ouvrez par exemple une fenêtre de login de Sentinel Control Center, puis spécifiez des références utilisateur erronées.

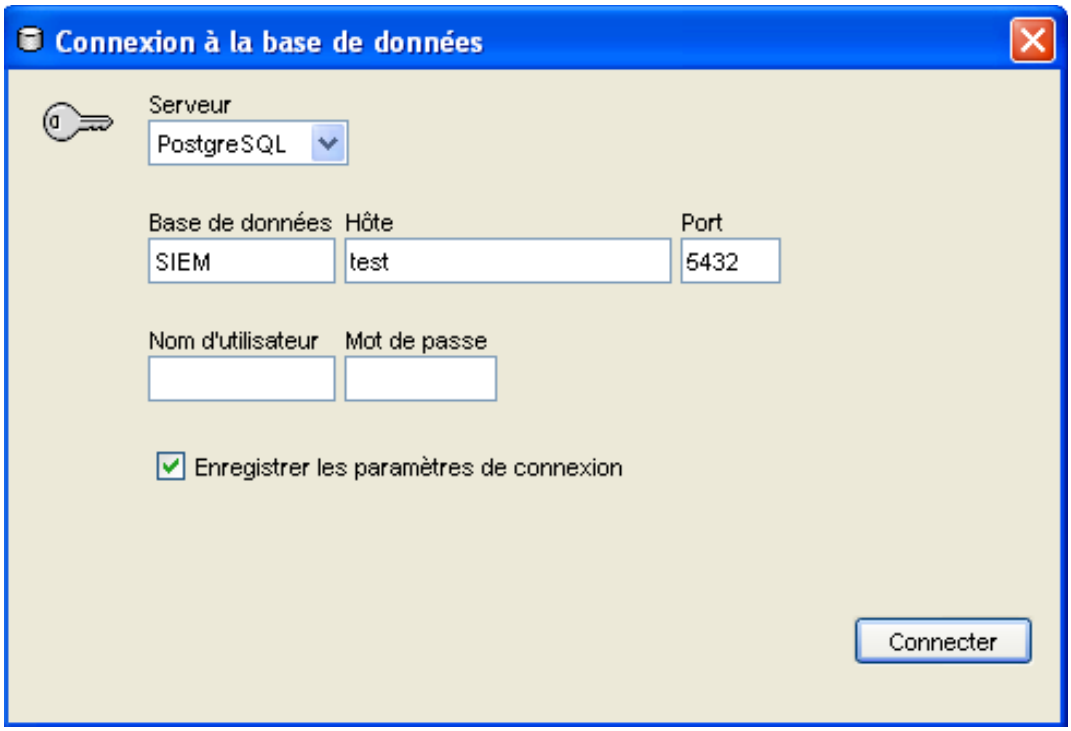
40 Cliquez sur l'onglet *Active Views*, puis vérifiez si l'événement corrélé a bien été généré.



41 Fermez Sentinel Control Center.

42 Sur la page Applications, cliquez sur *Démarrer le gestionnaire de données Sentinel*.

43 Loguez-vous au gestionnaire de données Sentinel en utilisant les références de l'administrateur de base de données spécifiées lors de l'installation (valeur par défaut : dbauser).



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

45 Fermez le gestionnaire de données Sentinel.

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

6.2 Nettoyage après test

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

1 Loguez-vous au système en tant qu'administrateur Sentinel spécifié durant l'installation (par défaut, admin).

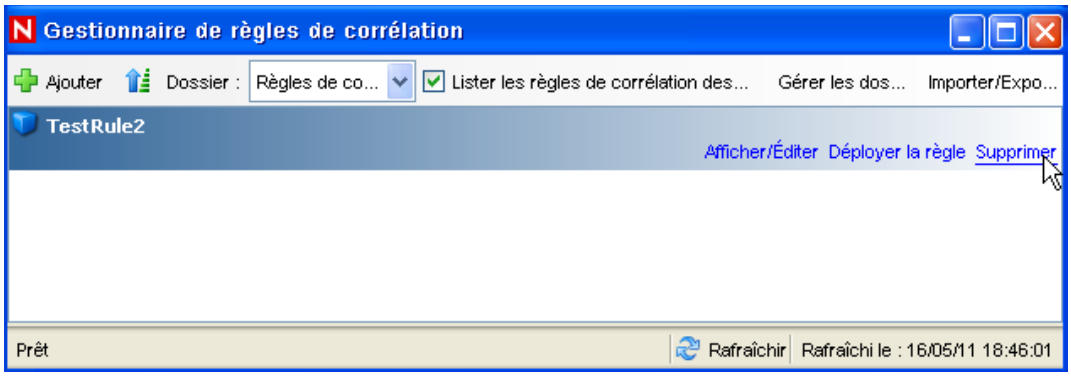
2 Sélectionnez l'onglet *Corrélation*.

