Sentinel™

Guide d'installation et de configuration

Juillet 2018

NetIQ

Mentions légales

À propos de ce guide et de la bibliothèque

Ce *Guide d'installation et de configuration* vous présente Sentinel et explique comment installer et configurer Sentinel.

Public

Ce guide est destiné aux administrateurs et aux consultants Sentinel.

Autres documents dans la bibliothèque

La bibliothèque propose les manuels suivants :

Guide d'administration

Fournit les informations et les tâches administratives requises pour la gestion d'un déploiement de Sentinel.

Guide de l'utilisateur

Présente des informations conceptuelles à propos de Sentinel. Ce manuel donne aussi un aperçu des interfaces utilisateur ainsi que des procédures pour diverses tâches.

Présentation de Sentinel

Cette section fournit des informations détaillées sur Sentinel et explique comment cette application fournit une solution de gestion des événements à votre organisation.

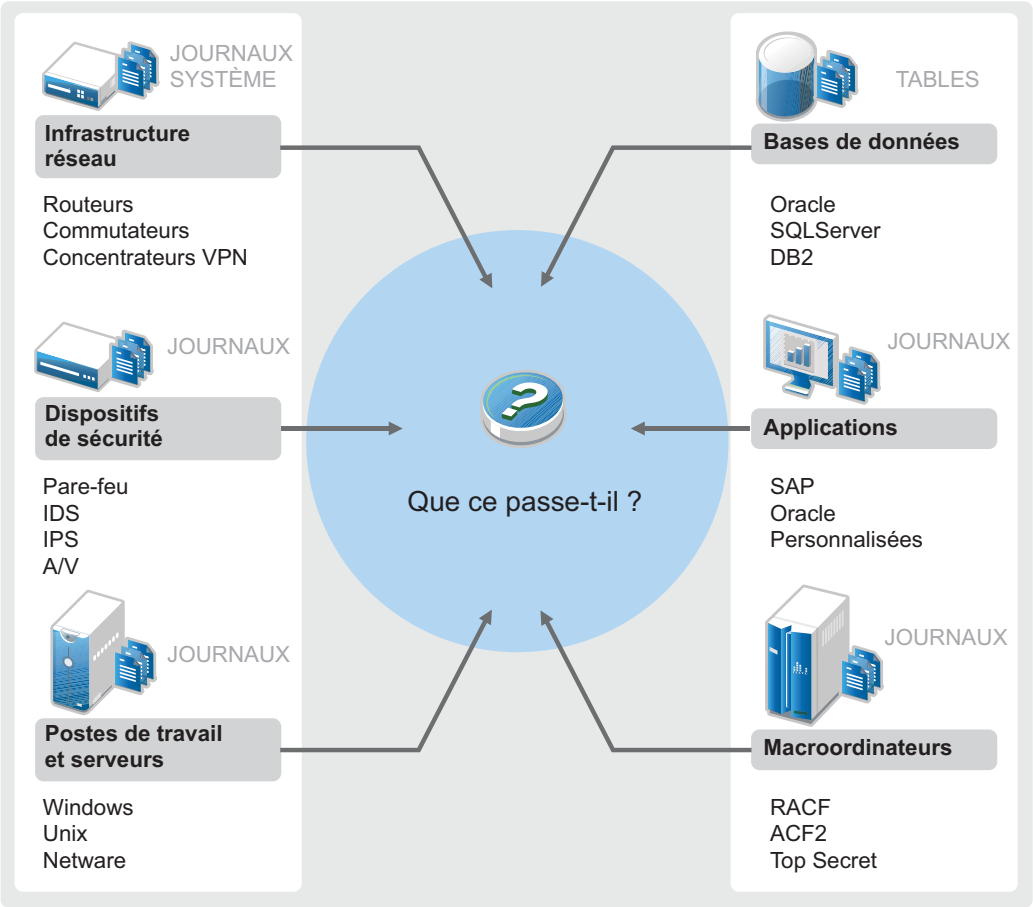
1 Qu'est-ce que Sentinel ?

Sentinel est une solution permettant de gérer les événements et les informations de sécurité (SIEM), mais aussi de surveiller la conformité. Elle surveille automatiquement les environnements informatiques les plus complexes et offre la sécurité nécessaire à leur protection.

Défis liés à la sécurisation d'un environnement informatique

Compte tenu de la complexité de l'environnement informatique, sa sécurisation constitue un véritable défi. Généralement, votre environnement informatique comprend de nombreux et nombreuses applications, bases de données, postes de travail et serveurs, et toutes ces entités génèrent des journaux d'événements. Vous avez peut-être également des périphériques de sécurité et des périphériques d'infrastructure réseau qui génèrent des journaux d'événements dans votre environnement informatique.

Figure 1-1 *Événements au sein de votre environnement*



Des défis surviennent pour les raisons suivantes :

- Votre environnement informatique compte de nombreux périphériques.
- Les journaux sont dans différents formats.
- Les journaux sont stockés à différents endroits.
- Le volume d'informations consignées dans les fichiers journaux est considérable.
- Il est impossible de déterminer les déclencheurs d'événements sans analyser manuellement les fichiers journaux.

Pour pouvoir exploiter les informations contenues dans les fichiers journaux, vous devez effectuer les opérations suivantes :

- Collecter les données.
- Consolider les données.
- Harmoniser les données disparates dans des événements facilement comparables.
- Assigner des événements à des réglementations standard.
- Analyser les données.
- Comparer les événements de plusieurs systèmes afin d'identifier les éventuels problèmes de sécurité.
- Envoyer des notifications lorsque les données ne respectent pas les normes.

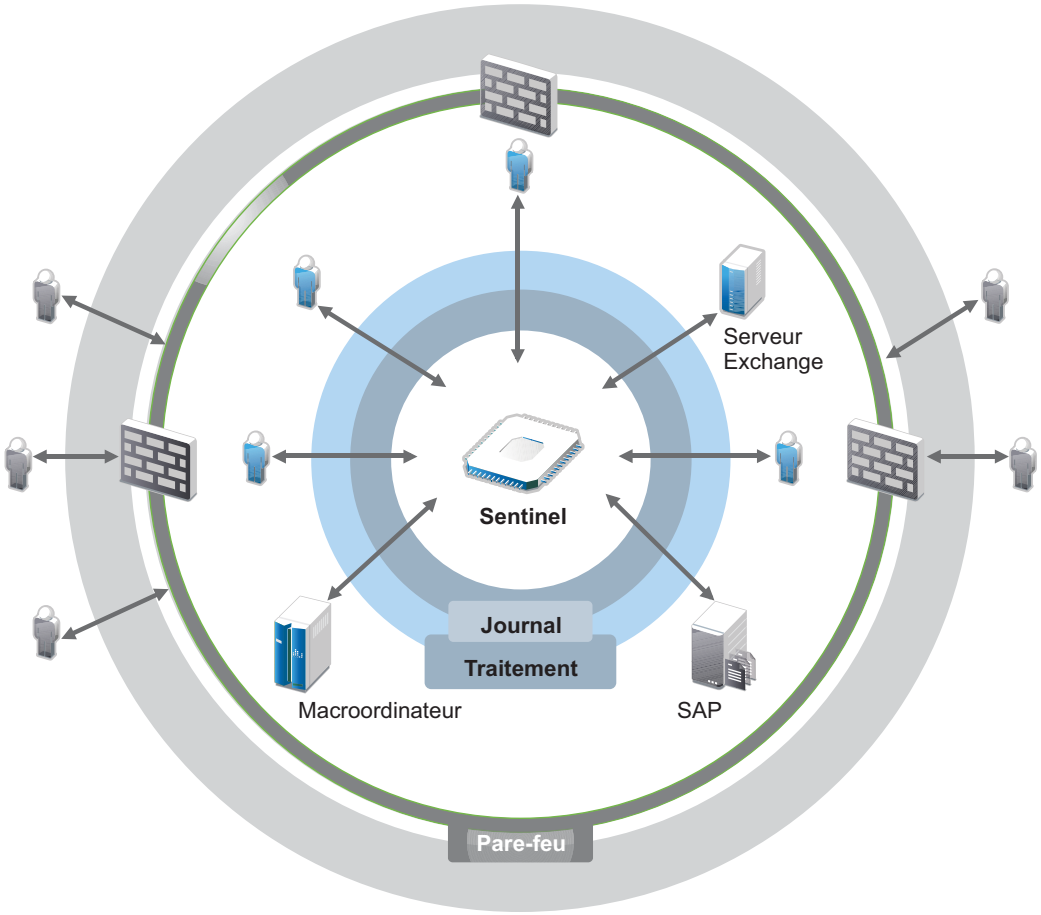
- Prendre des mesures afin de garantir la conformité aux stratégies d'entreprise.
- Générer des rapports pour prouver la conformité.

Une fois que vous avez compris les défis liés à la sécurisation de votre environnement informatique, vous devez définir une manière de sécuriser votre entreprise pour et contre les utilisateurs sans conséquences sur l'expérience utilisateur. Sentinel offre la solution.

Principe de la solution Sentinel

La solution Sentinel est le système nerveux central de la sécurité de votre entreprise. Elle collecte les données de l'ensemble de votre infrastructure (applications, bases de données, serveurs, stockage et périphériques de sécurité). Elle analyse les données, les met en corrélation et les rend exploitables, automatiquement ou manuellement.

Figure 1-2 *Principe de la solution Sentinel*



Sentinel vous permet de savoir à tout moment ce qui se passe dans votre environnement informatique et de connecter les opérations sur certaines ressources aux personnes qui les ont menées. Cela vous permet de déterminer le comportement utilisateur et de surveiller efficacement les activités pour éviter des actions malveillantes.

Pour ce faire, Sentinel :

- fournit une solution unique permettant de mener à bien les contrôles informatiques pour vous conformer à plusieurs standards de sécurité ;
- comble le vide existant entre ce qui devrait théoriquement se passer dans votre environnement informatique et ce qui se passe réellement ;
- vous aide à vous conformer aux standards de sécurité ;
- offre une solution de surveillance de la conformité et des programmes de création de rapports prêts à l'emploi.

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 surveille automatiquement les événements de sécurité et de conformité, ainsi que les contrôles informatiques. Il vous permet de prendre des mesures immédiates lorsqu'une violation de la sécurité ou un événement non conforme se produit. Sentinel vous permet également de collecter des informations récapitulatives sur votre environnement, et de les partager avec les principaux intéressés.

2 Fonctionnement de Sentinel

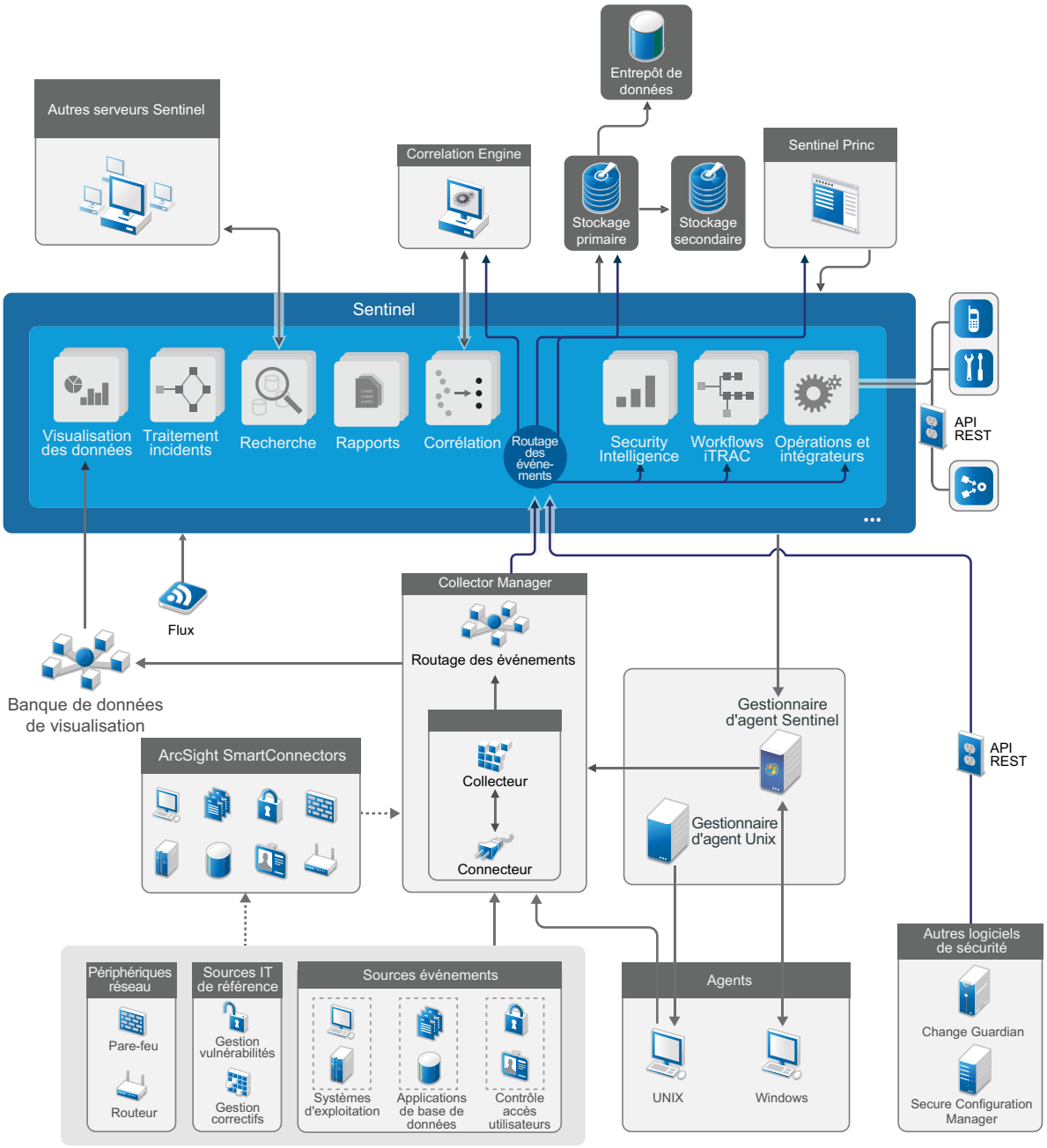
Sentinel gère en permanence les événements et les informations de sécurité dans l'ensemble de votre environnement informatique afin de vous offrir une solution de surveillance complète.