3 Ouvrez le gestionnaire de moteurs de corrélation.

4 Dans celui-ci, cliquez avec le bouton droit de la souris sur *TestRule1*, puis sélectionnez *Annuler le déploiement*.

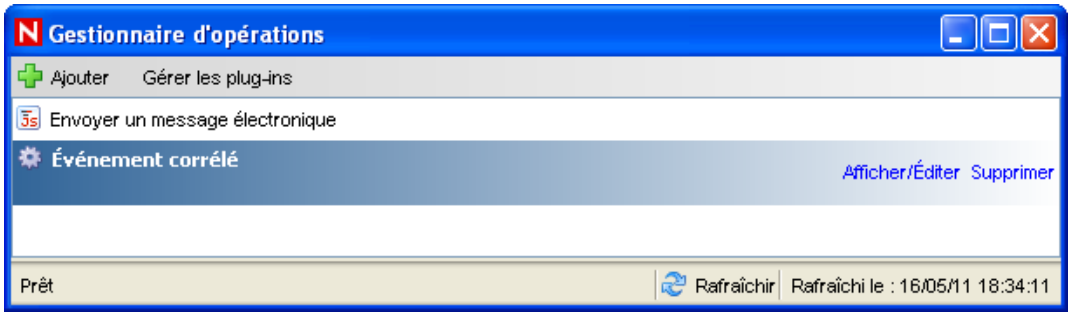
5 Ouvrez le gestionnaire de règle de corrélation.

6 Sélectionnez *TestRule1*, puis cliquez sur *Supprimer*.



7 Sélectionnez *Outils* > *Gestionnaire d'opérations* pour afficher la fenêtre Gestionnaire d'opérations.

8 Sélectionnez l'opération *CorrelatedEvent*, cliquez sur *Supprimer*, puis sur *Oui* pour valider la suppression.



9 Sélectionnez le menu *Gestion de source d'événements*, puis cliquez sur *Vue en direct*.

10 Dans la hiérarchie de source d'événements graphique, cliquez avec le bouton droit de la souris sur *Collecteur général*, puis sélectionnez *Arrêter*.

11 Fermez la fenêtre Gestion de source d'événements.

12 Cliquez sur l'onglet *Incidents*.

13 Ouvrez le gestionnaire de vues d'incidents.

14 Sélectionnez *TestIncident1*, cliquez avec le bouton droit de la souris dessus, puis sélectionnez *Supprimer*.

6.3 Utilisation des données réelles

Pour commencer à travailler avec les données réelles, vous devez importer et configurer les collecteurs appropriés pour votre environnement, configurer vos propres règles, créer les processus de travail iTRAC, etc. Pour plus d'informations, reportez-vous au *Guide de l'utilisateur de Sentinel Rapid Deployment*. Les Solution Packs de Sentinel permettent une mise en route rapide. Consultez la page de contenu Sentine (http://support.novell.com/products/sentinel/sentinel61.html) pour plus de détails.

Désinstallation de Sentinel Rapid Deployment 7

7.1 Désinstallation du serveur Sentinel Rapid Deployment

1. Loguez-vous en tant qu'utilisateur `root`.
2. Accédez au répertoire `setup`.

   `cd <install_directory>/setup`
3. Exécutez le script `uninstall.sh` pour désinstaller le serveur :

   `./uninstall.sh`

   Le script affiche un message indiquant que Sentinel Rapid Deployment va être entièrement supprimé.
4. Indiquez si vous souhaitez conserver ou supprimer l'utilisateur lors de la désinstallation du serveur Sentinel Rapid Deployment. Appuyez sur `y` pour supprimer l'utilisateur ou sur `n` pour le conserver.
5. Indiquez si vous souhaitez conserver ou supprimer le groupe lors de la désinstallation du serveur Sentinel Rapid Deployment. Appuyez sur `y` pour supprimer le groupe ou sur `n` pour le conserver.
6. Entrez `y` pour procéder à la désinstallation ou `n` pour quitter la procédure.