Sentinel assure les opérations suivantes :

- collecte des journaux, événements et informations de sécurité à partir des différentes sources de votre environnement informatique ;
- uniformise les journaux, événements et informations de sécurité collectés en un format Sentinel standard ;
- stocke les événements dans un espace de stockage des données basé sur des fichiers ou un espace de stockage évolutif Hadoop avec des stratégies de conservation des données flexibles personnalisables ;
- collecte des données de flux IP et aide à la surveillance approfondie des activités réseau ;
- permet d'établir un lien hiérarchique entre plusieurs systèmes Sentinel dont Sentinel Log Manager ;
- recherche des événements sur votre serveur Sentinel local, mais aussi sur d'autres serveurs Sentinel situés aux quatre coins du globe ;
- effectue une analyse statistique vous permettant de définir une ligne de base, puis de la comparer à la situation réelle afin de déterminer l'éventuelle présence de problèmes non identifiés ;
- met en corrélation un ensemble d'événements similaires ou comparables au cours d'un certain laps de temps, afin de dégager un modèle ;
- organise les événements en incidents, afin de garantir l'efficacité du suivi et de la gestion des réponses ;
- fournit des rapports sur la base des événements historiques et en temps réel.

La figure suivante illustre la façon dont Sentinel fonctionne avec un stockage traditionnel comme solution de stockage des données :

Figure 2-1 *Architecture de Sentinel*



Les sections suivantes décrivent en détail les composants Sentinel :

Sources d'événements

Sentinel collecte les événements et informations de sécurité à partir de diverses sources de votre environnement informatique. Ces sources sont appelées sources d'événements. En général, votre réseau comprend les sources d'événements suivantes :

Périmètre de sécurité : périphériques de sécurité incluant le matériel et les logiciels utilisés pour créer un périmètre de sécurité pour votre environnement, tels que pare-feu, IDS (Intrusion Detective Systems) et VPN (Virtual Private Network).

Systèmes d'exploitation : différents systèmes d'exploitation s'exécutant sur le réseau.

Sources informatiques du référentiel : logiciels utilisés pour assurer la gestion et le suivi des ressources, des correctifs, de la configuration et de la vulnérabilité.

Applications : diverses applications installées sur le réseau.

Contrôle d'accès des utilisateurs : applications ou périphériques qui permettent aux utilisateurs d'accéder aux ressources de l'entreprise.

Pour plus d'informations sur la collecte des événements à partir des sources d'événements, reportez-vous à la section « Collecting and Routing Event Data » (Collecte et routage des données d'événement) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Événement Sentinel

Sentinel reçoit des informations des périphériques, les normalise dans une structure appelée événement, catégorise l'événement et l'envoie pour qu'il soit traité.

Un événement représente un enregistrement de journal normalisé signalé à Sentinel par un périphérique de sécurité, de réseau ou d'application tiers, ou par une source Sentinel interne. Il existe plusieurs types d'événements :

- Les événements externes (reçus d'un périphérique de sécurité). Par exemple :
  - Une attaque détectée par un système de détection d'intrus (IDS)
  - Une connexion réussie signalée par un système d'exploitation
  - Une situation définie par le client telle qu'un utilisateur qui accède à un fichier
- Les événements internes (générés par Sentinel). Par exemple :
  - La désactivation d'une règle de corrélation
  - Le remplissage d'une base de données

Sentinel ajoute des informations de catégorie (taxonomie) aux événements, pour simplifier la comparaison des événements entre des systèmes aux méthodes de création de rapports différentes. Les événements sont traités par l'affichage en temps réel, Correlation Engine, les tableaux de bord et le serveur dorsal.

Un événement comprend plus de 200 champs. Les champs d'événements sont de différents types et possèdent différentes finalités. Certains sont prédéfinis, tels que ceux relatifs à la gravité, à la sévérité, à l'adresse IP de destination et au port de destination.

Il existe deux groupes de champs configurables :

- Champs réservés : dédiés à l'usage interne de Sentinel, permettent l'extension des fonctionnalités à l'avenir.
- Champs client : destinés au client, à des fins de personnalisation.

Un champ peut avoir une source externe ou de référentiel :

- La valeur d'un champ externe est explicitement définie par le périphérique ou le collecteur correspondant. Par exemple, un champ peut être défini pour être le code de génération du bâtiment contenant les ressources mentionnées comme adresse IP de destination d'un événement.
- La valeur d'un champ de référence est calculée en tant que fonction d'un ou de plusieurs autres champs à l'aide du service d'assignation. Par exemple, un champ peut être défini par le service d'assignation à l'aide d'une assignation définie par le client utilisant l'adresse IP de destination de l'événement.

- « Service d'assignation » page 23
- « Acheminement des assignations » page 23
- « Détection d'exploitation » page 23

Service d'assignation

Le service d'assignation propage des données pertinentes dans le système. Ces données peuvent enrichir les événements avec des informations de référence.

Vous pouvez étoffer les données d'événement à l'aide d'assignations afin d'ajouter des informations sur l'hôte et sur l'identité aux événements entrants qui proviennent des périphériques sources. Sentinel peut utiliser ces informations supplémentaires pour une corrélation et une création de rapports avancées. Sentinel prend en charge plusieurs assignations intégrées, ainsi que les assignations personnalisées définies par l'utilisateur.

Les assignations définies dans Sentinel sont stockées de deux manières :

- Les assignations intégrées sont stockées dans la base de données, sont mises à jour en interne, puis sont exportées automatiquement vers le service d'assignation.
- Les assignations personnalisées sont stockées en tant que fichiers CSV et peuvent être mises à jour dans le système de fichiers ou par l'intermédiaire de l'interface utilisateur de configuration des données d'assignation, puis chargées par le service d'assignation.

Dans les deux cas, les fichiers CSV sont conservés sur le serveur Sentinel central, mais les modifications apportées aux assignations sont distribuées sur chaque Collector Manager et appliquées localement. Ce processus distribué garantit que l'assignation ne surcharge pas le serveur principal.

Acheminement des assignations

Le service d'assignation utilise un modèle de mise à jour dynamique et achemine les assignations d'un point à un autre, ce qui évite l'accumulation d'assignations statiques volumineuses dans la mémoire dynamique. Ceci est pertinent dans un système critique en temps réel, tel que Sentinel, qui nécessite un mouvement de données stable, prédictif et agile, indépendant de toute charge transitoire du système.

Détection d'exploitation

Sentinel permet de recouper des signatures de données d'événement avec les données d'analyse de vulnérabilité. Sentinel avertit les utilisateurs automatiquement et immédiatement en cas de tentative d'exploitation d'un système vulnérable. Sentinel utilise pour ce faire les fonctions suivantes :

- la réception de données de flux Advisor,
- Détection d'intrusion
- Analyse de la vulnérabilité
- pare-feux

Les données de flux Advisor contiennent des informations sur les vulnérabilités et les menaces, ainsi qu'une normalisation de signatures d'événements et plug-ins de vulnérabilité. Elles fournissent une référence croisée entre les signatures de données d'événement et les données du scanner de vulnérabilité. Pour plus d'informations sur le flux Advisor, reportez-vous à la section « Detecting Vulnerabilities and Exploits » (Détection des vulnérabilités et des exploits) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Collector Manager

Collector Manager gère la collecte des données, surveille les messages d'état du système et filtre les événements. Ses principales fonctions sont les suivantes :

- Collecte des données par le biais de connecteurs
- Analyse et normalisation des données à l'aide des collecteurs

Collecteurs

Les collecteurs collectent les informations à partir des connecteurs et les normalisent. Ils effectuent les fonctions suivantes :

- Réception des données brutes envoyées par les connecteurs
- Analyse et normalisation des données :
  - Conversion des données spécifiques des sources d'événements en données propres à Sentinel ;
  - Enrichissement des événements en convertissant les informations des événements en un format pris en charge par Sentinel ;
  - Filtrage des événements selon les sources d'événements.
- Ajout de pertinence aux événements à l'aide du service d'assignation :
  - Assignation d'événements aux identités
  - Assignation d'événements aux ressources
- Routage des événements
- Transmission des données uniformisées, analysées et formatées à Collector Manager
- Envoi de messages relatifs à l'état de santé au serveur Sentinel

Pour plus d'informations sur les collecteurs, reportez-vous au site Web des plug-ins Sentinel.

Connecteurs

Les connecteurs fournissent des connexions au système Sentinel à partir des sources d'événements.

Les connecteurs fournissent les fonctionnalités suivantes :

- Acheminement des données d'événement brutes à partir des sources d'événements jusqu'au collecteur
- Filtrage spécifique à la connexion
- Gestion des erreurs de connexion

ArcSight SmartConnectors

Sentinel tire parti d'ArcSight SmartConnector pour collecter des événements à partir de différents types de sources d'événements qui ne sont pas directement pris en charge par Sentinel. SmartConnector collecte les événements provenant de périphériques pris en charge, normalise

ceux-ci au format CEF (Common Event Format) et les transmet à Sentinel via le connecteur Syslog. Le connecteur transmet ensuite les événements à Universal Common Event Format Collector pour analyse.

Pour plus d'informations sur la configuration de Sentinel avec SmartConnector, consultez la documentation relative à Universal Common Event Format Collector sur le site Web des plug-ins Sentinel.

Agent Manager

Agent Manager propose d'effectuer une collecte de données basée sur l'hôte qui vient compléter la collecte sans agent. Grâce à cette collecte, vous pouvez :

- accéder aux journaux qui ne sont pas disponibles via le réseau ;
- réaliser des opérations dans des environnements réseau hautement contrôlés ;
- renforcer la position de sécurité en limitant la surface d'attaque sur des serveurs critiques ;
- améliorer la fiabilité de la collecte de données pendant les interruptions réseau.

Agent Manager vous permet de déployer des agents, de gérer leur configuration, mais aussi de faire office de point de collecte pour les événements acheminés vers Sentinel. Pour plus d'informations sur Agent Manager, reportez-vous à la documentation correspondante.

Routage et stockage des données Sentinel

Sentinel fournit de nombreuses options pour le routage, le stockage et l'extraction des données collectées. Par défaut, Sentinel reçoit les données d'événement analysées ainsi que les données brutes des instances Collector Manager. Sentinel stocke les données brutes pour fournir une chaîne de preuves sécurisée et achemine les données d'événement analysées selon les règles que vous définissez. Vous pouvez filtrer les données d'événement analysées, les envoyer à l'espace de stockage ou à l'outil d'analyse en temps réel, mais aussi les acheminer vers des systèmes externes. En outre, Sentinel met toutes les données d'événement envoyées au stockage en correspondance avec des stratégies de conservation définies par l'utilisateur. Ces stratégies contrôlent le moment où les données d'événement doivent être supprimées du système.

Selon le taux d'événements par seconde (EPS) et vos besoins en matière de déploiement, vous pouvez choisir d'utiliser le stockage de données traditionnel basé sur des fichiers ou le stockage évolutif Hadoop comme solution de stockage des données. Pour plus d'informations, reportez-vous à la section « Considérations relatives au stockage de données » page 41.

Visualisation des événements

Sentinel fournit des visualisations d'événements qui présentent les données dans des graphiques, des tableaux et des assignations. Ces visualisations facilitent la visualisation et l'analyse de gros volumes d'événements, notamment les événements de flux IP. Vous pouvez également créer vos propres visualisations et tableaux de bord.

Les visualisations d'événements sont disponibles par défaut dans Sentinel avec un stockage évolutif. Dans une configuration de stockage traditionnelle, les visualisations d'événements sont disponibles uniquement si vous avez activé le magasin de données de visualisation (Elasticsearch) pour stocker et indexer des données. Pour plus d'informations sur l'activation d'Elasticsearch, reportez-vous à la section « Configuration de la zone de stockage de visualisation » page 45.

Corrélation

Un événement isolé peut sembler anodin, mais combiné à d'autres événements, il peut indiquer un problème potentiel. Sentinel vous permet de corréler ces événements à l'aide de règles que vous créez et déployez dans Correlation Engine, ainsi que de prendre les mesures appropriées pour résoudre tout problème.

La fonction de corrélation améliore la gestion des événements de sécurité en automatisant l'analyse des flux d'événements entrants en vue de rechercher des modèles pertinents. Cette fonction vous permet de définir des règles qui identifient les menaces critiques et les modèles d'attaque complexes de sorte que vous puissiez classer les événements par priorité ainsi que gérer les incidents et y répondre avec efficacité. Pour plus d'informations sur la corrélation, reportez-vous à la section « Correlating Event Data » (Corrélation de données d'événement) du *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

Pour surveiller les événements en fonction des règles de corrélation, vous devez déployer ces dernières dans Correlation Engine. Lorsqu'un événement correspondant aux critères de la règle se produit, Correlation Engine génère un événement de corrélation décrivant le schéma. Pour plus d'informations, reportez-vous à la section « Correlation Engine » du manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel 7.1).

Security Intelligence

La fonctionnalité de corrélation de Sentinel vous permet de rechercher des modèles connus d'activité, que vous pouvez analyser à des fins de sécurité, de conformité ou pour toute autre raison. La fonction Security Intelligence recherche toute activité inhabituelle qui pourrait être malveillante, mais ne correspond à aucun modèle connu.

La fonction Security Intelligence de Sentinel repose sur l'analyse statistique des données de série temporelle, qui permet aux analystes d'identifier et d'analyser les anomalies, soit au moyen d'un moteur statistique automatisé, soit en interprétant manuellement les données statistiques représentées visuellement. Pour plus d'informations, reportez-vous à la section « Analyzing Trends in Data (Analyse de tendances dans les données) » du manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

Réparation d'incident

Sentinel fournit un système de gestion automatisée des réponses aux incidents qui vous permet de documenter et de formaliser le processus de suivi, de réaffectation et de réponse aux incidents et violations de stratégies. Il garantit également une intégration bidirectionnelle avec des systèmes de tickets de dépannage. Sentinel permet de réagir rapidement et de résoudre les incidents efficacement. Pour plus d'informations, reportez-vous à la section « Configuring Incidents » (Configuration des incidents) du manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

Workflows iTRAC

Les workflows iTRAC constituent une solution simple et souple pour automatiser et suivre les processus de réponse aux incidents d'une entreprise. iTRAC utilise le système d'incidents interne de Sentinel pour assurer le suivi des problèmes système ou de sécurité, depuis leur identification (via des règles de corrélation ou par identification manuelle) jusqu'à leur résolution.

Vous pouvez créer des workflows en suivant des étapes manuelles et automatisées. Les workflows iTRAC prennent en charge des fonctions avancées telles que la création de branche, la réaffectation temporelle et les variables locales. L'intégration avec des scripts et plug-ins externes permet une interaction aisée avec les systèmes tiers. La création de rapports détaillés permet aux administrateurs de comprendre et d'optimiser les processus de réponse aux incidents. Pour plus d'informations, reportez-vous à la section « Configuring iTRAC Workflows » (Configuration de workflows iTRAC) du manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

Opérations et intégrateurs

Les opérations exécutent manuellement ou automatiquement certains types d'actions, tels que l'envoi d'un message électronique. Vous pouvez déclencher des opérations par l'acheminement de règles, par l'exécution manuelle d'une opération d'événement ou d'incident et par le biais des règles de corrélation. Sentinel propose une liste d'opérations préconfigurées. Vous pouvez utiliser les opérations par défaut et les reconfigurer au besoin ou en ajouter de nouvelles. Pour plus d'informations, reportez-vous à la section « Configuring Actions » (Configuration des opérations) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Une opération peut s'exécuter spontanément ou utiliser une instance d'intégrateur configurée à partir d'un plug-in d'intégrateur. Les plug-ins d'intégrateur étendent les fonctions et fonctionnalités des opérations de traitement d'incident Sentinel. Grâce aux intégrateurs, vous pouvez vous connecter à un système externe, notamment un serveur LDAP, SMTP ou SOAP, pour exécuter une opération. Pour plus d'informations, reportez-vous à la section « Configuring Integrators » (Configuration des intégrateurs) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Recherches

Sentinel propose une option permettant d'effectuer une recherche sur des événements. Si vous disposez de la configuration nécessaire, vous pouvez également effectuer une recherche dans les événements système générés par Sentinel et afficher les données brutes relatives à chaque événement. Pour plus d'informations, reportez-vous à la section « Searching Events » (Recherche d'événements) du *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

Vous pouvez également rechercher des serveurs Sentinel situés dans différents emplacements géographiques. Pour plus d'informations, reportez-vous à la section « Configuring Data Federation » (Configuration de la fédération des données) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Rapports

Sentinel vous permet d'exécuter des rapports sur les données collectées. Sentinel est livré avec divers rapports personnalisables. Certains de ces rapports sont configurables et vous permettent de spécifier les colonnes à afficher dans les résultats.

Vous pouvez exécuter, planifier et envoyer des rapports par message électronique au format PDF. Vous pouvez également exécuter les rapports comme s'il s'agissait d'une simple recherche pour ensuite utiliser les résultats (par exemple, affiner la recherche ou effectuer une opération sur les résultats). Vous pouvez aussi exécuter des rapports sur des serveurs Sentinel situés à divers emplacements géographiques. Pour plus d'informations, reportez-vous à la section « Reporting (Création de rapports) » du manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

Suivi des identités

Sentinel fournit une structure d'intégration qui permet d'identifier les systèmes de gestion et d'effectuer le suivi des identités de chaque compte utilisateur et des événements réalisés par ces identités. Sentinel fournit des informations utilisateur telles que les informations sur les contacts, les comptes utilisateur, les événements d'authentification et d'accès récents, les changements d'autorisation, etc. En affichant des informations sur les utilisateurs initiant une opération spécifique ou sur les utilisateurs affectés par une opération, Sentinel améliore le temps de réponse aux incidents et permet une analyse basée sur le comportement. Pour plus d'informations, reportez-vous à la section « Leveraging Identity Information » (Utilisation des informations sur l'identité) du manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

Analyse d'événements

Sentinel fournit un ensemble puissant d'outils qui vous permettent de rechercher et d'analyser facilement les données d'événement critiques. Sentinel optimise le système pour une efficacité optimale dans tout type d'analyse et fournit des méthodes simples pour des transitions transparentes d'un type d'analyse à un autre.

Dans Sentinel, les investigations relatives aux événements commencent souvent par les vues d'événement pratiquement en temps réel. Bien qu'il existe des outils plus élaborés, les flux d'événements filtrés et les graphiques récapitulatifs affichés dans les vues d'événement vous permettent de réaliser des analyses simples et rapides des tendances et données d'événement, mais aussi d'identifier des événements spécifiques. Avec le temps, vous pouvez créer des filtres personnalisés pour des classes de données spécifiques telles que la sortie depuis la corrélation. Vous pouvez utiliser les vues d'événement comme un tableau de bord qui présente la stratégie globale d'utilisation et de sécurité.

La recherche interactive permet alors d'effectuer une analyse détaillée des événements. Vous pouvez rechercher facilement et rapidement les données concernant une interrogation spécifique, par exemple une activité par un utilisateur spécifique ou sur un système donné. En cliquant sur les données d'événement ou en utilisant le panneau de filtrage à gauche, vous pouvez accéder aux événements spécifiques rapidement.

Lors de l'analyse de centaines d'événements, les fonctionnalités de création de rapports de Sentinel offrent un contrôle personnalisé sur la disposition des événements et peuvent afficher des volumes importants de données. Sentinel simplifie cette transition en vous permettant de transférer les recherches interactives créées dans l'interface de recherche vers un modèle de création de rapports. Cela crée instantanément un rapport qui affiche les mêmes données, mais dans un format plus adapté pour un grand nombre d'événements.

Sentinel comprend de nombreux modèles de création de rapports à cette fin. Il existe deux types de modèles de création de rapports :

- Des modèles précis pour afficher des types spécifiques d'informations, telles que des données d'authentification ou de création d'utilisateur.
- Des modèles génériques qui vous permettent de personnaliser des groupes et des colonnes de manière interactive sur le rapport.

Avec le temps, vous développerez des filtres que vous utiliserez régulièrement, ainsi que des rapports qui facilitent les workflows. Sentinel gère le stockage de ces informations et leur distribution auprès des membres de votre organisation. Pour plus d'informations, reportez-vous au manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

II Planification de votre installation Sentinel

Les chapitres suivants vous guident au cours de la planification de votre installation de Sentinel. Si vous souhaitez effectuer une configuration qui n'est pas abordée dans les chapitres suivants ou pour toute question, contactez le support technique de .

3 Liste de contrôle pour la mise en œuvre

Utilisez la liste de contrôle suivante pour planifier, installer et configurer Sentinel.

Si vous effectuez une mise à niveau à partir d'une version précédente de Sentinel, n'utilisez pas cette liste de contrôle. Pour plus d'informations sur la mise à niveau, reportez-vous à la Partie V, « Mise à niveau de Sentinel », page 149.

❒	Tâches	Voir
❒	Passez en revue les informations relatives à l'architecture du produit pour en savoir plus sur les composants Sentinel.	Partie I, « Présentation de Sentinel », page 13.
❒	Passez en revue les informations d''octroi de licence Sentinel pour déterminer si vous devez utiliser la licence d'évaluation ou la licence Sentinel destinée aux entreprises.	Chapitre 4, « Présentation des informations de licence », page 35.
❒	Évaluez votre environnement pour déterminer la configuration matérielle. Veillez à ce que les ordinateurs sur lesquels vous installez Sentinel et ses composants disposent de la configuration requise.	Chapitre 5, « Configuration du système », page 39.
❒	Déterminez le type de déploiement adapté à votre environnement en fonction des événements par seconde (EPS). Déterminez le nombre d'instances Collector Manager et Correlation Engine que vous devez installer pour améliorer les performances et l'équilibrage de la charge.	Chapitre 6, « Considérations sur le déploiement », page 41.
❒	Consultez les dernières notes de version de Sentinel afin de comprendre les nouvelles fonctionnalités et les problèmes connus.	Notes de version de Sentinel
❒	Installez Sentinel.	Partie III, « Installation de Sentinel », page 73.
❒	Configurez Sentinel.	Partie IV, « Configuration de Sentinel », page 117.
❒	Sentinel inclut des règles de corrélation prêtes à l'emploi. Certaines règles de corrélation sont configurées par défaut, pour exécuter une opération (par exemple, avertir l'administrateur de sécurité) qui envoie un message électronique lors du déclenchement de la règle. Vous devez donc configurer les paramètres du serveur de messagerie au niveau du serveur Sentinel en configurant l'intégrateur SMTP et l'opération Envoyer un message électronique.	Reportez-vous à la documentation concernant l'intégrateur SMTP et l'opération Envoyer un message électronique sur le site Web des plug-ins Sentinel.
❒	Installez les collecteurs et connecteurs supplémentaires nécessaires dans votre environnement.	Chapitre 16, « Installation de collecteurs et de connecteurs supplémentaires », page 113.

❒	Tâches	Voir
❒	Installez les instances Collector Manager et Correlation Engine supplémentaires nécessaires dans votre environnement.	Partie III, « Installation de Sentinel », page 73.

4 Présentation des informations de licence

Sentinel inclut un large spectre de fonctionnalités pour répondre aux divers besoins de ces nombreux clients. Vous pouvez choisir un modèle d'octroi de licence adapté à vos besoins.

La plate-forme Sentinel fournit les deux modèles d'octroi de licence suivants :

- **Sentinel Enterprise :** une solution complète qui comprend toutes les principales fonctions d'analyse visuelle en temps réel, ainsi que de nombreuses fonctionnalités supplémentaires. Sentinel Enterprise s'appuie sur des cas d'utilisation de la solution SIEM comme la détection des menaces en temps réel, les alertes et le traitement.
- **Sentinel for Log Management :** une solution pour des cas d'utilisation de gestion des logs comme la possibilité de collecter, de stocker et de rechercher des données, ainsi que de créer des rapports sur ces dernières.

  Sentinel for Log Management représente une mise à niveau substantielle de la fonctionnalité de Sentinel Log Manager 1.2.2, et dans certains cas, des parties importantes de l'architecture ont été modifiées. Pour planifier votre mise à niveau vers Sentinel for Log Management, consultez la page FAQ de Sentinel.

En fonction des solutions et produits complémentaires que vous achetez, vous pouvez acquérir les droits et clés de licence appropriés pour activer la fonctionnalité adéquate dans Sentinel. Les droits et clés de licence régissent l'accès standard aux fonctions et téléchargements des produits. Reportez-vous à votre contrat d'achat et à votre accord de licence utilisateur final pour consulter les termes contractuels supplémentaires.

Le tableau suivant décrit les services et fonctions spécifiques de chacune des solutions :

Tableau 4-1 *Services et fonctions Sentinel*

Services et fonctions	Sentinel Enterprise	Sentinel for Log Management
Fonctionnalité principale ◆ Collecte des événements, analyse, normalisation et classification taxonomique ◆ Collecte des données non liées aux événements (données relatives aux ressources, aux vulnérabilités et à l'identité des utilisateurs) ◆ Assignation contextuelle en ligne ◆ Stockage des événements à l'aide des stratégies de conservation et du non-rejet ◆ Routage des événements vers le stockage traditionnel (interne et externe) ◆ Recherches et visualisation des événements ◆ Visualisation, stockage et collecte de flux IP ◆ Création de rapports ◆ Activation FIPS 140-2 (Federal Information Processing Standard Publication 140-2) ◆ Opérations déclenchées manuellement ◆ Création et gestion manuelles des incidents	Oui	Oui
Sentinel Link	Oui	Oui
Synchronisation des données	Oui	Oui
Restauration des données d'événements à partir des archives	Oui	Oui
Fédération des données (recherche distribuée)	Oui	Oui
Détection d'exploits (Advisor)*	Oui	Oui
Stockage évolutif	Oui	Oui
Corrélation ◆ Corrélation de modèles d'événement en temps réel ◆ Opérations déclenchées par des règles de corrélation ◆ Triage des alertes ◆ Visualisation des alertes	Oui	Non
Security Intelligence ◆ Règles d'anomalie ◆ Analyse statistique en temps réel	Oui	Non

*Advisor, fourni par Security Nexus, est un service complémentaire. L'utilisation de ce service nécessite l'achat d'une licence supplémentaire.