7.2 Désinstallation du gestionnaire des collecteurs et des programmes clients Sentinel

7.2.1 Linux

1. Loguez-vous en tant qu'utilisateur `root`.
2. (Facultatif) Si vous désinstallez le gestionnaire des collecteurs, arrêtez les services Sentinel Rapid Deployment :

   `<install_directory>/bin/sentinel.sh stop`
3. Accédez à l'emplacement suivant :

   `<install_directory>/_uninst`

4 Exécutez l'une des commandes suivantes :

Mode	Commande
Interface graphique	`./uninstall.bin` Passez à l'Étape 5 page 86.
Console	`./uninstall.bin -console` Suivez les instructions à l'écran.

5 Sélectionnez une langue et cliquez sur *OK*.

6 Dans l'assistant de désinstallation de Sentinel, cliquez sur *Suivant*.

7 Sélectionnez les composants à désinstaller et cliquez sur *Suivant*.

8 Assurez-vous que toutes les applications Sentinel en cours d'exécution sont arrêtées et cliquez sur *Suivant*.

Le récapitulatif des fonctionnalités sélectionnées pour la désinstallation s'affiche.

9 Cliquez sur *Désinstaller*.

10 Cliquez sur *Terminer*.

7.2.2 Windows

1 Loguez-vous en tant qu'administrateur.

2 (Facultatif) Si vous désinstallez le gestionnaire des collecteurs, arrêtez les services Sentinel Rapid Deployment :

`<install_directory>\bin\sentinel.bat stop`

3 Effectuez l'une des opérations suivantes :

- Sélectionnez *Démarrer* > *Tous les programmes* > *Sentinel* > *Désinstaller Sentinel*.
- Sélectionnez *Démarrer* > *Exécuter*, saisissez `<répertoire_installation>\_uninst`, puis double-cliquez sur `uninstall.exe`.

4 Sélectionnez une langue et cliquez sur *OK*.

L'assistant de désinstallation de Sentinel Rapid Deployment apparaît.

5 Cliquez sur *Suivant*.

6 Sélectionnez les composants à désinstaller et cliquez sur *Suivant*.

7 Assurez-vous que toutes les applications Sentinel en cours d'exécution sont arrêtées et cliquez sur *Suivant*.

Le récapitulatif des fonctionnalités sélectionnées pour la désinstallation s'affiche.

8 Cliquez sur *Désinstaller*.

9 Choisissez de redémarrer le système et cliquez sur *Terminer*.

7.2.3 Procédures post-désinstallation

Après la désinstallation des applications, certains paramètres système persistent et peuvent être supprimés manuellement. Ils doivent d'ailleurs être supprimés avant une nouvelle installation de Sentinel, surtout si le programme de désinstallation de Sentinel a rencontré des erreurs.

Remarque : sur Linux, la désinstallation du gestionnaire des collecteurs ou des programmes clients ne supprime pas l'administrateur Sentinel du système d'exploitation. Vous devez supprimer manuellement cet utilisateur, le cas échéant.

- « Linux » page 87
- « Windows » page 87

Linux

1. Loguez-vous en tant qu'utilisateur `root`.
2. Supprimez le contenu du répertoire `<répertoire_installation>` dans lequel le logiciel Sentinel est installé.
3. Supprimez les fichiers suivants du répertoire `/etc/init.d`, le cas échéant :

   `sentinel`

   Cela ne s'applique que si le gestionnaire des collecteurs est installé.
4. Assurez-vous que personne n'est logué en tant qu'administrateur Sentinel (esecadm par défaut), puis supprimez cet utilisateur, son répertoire privé et le groupe esec :
   - Exécutez la commande `userdel -r esecadm`
   - Exécutez la commande `groupdel esec`
5. Supprimez le répertoire `/root/InstallShield`.
6. Supprimez la section InstallShield de `/etc/profile`.
7. Redémarrez la machine.

Windows

1. Supprimez le dossier `%CommonProgramFiles%\InstallShield\Universal` et l'ensemble de son contenu.
2. Supprimez le dossier `<répertoire_installation>` (par défaut : `C:\Program Files\Novell\Sentinel6`).
3. Cliquez avec le bouton droit sur Poste de travail, puis cliquez sur *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.