Licences Sentinel

Cette section fournit des informations sur les types de licences Sentinel.

Licence d'évaluation

La licence d'évaluation par défaut vous permet d'utiliser toutes les fonctions de Sentinel Enterprise au cours d'une période d'évaluation donnée avec un taux illimité d'EPS, selon la capacité de votre matériel. Pour plus d'informations sur les fonctionnalités disponibles dans Sentinel Enterprise, consultez le Tableau 4-1, « Services et fonctions Sentinel », page 36.

La date d'expiration du système est basée sur les données les plus anciennes du système. Si vous restaurez des événements anciens sur votre système, Sentinel met à jour la date d'expiration en conséquence.

Une fois la licence d'évaluation arrivée à expiration, Sentinel s'exécute avec une licence de base, gratuite, qui offre un ensemble restreint de fonctionnalités et un taux d'événements limité à 25 EPS. Ceci vaut uniquement si Sentinel est configuré pour utiliser le stockage traditionnel.

Dans les déploiements de stockage évolutif, Sentinel ne stocke plus les événements ni les données brutes lorsque la licence d'évaluation arrive à expiration.

Lorsque vous effectuez la mise à niveau vers une licence d'entreprise, toutes les fonctionnalités de Sentinel sont restaurées. Pour éviter de ne plus pouvoir utiliser l'ensemble des fonctionnalités, vous devez effectuer la mise à niveau du système à l'aide d'une licence d'entreprise avant l'expiration de la licence d'évaluation.

Licence gratuite

La licence gratuite vous permet d'utiliser un ensemble restreint de fonctionnalités et un taux d'événements limité à 25 EPS. La licence gratuite n'est valable que si Sentinel utilise un stockage traditionnel.

La licence gratuite vous permet de collecter et de stocker des événements. Lorsque le taux d'EPS dépasse 25, Sentinel stocke les événements reçus, mais n'en affiche pas les détails de ces derniers dans les résultats de recherche ni dans les rapports. Sentinel identifie ces événements avec la balise `OverEPSLimit`.

La licence gratuite n'offre pas de fonctionnalités en temps réel. Vous pouvez récupérer l'ensemble des fonctionnalités en mettant à niveau la licence vers une licence d'entreprise.

REMARQUE : Le support technique et les mises à jour de produit ne sont pas disponibles pour la version gratuite de Sentinel.

Licences d'entreprise

Lorsque vous faites l'acquisition de Sentinel, vous recevez une clé de licence par l'intermédiaire du portail client. En fonction de la licence achetée, votre clé de licence active un taux de collecte des données, certaines fonctions et sources d'événements. Certaines clauses supplémentaires de la licence peuvent ne pas être appliquées par la clé de licence ; veuillez donc lire attentivement l'accord de licence.

Pour modifier votre licence, contactez le gestionnaire de votre compte.

Vous pouvez ajouter la clé de licence d'entreprise pendant l'installation ou à tout moment après l'installation. Pour ajouter la clé de licence, reportez-vous à la section « Adding a License Key » (Ajout d'une clé de licence) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

5 Configuration du système

Les recommandations nécessaires à l'implémentation de Sentinel dépendent de votre environnement informatique, vous devez donc contacter les services consulting ou un partenaire Sentinel avant de finaliser l'architecture Sentinel pour votre environnement.

Pour plus d'informations sur la configuration matérielle recommandée, les systèmes d'exploitation pris en charge, les plates-formes d'applicatifs et les navigateurs, consultez le site Web des informations techniques relatives à Sentinel.

Configuration système requise des connecteurs et des collecteurs

Chaque connecteur et collecteur dispose de son propre ensemble de configuration système et de plates-formes prises en charge. Reportez-vous à la documentation relative au connecteur et au collecteur sur le site Web des plug-ins Sentinel.

Environnement virtuel

Sentinel est pris en charge sur les serveurs VMware ESX. Lorsque vous configurez un environnement virtuel, les machines virtuelles doivent disposer de deux UC ou plus. Pour obtenir des performances identiques aux résultats des tests effectués sur la machine physique sous ESX ou dans tout autre environnement virtuel, les caractéristiques de mémoire, de processeur, d'espace disque et d'E/S de l'environnement virtuel doivent être conformes aux recommandations applicables à la machine physique.

Pour plus d'informations sur les recommandations applicables à la machine physique, consultez le site Web des informations techniques concernant Sentinel.

6 Considérations sur le déploiement

Sentinel dispose d'une architecture évolutive qui peut gérer la charge que vous devez y placer. Ce chapitre présente les points essentiels à prendre en compte lors de l'évolution d'un déploiement Sentinel. Un spécialiste du support technique de ou des services dédiés aux partenaires de peut vous aider à concevoir le système Sentinel adapté à votre environnement informatique.

Considérations relatives au stockage de données

Selon le taux d'événements par seconde, vous pouvez choisir d'utiliser un stockage traditionnel ou évolutif pour stocker et indexer vos données Sentinel. Votre déploiement Sentinel dépend de la solution de stockage des données que vous choisissez d'utiliser.

Tableau 6-1 *Comparaison entre le stockage traditionnel et évolutif*

Stockage traditionnel	Stockage évolutif
Par défaut, les données sont stockées dans un espace de stockage traditionnel basé sur des fichiers et l'indexation s'effectue en local sur le serveur Sentinel. En plus du stockage des données basé sur des fichiers, vous pouvez également choisir de stocker et d'indexer les événements dans la zone de stockage des données de visualisation pour tirer parti des fonctionnalités de visualisation de données. Pour plus d'informations, reportez-vous à la section « Configuration de la zone de stockage de visualisation » page 45.	Les données sont stockées dans un espace de stockage évolutif Hadoop et l'indexation des données utilise un mécanisme d'indexation distribué évolutif.
Peut évoluer sans problème verticalement jusqu'à environ 20 000 EPS. Au-delà de cette valeur, vous devez ajouter des serveurs Sentinel supplémentaires pour pouvoir prendre en charge un taux d'EPS beaucoup plus élevé.	Peut évoluer sans difficulté vers un taux d'EPS horizontalement très élevé, par exemple, 1 million d'événements par seconde.
La charge de la collecte de données est répartie entre plusieurs serveurs Sentinel. Par conséquent, les données sont réparties sur plusieurs serveurs Sentinel et doivent être gérées individuellement.	La collecte des données est gérée par un seul serveur Sentinel. Par conséquent, la gestion des données et des ressources est centralisée sur un seul serveur Sentinel.
Le locataire des données est indiqué dans les données, mais elles ne sont pas pour autant séparées sur le disque en fonction de celui-ci.	Les données sont libellées et séparées en fonction de leur locataire sur le disque.
La disponibilité et la réplication des données doivent être effectuées manuellement ou à l'aide de mécanismes de stockage coûteux tels qu'un disque SAN.	La disponibilité et la réplication des données sont économiques puisque Hadoop s'exécute sur du matériel courant.

- « Planification du stockage traditionnel » page 43
- « Planification du stockage évolutif » page 46
- « Structure des répertoires de Sentinel » page 48

Planification du stockage traditionnel

Le stockage des données basé sur des fichiers est structuré en trois niveaux :

Stockage en ligne	Stockage primaire, intitulé auparavant stockage local.	Optimisé pour des écritures et des récupérations rapides. Stocke les dernières données d'événement collectées et les données d'événement les plus souvent recherchées.
	Stockage secondaire, intitulé auparavant stockage réseau. (facultatif)	Optimisé pour réduire l'utilisation de l'espace d'un stockage facultatif et moins coûteux, avec prise en charge de l'extraction rapide. Sentinel migre automatiquement les partitions de données vers l'espace de stockage secondaire.
	REMARQUE : l'utilisation de l'espace de stockage secondaire est facultative. Les rapports, recherches et stratégies de conservation des données fonctionnent de la même manière sur les partitions de données d'événement, qu'elles soient sur un espace de stockage primaire, secondaire ou les deux.	
Stockage hors ligne	Stockage d'archivage	Lorsque les partitions sont fermées, vous pouvez sauvegarder la partition sur le service de stockage de fichiers de votre choix, par exemple Amazon Glacier. Vous pouvez temporairement réimporter les partitions pour les utiliser dans le cadre d'une analyse a posteriori à long terme si nécessaire.

De même, vous pouvez configurer Sentinel pour extraire les données d'événement et les résumés de données d'événement vers une base de données externe à l'aide de stratégies de synchronisation des données. Pour plus d'informations, reportez-vous à la section « Configuring Data Synchronization (Configuration de la synchronisation des données) » du *Sentinel Administration Guide (Guide d'administration de NetIQ Sentinel 7.0.1)*.

Lorsque vous installez Sentinel, vous devez monter la partition de disque pour le stockage primaire au même emplacement que l'installation de Sentinel. Par défaut, il s'agit du répertoire `/var/opt/novell`.

Pour que les calculs d'utilisation du disque soient corrects, l'ensemble de la structure du répertoire `/var/opt/novell/sentinel` doit se trouver sur une seule partition de disque. À défaut, les fonctionnalités de gestion automatique des données risquent de supprimer des données d'événement prématurément. Pour plus d'informations sur la structure du répertoire Sentinel, reportez-vous au « Structure des répertoires de Sentinel » page 48.

Nous vous recommandons de stocker ce répertoire sur une partition de disque distincte de celle qui contient les fichiers exécutables, de configuration et du système d'exploitation. L'isolation des données variables présente l'avantage de faciliter la sauvegarde et la récupération des ensembles de fichiers en cas d'altération et d'offrir un degré de protection supplémentaire si la partition du disque venait à être saturée. Les performances globales des systèmes sont également améliorées, car les petits systèmes de fichiers sont plus efficaces. Pour plus d'informations, reportez-vous à l'article en anglais Disk Partitioning (Partitionnement de disque).

REMARQUE : Les systèmes de fichiers EXT3 ont une limite en matière de stockage de fichiers. En effet, un répertoire ne peut pas contenir plus de 32 000 fichiers ou sous-répertoires. Vous pouvez utiliser le système de fichiers XFS si vous envisagez d'avoir un grand nombre de stratégies de conservation ou de conserver les données pour de longues périodes, comme une année.

- « Utilisation de partitions dans des installations traditionnelles » page 44
- « Utilisation de partitions dans des installations d'applicatif » page 44

- « Meilleures pratiques en matière de disposition des partitions » page 44
- « Configuration de la zone de stockage de visualisation » page 45

Utilisation de partitions dans des installations traditionnelles

Sur les installations traditionnelles, vous pouvez modifier la disposition de la partition de disque du système d'exploitation avant d'installer Sentinel. L'administrateur doit créer et monter les partitions souhaitées dans les répertoires appropriés, en fonction de la structure de répertoires indiquée à la « Structure des répertoires de Sentinel » page 48. Lorsque vous exécutez le programme d'installation, Sentinel est installé dans les répertoires créés au préalable. En d'autres termes, l'installation s'étend sur plusieurs partitions.

REMARQUE :

- Vous pouvez utiliser l'option `--location` lors de l'exécution du programme d'installation afin d'indiquer un emplacement de stockage à la racine différent des répertoires par défaut. La valeur que vous transmettez à l'option `--location` est ajoutée au début des chemins d'accès aux répertoires. Par exemple, si vous indiquez `--location=/foo`, le répertoire des données est `/foo/var/opt/novell/sentinel/data` et le répertoire de configuration est `/foo/etc/opt/novell/sentinel/config`.
- Vous ne devez pas utiliser les liens du système de fichiers (les liens symboliques par exemple) pour l'option `--location`.

Utilisation de partitions dans des installations d'applicatif

Si vous utilisez un format d'applicatif DVD ISO, vous pouvez configurer le partitionnement du système de fichiers de l'applicatif au cours de l'installation en suivant les instructions affichées dans les écrans YaST. Par exemple, vous pouvez créer une partition distincte pour le point de montage `/var/opt/novell/sentinel` afin de placer l'ensemble des données sur une partition distincte. Toutefois, pour les autres formats d'applicatif, vous ne pouvez configurer le partitionnement qu'après l'installation. L'outil de configuration système SuSE YaST permet d'ajouter des partitions et de déplacer un répertoire vers la nouvelle partition. Pour plus d'informations sur la création de partitions après l'installation, reportez-vous à la « Création de partitions pour le stockage traditionnel » page 109.

Meilleures pratiques en matière de disposition des partitions

De nombreuses organisations disposent de leurs propres meilleures pratiques en matière de schémas de disposition des partitions pour les programmes installés. La proposition suivante de partition a pour objet de guider les organisations qui n'ont pas de stratégie définie, et prend en compte l'utilisation spécifique par Sentinel du système de fichiers. En général, Sentinel se conforme à la norme de hiérarchie du système de fichiers si possible.

Partition	Point de montage	Taille	Remarques
Root	`/`	100 Go	Contient les fichiers du système d'exploitation et les fichiers binaires/la configuration Sentinel.
Boot	`/boot`	150 Mo	Partition de démarrage

Partition	Point de montage	Taille	Remarques
Stockage primaire	`/var/opt/novell/sentinel`	Effectuez votre calcul à l'aide des informations de dimensionnement des systèmes.	Cette zone contiendra les principales données Sentinel collectées, ainsi que d'autres données variables telles que les fichiers journaux. Cette partition peut être partagée avec d'autres systèmes.
Stockage secondaire	Emplacement basé sur le type de stockage, NFS, CIFS ou SAN.	Effectuez votre calcul à l'aide des informations de dimensionnemment des systèmes.	Il s'agit de la zone de stockage secondaire qui peut être montée localement, comme indiqué, ou à distance.
Stockage d'archivage	Système distant	Effectuez votre calcul à l'aide des informations de dimensionnement des systèmes.	Cet espace de stockage est destiné aux données archivées.

Configuration de la zone de stockage de visualisation

Sentinel fournit des visualisations d'événements qui présentent les données dans des graphiques, des tableaux et des assignations. Ces visualisations facilitent la visualisation et l'analyse de gros volumes d'événements. Vous pouvez également créer vos propres visualisations et tableaux de bord.

Sentinel tire parti de Kibana, un tableau de bord d'analyse et de recherche basé sur un navigateur, qui vous aide à rechercher et à analyser des événements. Kibana accède aux données de la zone stockage des données de visualisation (Elasticsearch) pour présenter les événements dans des tableaux de bord. Par défaut, Sentinel comprend un nœud Elasticsearch qui stocke et indexe uniquement les alertes. Vous devez activer la visualisation des événements pour stocker et indexer les événements dans Elasticsearch.

Lorsque vous activez Elasticsearch pour stocker et indexer des données, Sentinel indexe uniquement certains champs d'événement spécifiques requis pour les visualisations et stocke les champs indexés dans Elasticsearch. Sentinel crée un index spécial pour chaque jour et utilise le fuseau horaire UTC (de minuit à minuit) pour calculer la date de l'index. Le nom de l'index est au format `security.events.normalized_aaaaMMjj`. Par exemple, l'index `security.events.normalized_20160101` contient tous les événements qui se sont déroulés le 1er janvier 2016.

La configuration de la zone de stockage des données de visualisation implique les opérations suivantes :

- **Installation des nœuds Elasticsearch dans un mode en grappe :** Par défaut, Sentinel comprend un nœud Elasticsearch. Pour optimiser les performances et la stabilité du serveur Sentinel, il est obligatoire d'installer les nœuds Elasticsearch supplémentaires dans un mode en grappe. Pour plus d'informations, reportez-vous à la section Chapitre 12, « Installation et configuration d'Elasticsearch », page 79.
- **Activer la visualisation des événements :** La visualisation des événements est désactivée par défaut. Pour activer la visualisation des événements, reportez-vous à la section Chapitre 20, « Activation de la visualisation des événements », page 127.

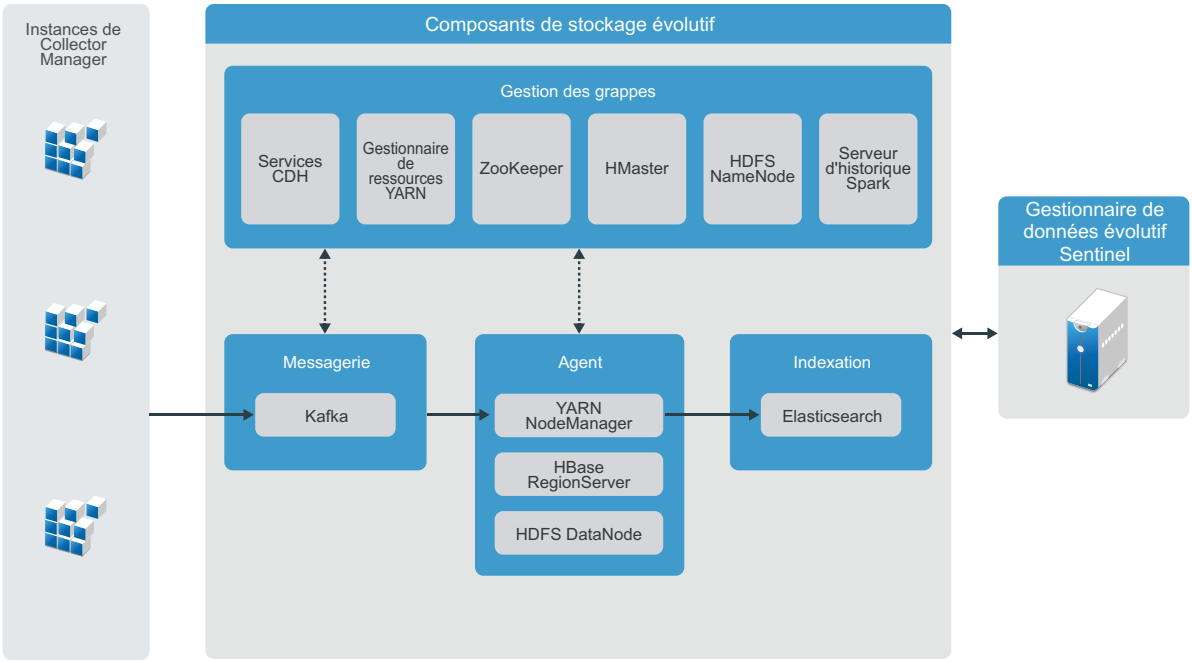
❒ **Réglage des performances :** Sentinel configure automatiquement certains paramètres Elasticsearch pour optimiser les performances. Vous pouvez personnaliser ces paramètres selon vos besoins. Par exemple, vous pouvez modifier les champs d'événement que vous souhaitez voir indexés par Elasticsearch. Pour plus d'informations, reportez-vous à la section « Réglage des performances pour Elasticsearch » page 85.

Planification du stockage évolutif

Sentinel utilise la distribution Cloudera, y compris l'infrastructure Apache Hadoop (CDH) pour stocker et gérer les gros volumes de données. Pour l'indexation des événements, Sentinel utilise un moteur d'indexation distribué, évolutif appelé Elasticsearch proposé par Elastic.

L'illustration suivante explique les différents composants du stockage évolutif :

Figure 6-1 *Architecture du stockage évolutif*



- **Messagerie :** Sentinel utilise Apache Kafka comme système de messagerie évolutif qui reçoit des événements normalisés ainsi que des données brutes de la part des instances Collector Manager. Les instances Collector Manager envoient des données brutes et d'événements aux grappes Kafka.

  Par défaut, Sentinel crée les rubriques Kafka suivantes :

  - **security.events.normalized :** stocke toutes les données d'événement traitées et normalisées, y compris les événements générés par le système et les événements internes.
  - **security.events.raw :** stocke toutes les données brutes provenant des sources d'événements.

  Les événements et les données brutes suivent le schéma Apache Avro. Pour plus d'informations, reportez-vous à la documentation d'Apache Avro. Les fichiers de schéma sont disponibles dans le répertoire `/etc/opt/novell/sentinel/scalablestore`.

- **Agent :** Ce noeud héberge des tâches de traitement en temps réel et de stockage. Apache Spark traite des données à grande échelle en temps réel. Ce traitement consiste notamment à séparer les événements en fonction de leur ID de locataire, nécessitant un grand volume de données ainsi qu'un grand volume de stockage sur le système des enregistrements (SOR) ainsi qu'une indexation évolutive.

  Apache HBase est une banque de données distribuée et évolutive basée sur Hadoop. Elle est utilisée comme SOR pour les événements normalisés et les données brutes, et trie les données en fonction de l'ID de leur locataire.

  En fonction de l'ID du locataire, Sentinel crée un espace de nom distinct pour chaque locataire. Par exemple, l'espace de nom pour le locataire par défaut est 1. Dans chaque espace de nom, Sentinel crée les tables suivantes et stocke les données en fonction de l'heure de l'événement.

  - ***<ID_locataire>*:security.events.normalized:** stocke toutes les données d'événement traitées et normalisées, y compris les événements générés par le système et les événements internes.
  - ***<ID_locataire>*:security.events.raw:** Stocke toutes les données brutes provenant des sources d'événements.
- **Gestion des grappes :** Ce noeud héberge tous les masters et services de gestion des grappes. Apache ZooKeeper agit comme un service centralisé pour la maintenance des informations de configuration, des services d'assignation de nom, offrant une synchronisation distribuée et des services de groupe.
- **Indexation :** Sentinel utilise Elasticsearch pour l'indexation distribuée et évolutive des événements. Vous pouvez accéder aux données à partir d'Elasticsearch pour rechercher et visualiser des événements.

  Sentinel crée un index spécial pour chaque jour et utilise le fuseau horaire UTC (de minuit à minuit) pour calculer la date de l'index. Le nom de l'index est au format `security.events.normalized_aaaaMMjj`. Par exemple, l'index `security.events.normalized_20160101` contient tous les événements qui se sont déroulés le 1er janvier 2016. Pour optimiser les performances, Sentinel n'indexe que certains champs d'événement spécifiques. Vous pouvez modifier les champs d'événement que vous souhaitez voir indexés par Elasticsearch. Pour plus d'informations, reportez-vous à la section « Réglage des performances pour Elasticsearch » page 85.

Configuration du stockage évolutif

Quand vous activez le stockage évolutif, l'interface utilisateur du serveur Sentinel est réduite à la plus grande simplicité : seules y figurent certaines fonctions de Sentinel notamment la collecte de données, la corrélation, le routage d'événements, la recherche et la visualisation des événements, et des activités d'administration. Cette version réduite de Sentinel est appelée SSDM (Sentinel Scalable Data Manager), autrement dit « gestionnaire de données évolutif Sentinel ». Pour accéder aux autres fonctionnalités de Sentinel comme Security Intelligence, la recherche classique et les rapports, vous devez installer des instances distinctes de Sentinel avec un stockage classique des données et acheminer les données d'événements spécifiques depuis SSDM à Sentinel via Sentinel Link.

La liste ci-dessous fournit des informations sur les services et les fonctions non disponibles dans SSDM :

- Rapports
- Security Intelligence
- Opérations sur les événements pendant la recherche
- Tests des règles de corrélation
- Création et gestion des incidents

- Opérations manuelles sur des événements
- Synchronisation des données
- Workflows iTRAC
- Analyse méthodique des événements déclencheurs de l'événement corrélé
- Visualisation des fichiers joints aux événements pour les événements Secure Configuration Manager et Change Guardian

L'activation du stockage évolutif est une configuration qui n'est effectuée qu'une seule fois et qui ne peut pas être annulée. Pour désactiver le stockage évolutif et passer au mode de stockage traditionnel, il faut réinstaller Sentinel.

La liste de contrôle suivante fournit des informations très détaillées sur les tâches à effectuer pour configurer un stockage évolutif :

Tableau 6-2 *Liste de contrôle pour la configuration du stockage évolutif*

	Tâches	Voir
❒	Passez en revue les informations de déploiement pour comprendre comment déployer Sentinel à l'aide d'un stockage évolutif.	« Déploiement à trois niveaux à l'aide du stockage évolutif » page 54
❒	Passez en revue les conditions préalables et effectuez l'ensemble des tâches requises.	Chapitre 13, « Installation et configuration du stockage évolutif », page 89.
❒	Activez le stockage évolutif. Vous pouvez activer le stockage évolutif durant l'installation ou après celle-ci. Pour les installations de mise à niveau, le stockage évolutif ne peut être activé qu'après la mise à niveau de Sentinel.	Pour activer le stockage évolutif pendant l'installation, effectuez une installation personnalisée de Sentinel. Reportez-vous à la « Installation personnalisée du serveur Sentinel » page 94. Pour activer le stockage évolutif après l'installation ou la mise à niveau, reportez-vous à la section Enabling Scalable Storage Post-Installation (Activation du stockage évolutif après l'installation) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
❒	Configurez les composants CDH et Elasticsearch à l'aide de Sentinel.	Section Configuring Scalable Storage (Configuration du stockage évolutif) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Structure des répertoires de Sentinel

Par défaut, les répertoires Sentinel se trouvent aux emplacements suivants :

- Les fichiers de données sont stockés dans les répertoires `/var/opt/novell/sentinel/data` et `/var/opt/novell/sentinel/3rdparty`.
- Les fichiers exécutables et les bibliothèques se trouvent dans le répertoire `/opt/novell/sentinel/`..
- Les fichiers journaux se trouvent dans le répertoire `/var/opt/novell/sentinel/log`.
- Les fichiers temporaires se trouvent dans le répertoire `/var/opt/novell/sentinel/tmp`.
- Les fichiers de configuration se trouvent dans le répertoire `/etc/opt/novell/sentinel`.

- Le fichier d'ID de processus (PID) se trouve dans le répertoire `/home/novell/run/sentinel/server.pid`.

  Le PID permet aux administrateurs d'identifier le processus parent du serveur Sentinel, et de surveiller ou d'y mettre fin.

Avantages des déploiements distribués

Par défaut, le serveur Sentinel comprend les composants suivants :

- **Collector Manager :** il fournit un point flexible de collecte de données pour Sentinel.
- **Correlation Engine :** il traite les événements à partir du flux d'événements en temps réel pour déterminer s'ils doivent déclencher l'une des règles de corrélation.
- **Elasticsearch :** Composant de stockage des données facultatif permettant de stocker et d'indexer des données. Par défaut, Sentinel comprend un nœud Elasticsearch. Si vous prévoyez beaucoup d'EPS, plus de 2 500, vous devez déployer des nœuds Elasticsearch supplémentaires dans une grappe.