7 Supprimez tous les raccourcis Sentinel du Bureau.

8 Supprimez le dossier de raccourcis en sélectionnant *Démarrer* > *Programmes* > *Sentinel* > .

9 Redémarrez la machine.

Mise à jour du nom d'hôte de Sentinel Rapid Deployment

A

A.1 Serveur

Sur le serveur Sentinel, les modifications apportées au nom d'hôte sont mises à jour automatiquement au cours de l'exécution ou de l'installation. Si le serveur ne fonctionne pas correctement après la mise à jour du nom d'hôte, vous devez vérifier manuellement les éléments suivants :

- Tous les fichiers `jnlp` et le fichier `configuration.xml` sont mis à jour au redémarrage de Sentinel.
- L'entrée du nom d'hôte dans la table de base de données `sentinel_host` est mise à jour.
- Toutes les références à la boucle locale (localhost ou 127.0.0.1) du fichier `<répertoire_installation>/config/configuration.xml` restent identiques.

A.2 Programmes clients

Pour les programmes clients, vous devez modifier manuellement le nom d'hôte ou l'adresse IP du serveur dans les emplacements suivants afin de pointer vers le serveur correct :

- `<répertoire_installation>/config/configuration.xml`.

  Sentinel Control Center et Solution Designer utilisent ces informations.
- URL de l'aide fournie dans le fichier `<répertoire_installation>/config/SentinelPreferences.properties`
- Exécutez la commande suivante pour mettre à jour le nom d'hôte dans le fichier `sdm.connect` :

  ```
  sdm -action saveConnection -server <postgresql> -host <hostIpaddress/
  hostName> -port <portnum> -database <databaseName/SID> [-driverProps
  <propertiesFile] {-user <dbUser> -password <dbPass> | -winAuth} -
  connectFile <filenameToSaveConnection>
  ```

Conseils de dépannage

B

Cette section fournit des conseils de dépannage susceptibles de vous aider à résoudre certains problèmes d'installation de Sentinel Rapid Deployment.

B.1 L'authentification de la base de données échoue lors de la saisie de références non valides

Cause commune : l'authentification de la base de données échoue si un nom d'hôte ou une adresse IP du serveur LDAP non valides sont saisis lors de la configuration du serveur Sentinel Rapid Deployment pour l'authentification LDAP.

Action : assurez-vous qu'un nom d'hôte ou une adresse IP du serveur LDAP valides sont saisis.

B.2 L'interface Web de Sentinel ne démarre pas

Cause commune : vous avez installé Sentinel Rapid Deployment sur une machine sur laquelle le processus Identity Audit est en cours d'exécution ou sur laquelle la désinstallation n'a pas été finalisée.

Action : Sentinel Rapid Deployment et Novell Identity Audit ne peuvent pas être installés sur la même machine. Avant d'installer Sentinel Rapid Deployment sur la machine sur laquelle l'application Identity Audit est installée, désinstallez entièrement celle-ci.

Si les processus Identity Audit ne sont pas complètement arrêtés, Identity Audit ne peut pas être totalement désinstallé. Dans ce cas, des conflits risquent de survenir lors de l'installation de Sentinel Rapid Deployment ou lors du démarrage de ses applications.

1. Exécutez la commande suivante pour fermer les services Identity Audit :

   ```
   /etc/init.d/identity_audit stop
   ```

2. Exécutez la commande suivante pour vous assurer que plus aucun processus Identity Audit n'est en cours d'exécution :

   ```
   ps -ef | grep novell
   ```

3. Arrêtez les processus restants manuellement le cas échéant.

   ```
   kill -9 pid
   ```

4 Désinstallez Identity Audit avec les autorisations `root` nécessaires.

Pour plus d'informations, reportez-vous au Guide d'Identity Audit (http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/).

B.3 Le gestionnaire des collecteurs à distance génère une exception sous Windows 2008 lorsque le contrôle d'accès utilisateur est activé

Problème : loguez-vous en tant qu'utilisateur appartenant au groupe administrateur et exécutez la commande `setup.bat` à l'invite du terminal pour installer le gestionnaire des collecteurs. Redémarrez le système ou démarrez manuellement les services du gestionnaire des collecteurs, puis loguez-vous avec les mêmes références utilisateur. Les exceptions sont consignées dans le fichier `collector_manager0.0.log` qui a une incidence sur les fonctionnalités suivantes du gestionnaire des collecteurs :