IMPORTANT : Dans les environnements de production, vous pouvez configurer un déploiement distribué, car il isole les composants de collecte de données sur un ordinateur distinct, ce qui permet de gérer les pointes de trafic et les autres anomalies tout en garantissant une stabilité maximale du système.

Cette section décrit les avantages des déploiements distribués.

- « Avantages de l'installation d'instances Collector Manager supplémentaires » page 49
- « Avantages des instances Correlation Engine supplémentaires » page 50

Avantages de l'installation d'instances Collector Manager supplémentaires

Par défaut, le serveur Sentinel comprend une instance Collector Manager. Cependant, pour les environnements de production, les instances Collector Manager distribuées assurent un isolement bien supérieur lors de la réception de gros volumes de données. Dans ce cas, même si une instance Collector Manager distribuée est surchargée, le serveur Sentinel continue de répondre aux demandes de l'utilisateur.

L'installation de plusieurs instances Collector Manager dans un réseau distribué présente les avantages suivants :

- **Des performances système améliorées :** les instances Collector Manager supplémentaires peuvent analyser et traiter des données d'événements dans un environnement distribué, améliorant ainsi les performances système.
- **Une sécurité accrue des données et des exigences de bande passante moindres :** si les instances Collector Manager se trouvent au même emplacement que les sources d'événements, le filtrage, le chiffrement de même que la compression des données peuvent être effectués à la source.
- **Caching de fichiers :** les instances Collector Manager supplémentaires peuvent 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. Cette fonction est avantageuse pour les protocoles, tels que syslog qui ne prennent pas d'office en charge le caching d'événements.

Vous pouvez installer des instances Collector Manager supplémentaires aux emplacements appropriés sur votre réseau. Ces instances Collector Manager distantes exécutent des connecteurs et collecteurs et transfèrent les données collectées au serveur Sentinel à des fins de stockage et de traitement. Pour obtenir des informations sur l'installation d'instances Collector Manager supplémentaires, reportez-vous à la Partie III, « Installation de Sentinel », page 73.

REMARQUE : vous ne pouvez pas installer plusieurs instances Collector Manager sur le même système. En revanche, vous pouvez installer des instances Collector Manager supplémentaires sur des systèmes distants, puis les connecter au serveur Sentinel.

Avantages des instances Correlation Engine supplémentaires

Vous pouvez déployer plusieurs instances Correlation Engine, chacune sur son propre serveur, sans devoir répliquer de configurations ni ajouter des bases de données. Dans les environnements comptant un nombre élevé de règles de corrélation ou des taux d'événement extrêmement élevés, vous aurez avantage à installer plusieurs instances Correlation Engine et à redéployer certaines règles sur chaque nouvelle instance Correlation Engine. Ces instances Correlation Engine supplémentaires permettent de s'adapter à mesure que le système Sentinel intègre de nouvelles sources de données ou que les taux d'événements augmentent. Pour plus d'informations sur l'installation d'instances Correlation Engine supplémentaires, consultez la Partie III, « Installation de Sentinel », page 73.

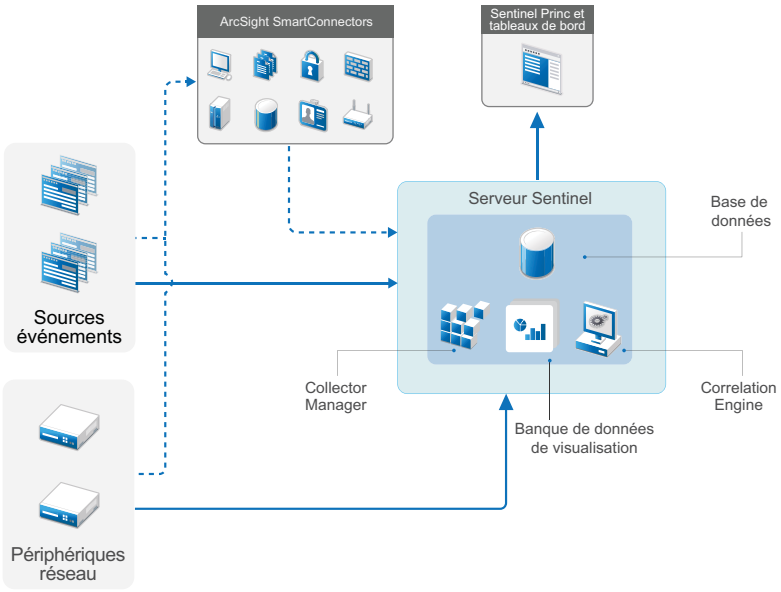
REMARQUE : vous ne pouvez pas installer plusieurs instances de Correlation Engine sur le même système. En revanche, vous pouvez installer des instances Correlation Engine supplémentaires sur des systèmes distants, puis les connecter au serveur Sentinel.

Déploiement tout-en-un

L'option de déploiement la plus basique est celle d'un système tout-en-un contenant tous les composants Sentinel sur un même ordinateur. Un déploiement tout-en-un convient uniquement si la charge du système est faible et si les machines Windows ne nécessitent aucune surveillance. Dans de nombreux environnements, des charges variables et imprévisibles, ainsi que des conflits de ressources entre composants peuvent entraîner des problèmes de performances.

IMPORTANT : Pour les environnements de production, vous pouvez configurer un déploiement distribué, car il isole les composants de collecte de données sur un ordinateur distinct, ce qui permet de gérer les pointes de trafic et les autres anomalies tout en garantissant une stabilité maximale du système.

Figure 6-2 *Déploiement tout-en-un*

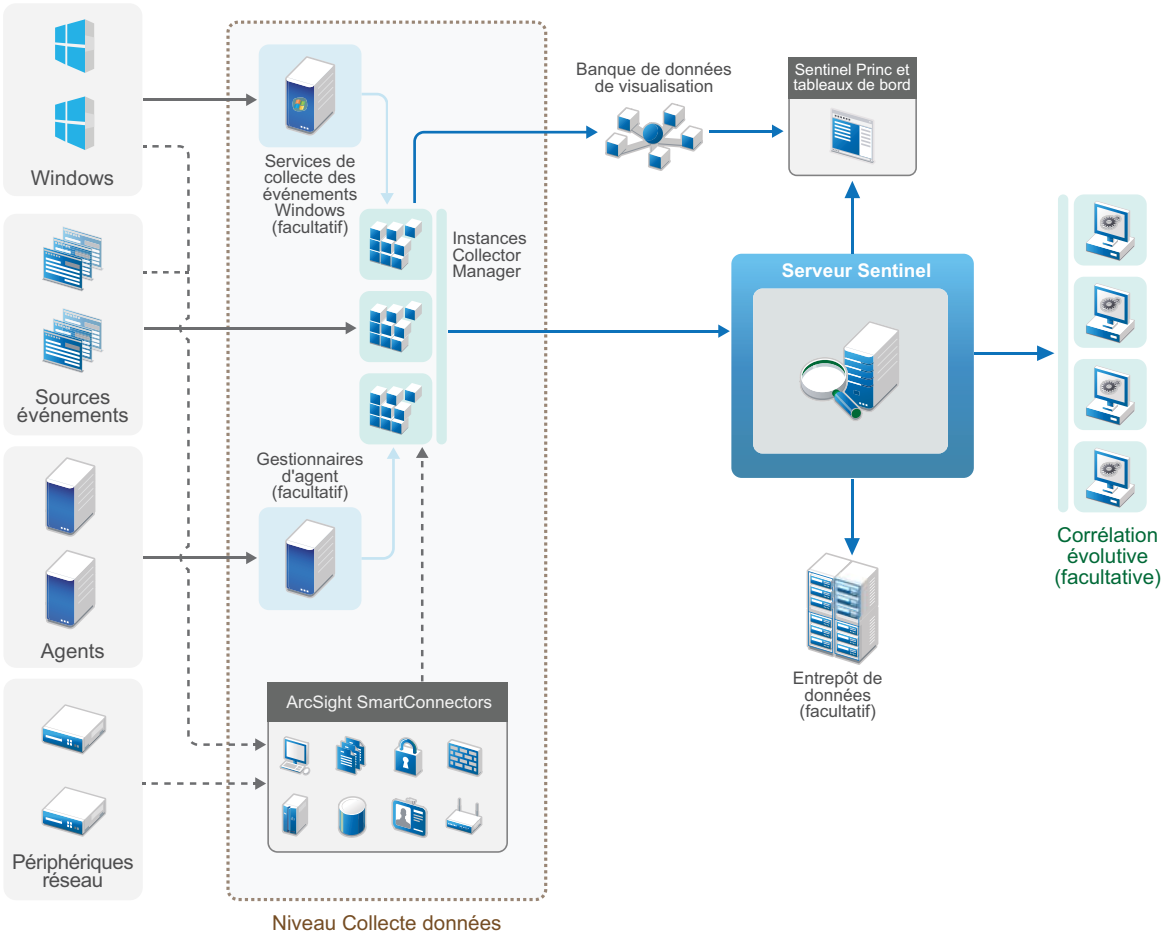


Déploiement distribué en un niveau

Le déploiement en un niveau permet de surveiller les ordinateurs Windows et de gérer des charges plus importantes que le déploiement tout-en-un. Vous pouvez distribuer la collecte et la corrélation de données en ajoutant des ordinateurs dédiés aux ordinateurs Collector Manager et Correlation Engine, qui déchargent le serveur Sentinel central de ces fonctions de traitement. Outre la gestion de la charge des événements et règles de corrélation, les gestionnaires des collecteurs et les moteurs de corrélation libèrent également des ressources sur le serveur central Sentinel qui peuvent servir à répondre à d'autres requêtes telles que le stockage d'événements et les recherches. Au fur et à mesure de l'augmentation de la charge sur le système, le serveur central Sentinel finit par devenir un goulot d'étranglement qui vous oblige à déployer d'autres niveaux afin d'améliorer l'évolutivité.

Vous pouvez également configurer Sentinel pour copier les données d'événements dans un entrepôt de données. Ce procédé peut être utile pour télécharger des rapports personnalisés ou des analyses, ou pour effectuer d'autres traitements sur un autre système.

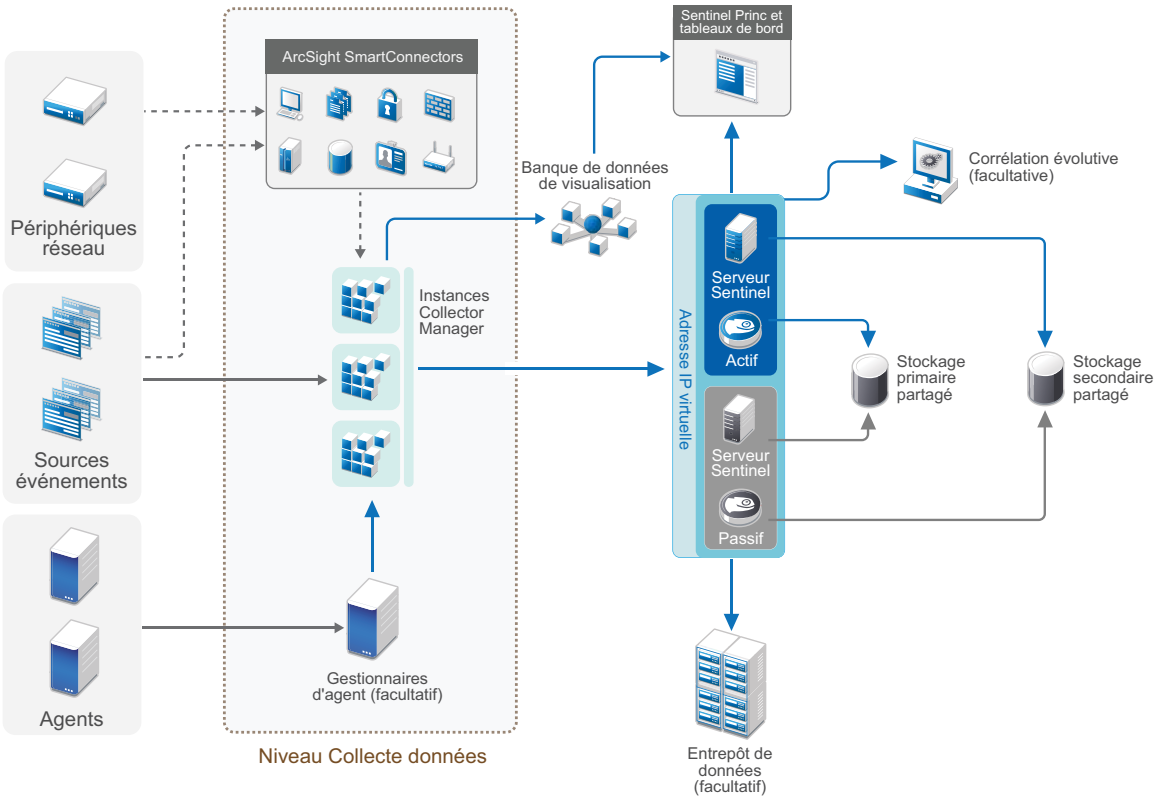
Figure 6-3 *Déploiement distribué en un niveau*



Déploiement distribué en un niveau avec haute disponibilité

Le déploiement distribué en un niveau indique comment il peut devenir un système à haute disponibilité et avec redondance pour reprise après échec. Pour plus d'informations sur le déploiement de Sentinel en haute disponibilité, reportez-vous à l'Partie VII, « Déploiement de Sentinel pour une haute disponibilité », page 189.

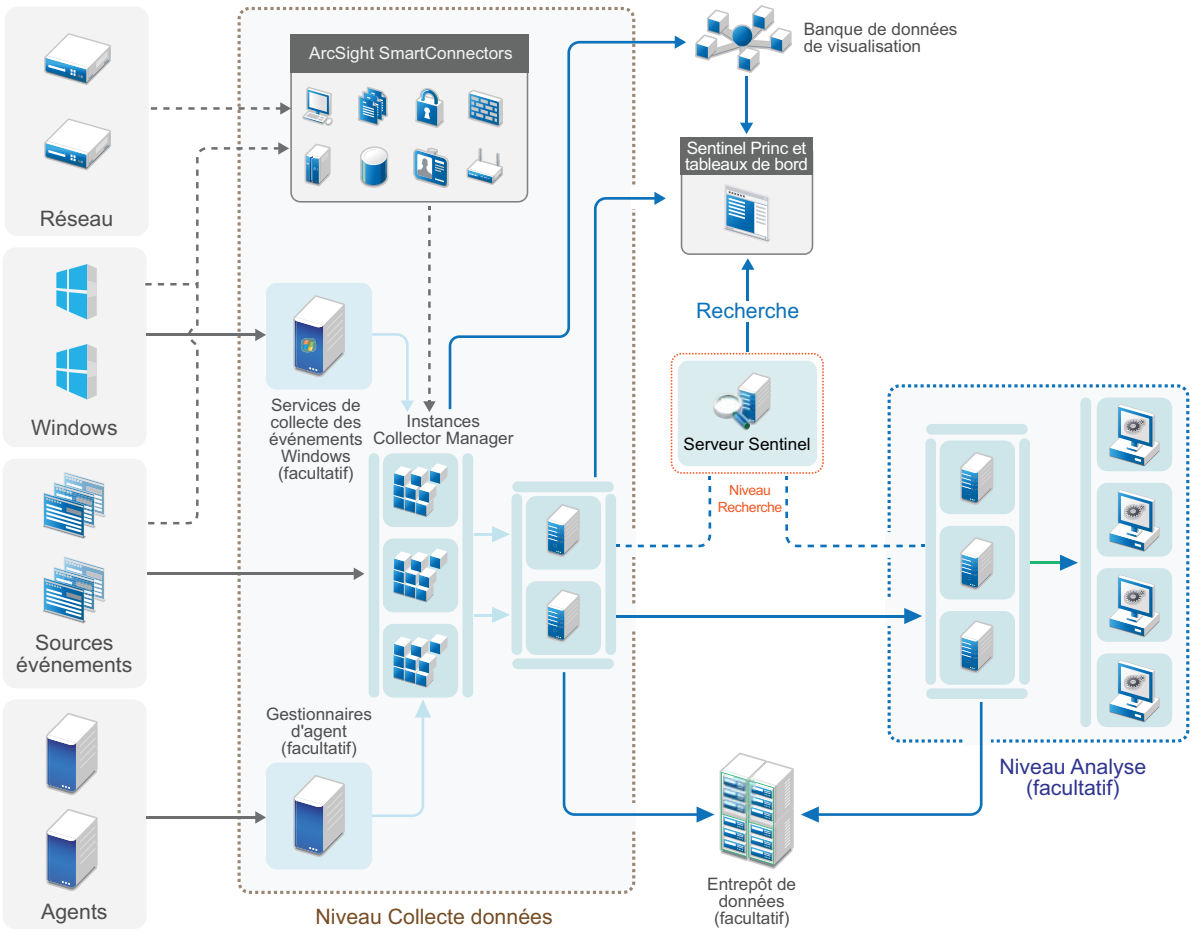
Figure 6-4 *Déploiement distribué en un niveau avec haute disponibilité*



Déploiement distribué en deux ou trois niveaux

Ces déploiements permettent de surpasser les fonctionnalités de gestion des charges d'un seul serveur central Sentinel et de répartir la charge de traitement entre plusieurs instances Sentinel en tirant parti des fonctionnalités de liaison et de fédération des données de Sentinel. La collecte des données équilibre la charge sur plusieurs serveurs Sentinel, chacun d'entre eux ayant plusieurs instances Collector Manager, comme l'indique le niveau de collecte des données. Si vous souhaitez effectuer une corrélation d'événements ou utiliser la fonctionnalité Security Intelligence, vous pouvez transmettre des données au niveau Analyses à l'aide de Sentinel Link. Grâce à la fonction de fédération des données de Sentinel, le niveau de recherche fournit un seul point d'accès pour les recherches sur tous les systèmes dans tous les autres niveaux. Lorsqu'une demande de recherche est fédérée sur plusieurs instances de Sentinel, ce déploiement dispose également de propriétés d'équilibrage de charge très utiles dans le cadre de l'évolutivité pour la gestion de charges de recherche lourdes.

Figure 6-5 *Déploiement distribué en deux ou trois niveaux*



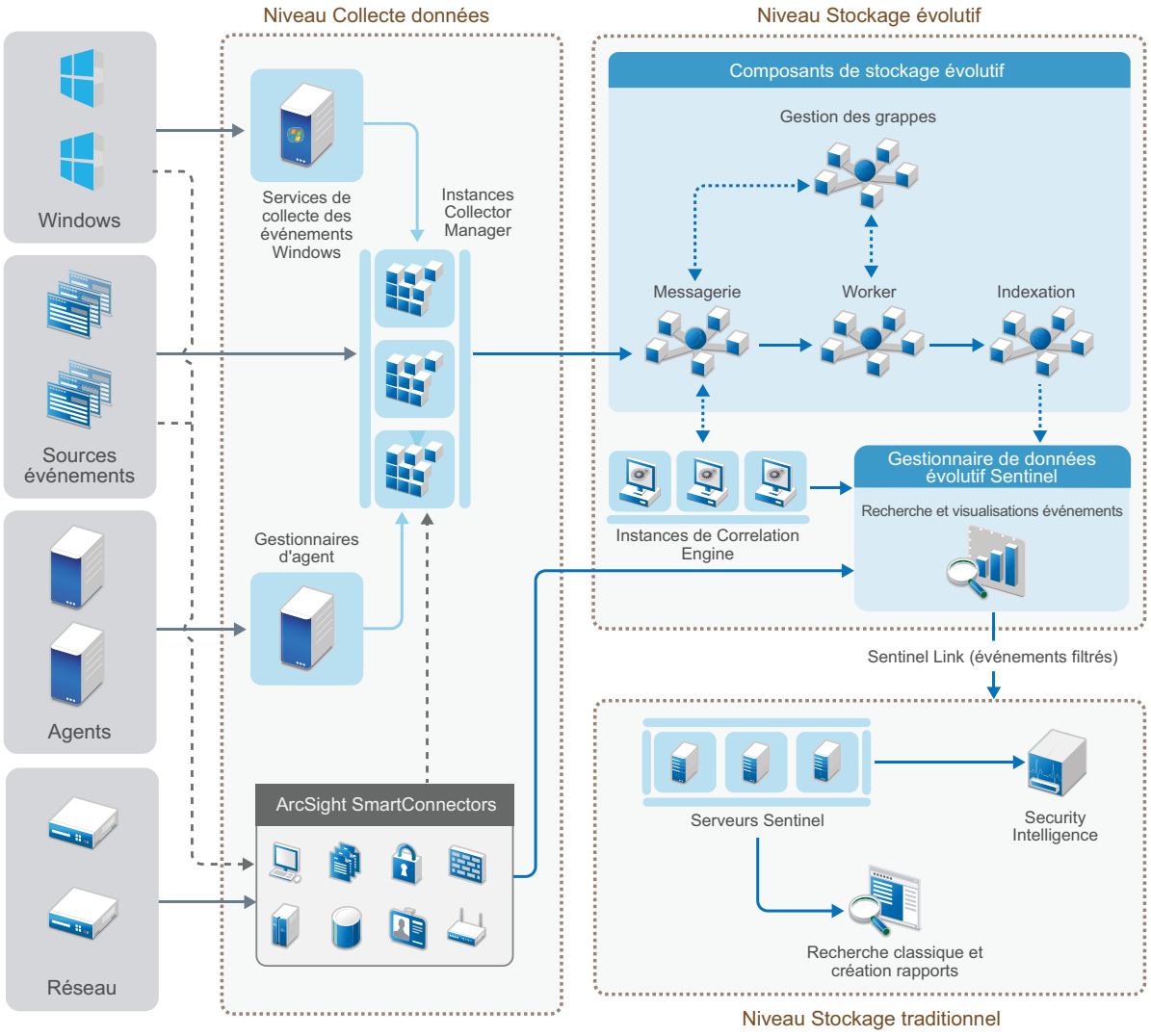
Déploiement à trois niveaux à l'aide du stockage évolutif

Lorsque vous devez traiter et stocker des données volumineuses sans pour autant devoir distribuer les événements sur plusieurs serveurs Sentinel ni dupliquer les paramètres de configuration sur plusieurs instances, vous pouvez configurer un déploiement distribué en trois niveaux à l'aide du stockage évolutif. Ce déploiement permet de stocker et de gérer des données volumineuses en n'employant qu'un seul serveur Sentinel au moyen du stockage évolutif au lieu d'utiliser plusieurs serveurs Sentinel.

Vous pouvez définir un nouveau serveur Sentinel avec stockage évolutif ou mettre à niveau votre serveur Sentinel existant afin d'activer le stockage évolutif.

Déterminez le paramétrage de votre déploiement Sentinel selon les fonctionnalités que vous souhaitez utiliser.

Figure 6-6 *Déploiement à trois niveaux pour le stockage évolutif*



Ce déploiement inclut les niveaux suivants :

- **Niveau Collecte de données :** pour collecter les événements à partir d'un large éventail de sources d'événements. Sinon, si vous souhaitez conserver votre configuration existante de collecte de données à l'aide d'un stockage Sentinel traditionnel tout en exploitant les capacités du stockage évolutif, vous pouvez faire suivre les effets souhaités directement depuis le stockage traditionnel vers le stockage évolutif grâce au script `data_uploader.sh`. Pour plus d'informations, reportez-vous à la section Chapitre 32, « Migration de données vers un stockage évolutif », page 179.
- **Niveau Stockage évolutif :** Pour stocker, indexer et analyser des données volumineuses. Le serveur SSDM à ce niveau vous permet de gérer la collecte et la corrélation de données et vous offre d'autres fonctionnalités SSDM. Pour utiliser les fonctionnalités Sentinel qui ne sont pas disponibles dans SSDM, vous pouvez configurer le niveau Stockage traditionnel. Vous pouvez également transférer les données collectées à un autre système SIEM ou activer d'autres outils d'informatique décisionnelle pour interroger des données ou effectuer des analyses directement sur votre distribution Hadoop via les API compatibles Hadoop, Kafka, Spark et Elasticsearch.

- **Niveau Stockage traditionnel :** Pour utiliser les fonctionnalités Sentinel comme Security Intelligence, la recherche classique et les rapports, vous devez installer des instances distinctes de Sentinel avec un stockage traditionnel. Vous pouvez configurer des règles de routage d'événements pour acheminer les événements souhaités depuis SSDM à Sentinel via Sentinel Link.

  Vous pouvez effectuer des recherches et créer des rapports à l'aide de l'un des serveurs Sentinel dans le niveau Stockage traditionnel. Vous pouvez configurer un niveau Recherche distinct qui fournit un point d'accès unique et pratique pour effectuer des recherches et créer des rapports sur tous les serveurs Sentinel au niveau Stockage traditionnel (facultatif). Pour lancer une recherche dans les événements du stockage évolutif, utilisez l'option de recherche de SSDM.

Pour plus d'informations sur l'installation et la configuration d'un stockage évolutif, reportez-vous au Chapitre 13, « Installation et configuration du stockage évolutif », page 89.

7 Considérations sur le déploiement pour le mode FIPS140-2

Vous pouvez éventuellement configurer Sentinel pour utiliser les services de sécurité réseau de Mozilla (NSS - Network Security Services), un module cryptographique certifié FIPS 140-2, pouvant servir au chiffrement interne et pour d'autres fonctions. Cette configuration permet de garantir que Sentinel intègre la certification FIPS 140-2 et est conforme aux normes et stratégies de l'administration fédérale américaine en matière d'achats.

Lorsque le mode FIPS 140-2 est activé dans Sentinel, la communication entre le serveur Sentinel, les instances Collector Manager Sentinel distantes, les instances Correlation Engine Sentinel distantes, l'interface principale de Sentinel, Sentinel Control Center et le service Sentinel Advisor utilisent une cryptographie certifiée FIPS 140-2.

IMPORTANT : Le mode FIPS est pris en charge uniquement pour Sentinel. Sentinel n'est pas pris en charge si le système d'exploitation est en mode FIPS.

Implémentation FIPS dans Sentinel

Sentinel utilise les bibliothèques NSS Mozilla fournies par le système d'exploitation. Red Hat Enterprise Linux (RHEL) et SUSE Linux Enterprise Server (SLES) ont différents ensembles de paquetages NSS.

Le module de chiffrement de NSS, à partir de RHEL 6.3, est conforme à la norme FIPS 140-2. Le module de chiffrement de NSS fourni avec SLES 11 n'est pas encore officiellement conforme à FIPS 140-2, mais la validation de la conformité du module SUSE avec cette norme est en cours. Une fois la validation obtenue, aucun changement ne devrait être apporté à Sentinel pour garantir l'intégration de « FIPS 140-2 Inside » sur la plate-forme SUSE.