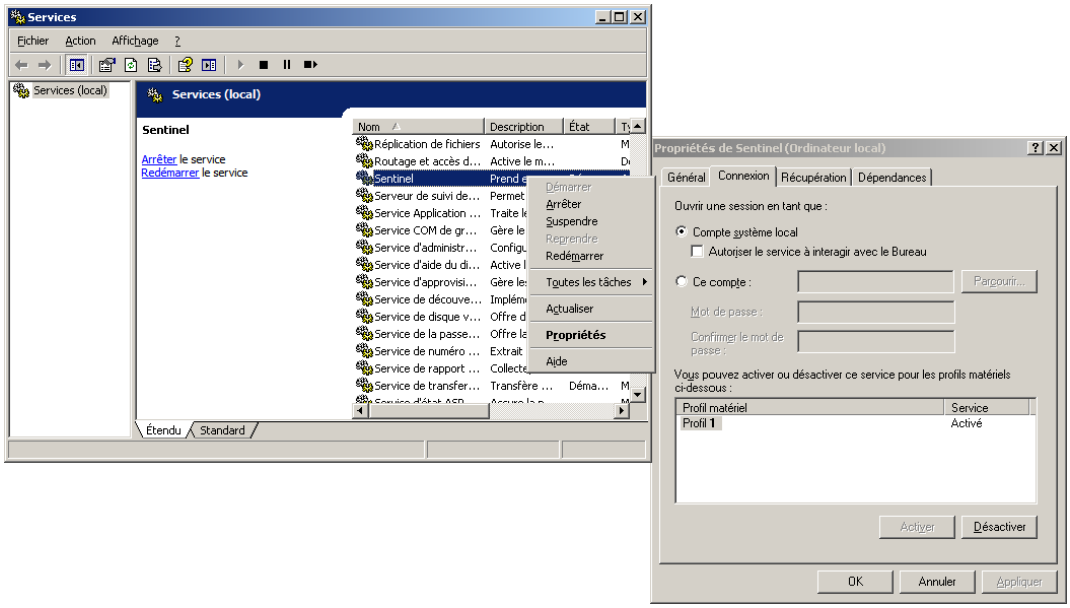
- Les assignations ne sont pas initialisées.
- Vous ne pouvez pas choisir de fichier source d'événements sur le système de fichiers de la machine du gestionnaire des collecteurs (Win2008) en utilisant le connecteur de fichier.

Cause commune : vous avez installé le gestionnaire des collecteurs sur une machine Windows 2008 SP1 Standard Edition 64 bits. Le contrôle d'accès utilisateur de cette machine est défini par défaut sur *Activé*.

Action : changez le propriétaire *Se connecter* des services Sentinel Rapid Deployment et sélectionnez l'utilisateur actuel. Par défaut, le propriétaire *Se connecter* est défini sur *Local System Account (Compte système local)*. Pour modifier l'option par défaut, procédez comme suit :

1 Exécutez `services.msc` pour ouvrir la fenêtre *Services*.

2 Cliquez avec le bouton droit sur Sentinel, puis sélectionnez *Propriétés*.



3 Dans la fenêtre Sentinel Properties (Propriétés Sentinel), sélectionnez l'onglet *Se connecter*.

4 Sélectionnez *This Account (Ce compte)*, puis fournissez les références de l'utilisateur en cours que vous avez utilisées pour l'installation du gestionnaire des collecteurs.

B.4 L'UUID n'est pas créé pour les images de gestionnaires des collecteurs

Si vous créez l'image d'un serveur de gestionnaire des collecteurs (par exemple en utilisant l'outil de création d'image ZenWorks) et si vous restaurez les images sur différentes machines, Sentinel Rapid Deployment n'identifie pas de façon unique les nouvelles instances du gestionnaire des collecteurs. Ceci est dû aux UUID dupliqués.

Vous devez générer l'UUID en suivant les étapes ci-après sur les systèmes de gestionnaire des collecteurs que vous venez d'installer :

1 Supprimez le fichier `host.id` ou `sentinel.id` situé dans le dossier `<répertoire_installation>/data`.

2 Redémarrez le gestionnaire des collecteurs.

Le gestionnaire des collecteurs génère automatiquement l'UUID.

Meilleures pratiques pour la gestion d'une base de données PostgreSQL

C

Vous pouvez paramétrer la base de données afin d'améliorer les performances du serveur de base de données. Les limites recommandées dans cette section sont approximatives. Il n'existe aucune limite matérielle. Toutefois, sur les systèmes hautement dynamiques, il est recommandé de créer des tampons et de prévoir de l'espace en vue de répondre aux besoins de croissance éventuels du système.

C.1 Modification des paramètres de configuration de la mémoire

Pour paramétrer le serveur de base de données PostgreSQL, modifiez les paramètres suivants de configuration de la mémoire dans le fichier `<rép_installation>/3rd party/postgresql/data/postgresql.conf` :

- **shared_buffers :** détermine la quantité de mémoire dédiée à PostgreSQL pour le caching des données. Pour optimiser les performances, vous pouvez définir la valeur de ce paramètre sur un quart de la mémoire RAM.
- **effective_cache_size :** détermine la quantité de mémoire disponible pour le caching du disque par le système d'exploitation et au sein de la base de données. Vous pouvez estimer la valeur de ce paramètre en prenant en compte les éléments utilisés par le système d'exploitation et les autres applications. Vous pouvez définir ce paramètre sur la moitié de la taille totale de la mémoire système disponible.
- **work_mem :** détermine la quantité de mémoire utilisée par les opérations de tri internes et les tables de hachage avant de passer aux fichiers disque temporaires. La valeur est indiquée en kilo-octets. La valeur par défaut est de 1024 ko (1 Mo).

  Pour une requête complexe, plusieurs opérations de tri ou de hachage peuvent s'exécuter en parallèle. Chaque opération utilise autant de mémoire que la mémoire spécifiée dans le paramètre work_mem avant l'insertion des données dans les fichiers disque temporaires. Si vous programmez plus de rapports sur votre système Sentinel Rapid Deployment, définissez cette valeur entre 500 Mo et 1 Go.
- **maintenance_work_mem :** détermine la quantité maximum de mémoire à utiliser pour les opérations de maintenance de la base de données, comme la purge, la création d'index et la modification de la clé étrangère d'ajout de table. La valeur est indiquée en kilo-octets. La valeur par défaut est de 16 384 ko (16 Mo).

  Des paramètres plus élevés peuvent améliorer les performances de la purge et de la restauration des vidages de base de données. Ne modifiez pas ces paramètres : la valeur par défaut est suffisante pour les opérations de Sentinel Rapid Deployment.

C.2 Réduction de l'impact E/S des processus de purge/d'analyse

Vous pouvez améliorer les performances de la base de données PostgreSQL de différentes façons.

- Les deux paramètres suivants contrôlent les opérations de purge automatiques. Par défaut, ces paramètres sont commentés lors de l'installation du serveur Sentinel Rapid Deployment. Vous devez supprimer le commentaire et définir les valeurs.
  - **vacuum_cost_delay :** détermine la période pendant laquelle le processus reste en veille en cas de dépassement de la limite de coût. Vous pouvez, par exemple, définir cette valeur sur 100.
  - **vacuum_cost_limit :** détermine le coût cumulé qui entraîne la mise en veille du processus de purge. Vous pouvez, par exemple, définir cette valeur sur 10 000.

    Le fait de définir ces paramètres sur une valeur autre que zéro réduira l'impact E/S des commandes de purge et d'analyse sur l'activité de base de données normale. Il se peut que l'impact sur les performances soit négligeable lors de l'exécution des rapports, dans la mesure où la purge prend plus de temps qu'auparavant.
- Par défaut, le processus `autovacuum` s'exécute régulièrement pour restaurer l'espace disque et mettre à jour les statistiques du planificateur. Lorsque la taille de la base de données augmente, `autovacuum` ne peut pas assurer la maintenance de tous les objets de la base de données. Dans un tel cas et si les performances s'affaiblissent, exécutez le script `AnalyzePartitions.sh` en tant que tâche cron. Cette tâche cron doit être définie par l'utilisateur propriétaire des processus Sentinel Rapid Deployment.

  Par exemple :

  ```
  30 11 * * * $ESEC_HOME/bin/AnalyzePartitions.sh
  ```

  Où :
  - `30` correspond à la durée en minutes.
  - `11` correspond à la durée en heures.
  - `ESEC_HOME` correspond au chemin absolu de la base de données.

  Dans cet exemple, le script s'exécute tous les jours à 11h30.
- Évitez de programmer l'archivage pendant la création de rapports. Si vous programmez les deux processus en même temps, la création de rapports se met en attente car PostgreSQL bogue et démarre le traitement des données après l'exécution de la tâche d'archivage. Cette modification affecte les performances de la base de données.