Pour plus d'informations sur la certification RHEL FIPS 140-2, reportez-vous à https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2711 et https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1837.

Paquetages NSS RHEL

Pour prendre en charge le mode FIPS 140-2, Sentinel doit disposer des paquetages NSS 64 bits suivants :

- nspr-*
- nss-sysinit-*

- nss-util-*
- nss-softokn-freebl-*
- nss-softokn-*
- nss-*
- nss-tools-*

Si certains de ces paquetages ne sont pas installés, vous devez les installer avant d'activer le mode FIPS 140-2 dans Sentinel.

Paquetages NSS SLES

Pour prendre en charge le mode FIPS 140-2, Sentinel doit disposer des paquetages NSS 64 bits suivants :

- libfreebl3-*
- mozilla-nspr-*
- mozilla-nss-*
- mozilla-nss-tools-*

Si certains de ces paquetages ne sont pas installés, vous devez les installer avant d'activer le mode FIPS 140-2 dans Sentinel.

Composants compatibles FIPS dans Sentinel

Les composants Sentinel suivants prennent en charge le mode FIPS 140-2 :

- Tous les composants de la plate-forme Sentinel sont mis à jour pour prendre en charge le mode FIPS 140-2.
- Les plug-ins Sentinel suivants activés pour la cryptographie sont mis à jour pour prendre en charge le mode FIPS 140-2 :
  - Agent Manager Connector 2011.1r1 et versions ultérieures
  - Database (JDBC) Connector 2011.1r2 et versions ultérieures
  - File Connector 2011.1r1 et versions ultérieures (uniquement si le type de source d'événements de fichiers est local ou NFS)
  - LDAP Integrator 2011.1r1 et versions ultérieures
  - Sentinel Link Connector 2011.1r3 et versions ultérieures
  - Sentinel Link Integrator 2011.1r2 et versions ultérieures
  - SMTP Integrator 2011.1r1 et versions ultérieures
  - Syslog Connector 2011.1r2 et versions ultérieures
  - Windows Event (WMI) Connector 2011.1r2 et versions ultérieures
  - Check Point (LEA) Connector 2011.1r2 et versions ultérieures
  - Syslog Integrator 2011.1r1 et versions ultérieures

  Pour plus d'informations sur la configuration de ces plug-ins Sentinel pour une exécution en mode FIPS 140-2, reportez-vous à la section « Configuration des plug-ins Sentinel pour une exécution en mode FIPS 140-2. » page 138.

Au moment de la parution de ce document, les connecteurs Sentinel qui prennent en charge la cryptographie de manière facultative n'avaient pas encore été mis à jour pour une compatibilité avec le mode FIPS 140-2. Toutefois, vous pouvez continuer à collecter des événements à l'aide de ces connecteurs. Pour plus d'informations sur l'utilisation de ces connecteurs avec Sentinel en mode FIPS 140-2, reportez-vous à la section « Utilisation de connecteurs non compatibles FIPS avec Sentinel en mode FIPS 140-2 » page 144.

- Cisco SDEE Connector 2011.1r1
- File Connector 2011.1r1 (les fonctionnalités CIFS et SCP impliquent un codage et ne fonctionneront pas en mode FIPS 140-2.
- Audit Connector 2011.1r1
- SNMP Connector 2011.1r1

Au moment de la parution de ce document, les intégrateurs Sentinel qui prennent en charge SSL n'avaient pas encore été mis à jour pour être compatibles avec le mode FIPS 140-2. Vous pouvez toutefois continuer à utiliser des connexions non chiffrées lorsque ces intégrateurs sont utilisés avec Sentinel en mode FIPS 140-2.

- Remedy Integrator 2011.1r1 ou version ultérieure
- SOAP Integrator 2011.1r1 ou version ultérieure

Tous les autres plug-ins Sentinel non repris dans la liste ci-dessus n'utilisent pas la cryptographie et ne sont pas affectés par l'activation du mode FIPS 140-2 dans Sentinel. Vous pouvez les utiliser avec Sentinel en mode FIPS 140-2 sans devoir effectuer la moindre étape supplémentaire.

Pour plus d'informations sur les plug-ins Sentinel, reportez-vous au site Web des plug-ins Sentinel. Si vous souhaitez que l'un des plug-ins n'ayant pas encore été mis à jour prenne en charge le mode FIPS, faites-en la demande à l'aide de Bugzilla.

Connexions de données affectées par le mode FIPS

Si Sentinel est en mode FIPS 140-2, vous ne pouvez pas effectuer de connexion chiffrée à Microsoft SQL Server. Cette considération affecte les types suivants d'opérations Sentinel :

- Stratégies de synchronisation des données à SQL Server
- Serveur Sentinel communiquant avec la base de données Agent Manager
- Connecteur de base de données collectant des données de SQL Server

Liste de contrôle pour la mise en œuvre

Le tableau suivant fournit un aperçu des tâches requises pour configurer Sentinel de manière à fonctionner en mode FIPS 140-2.

Tâches	Pour plus d'informations, reportez-vous à la section…
Planifiez le déploiement.	« Scénarios de déploiement » page 60.

Tâches	Pour plus d'informations, reportez-vous à la section…
Déterminez si vous devez activer le mode FIPS 140-2 pendant l'installation de Sentinel ou plus tard. Pour activer le mode FIPS 140-2 pendant l'installation de Sentinel, vous devez sélectionner la méthode d'installation personnalisée ou silencieuse lors de la procédure d'installation.	« Installation personnalisée du serveur Sentinel » page 94. « Installation silencieuse » page 99 Chapitre 23, « Activation du mode FIPS 140-2 dans une installation Sentinel existante », page 133
Configurez les plug-ins Sentinel pour qu'ils s'exécutent en mode FIPS 140-2.	« Configuration des plug-ins Sentinel pour une exécution en mode FIPS 140-2. » page 138.
Importez les certificats dans le keystore FIPS de Sentinel.	« Importation de certificats dans une base de données keystore FIPS » page 145

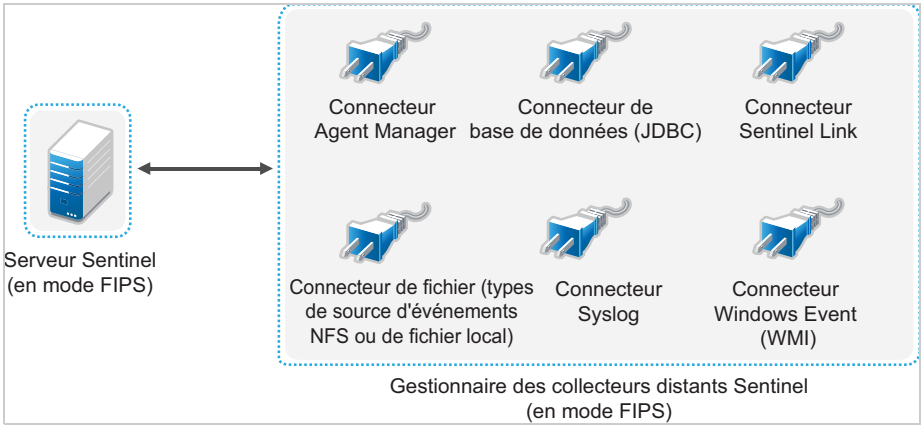
REMARQUE : Sauvegardez vos systèmes Sentinel avant de commencer la conversion au mode FIPS. Si le serveur doit être restauré en mode non FIPS par la suite, la seule méthode prise en charge implique la restauration à partir d'une sauvegarde. Pour plus d'informations sur la restauration en mode non FIPS, reportez-vous à la section « Rétablissement de Sentinel en mode non-FIPS » page 145.

Scénarios de déploiement

Cette section fournit des informations sur les scénarios de déploiement de Sentinel en mode FIPS 140-2.

Scénario 1 : collecte de données en mode FIPS 140-2 complet

Dans ce scénario, la collecte de données s'effectue uniquement via les connecteurs qui prennent en charge le mode FIPS 140-2. Cet environnement est supposé impliquer la présence d'un serveur Sentinel et une collecte de données via une instance Collector Manager distante. Vous pouvez avoir une ou plusieurs instances Collector Manager distantes.



Vous ne devez effectuer la procédure suivante que si votre environnement implique une collecte de données à partir de sources d'événements à l'aide de connecteurs compatibles avec le mode FIPS 140-2.

1 Votre serveur Sentinel doit être en mode FIPS 140-2.

REMARQUE : si le serveur Sentinel (que vous venez d'installer ou de mettre à jour) n'est pas en mode FIPS, faites-le basculer dans ce mode. Pour plus d'informations, reportez-vous à la section « Activation du serveur Sentinel pour une exécution en mode FIPS 140-2 » page 133.

---

2 Votre instance Collector Manager distante Sentinel doit être exécutée en mode FIPS 140-2.

REMARQUE : si l'instance Collector Manager distante (que vous venez d'installer ou de mettre à jour) n'est pas exécutée en mode FIPS, vous devez activer ce mode. Pour plus d'informations, reportez-vous à la section « Activation du mode FIPS 140-2 sur des instances Collector Manager et Correlation Engine distantes » page 134.

---

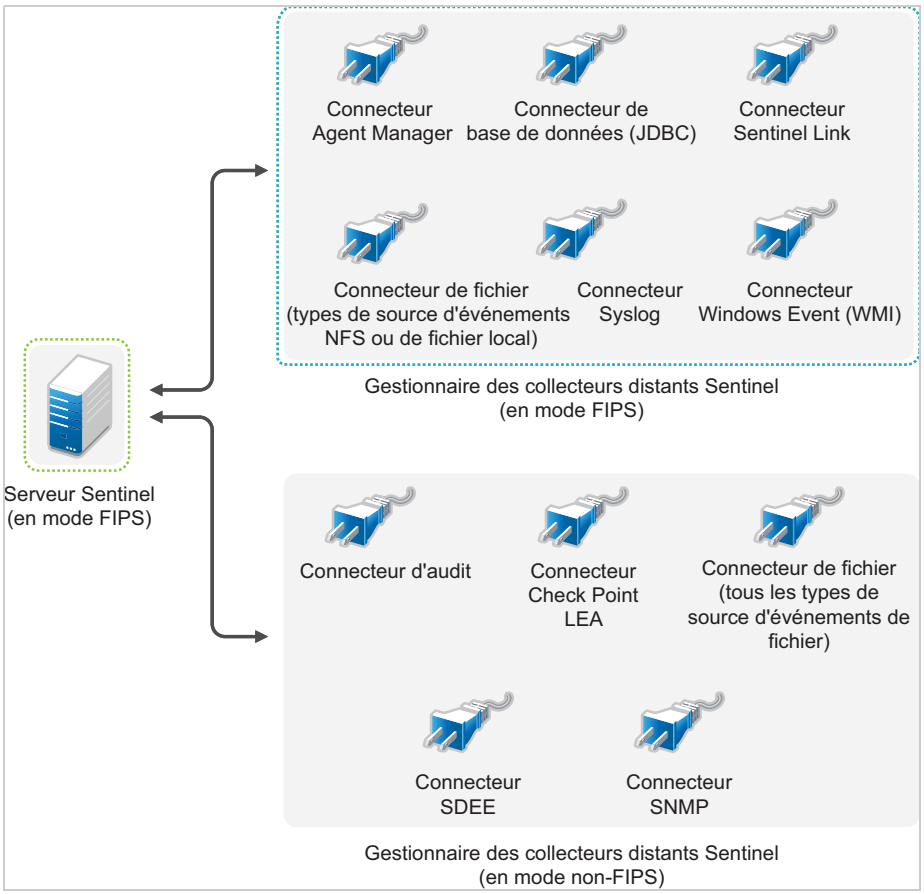
3 Veillez à ce que le serveur FIPS et les instances Collector Manager distantes communiquent entre elles.

4 Faites basculer les instances Correlation Engine distantes (le cas échéant) pour qu'elles s'exécutent en mode FIPS. Pour plus d'informations, reportez-vous à la section « Activation du mode FIPS 140-2 sur des instances Collector Manager et Correlation Engine distantes » page 134.

5 Configurez les plug-ins Sentinel pour qu'ils s'exécutent en mode FIPS 140-2. Pour plus d'informations, reportez-vous à la section « Configuration des plug-ins Sentinel pour une exécution en mode FIPS 140-2. » page 138.

Scénario 2 : collecte de données en mode FIPS 140-2 partiel

Dans ce scénario, la collecte de données s'effectue à l'aide de connecteurs prenant en charge le mode FIPS 140-2 et de connecteurs non compatibles avec ce mode. Nous supposons que les données sont collectées par le biais d'une instance Collector Manager distante. Vous pouvez avoir une ou plusieurs instances Collector Manager distantes.



Pour traiter la collecte de données à l'aide de connecteurs compatibles et non compatibles avec le mode FIPS 140-2, il est recommandé de disposer de deux instances Collector Manager distantes : l'une s'exécutant en mode FIPS 140-2 pour les connecteurs compatibles FIPS et l'autre s'exécutant en mode non FIPS (normal) pour les connecteurs ne prenant pas en charge ce mode.

Vous devez effectuer la procédure suivante si votre environnement implique une collecte de données à partir de sources d'événements à l'aide de connecteurs mixtes, à savoir des connecteurs prenant en charge le mode FIPS 140-2 et d'autres ne le prenant pas en charge.

1 Votre serveur Sentinel doit être en mode FIPS 140-2.

REMARQUE : si le serveur Sentinel (que vous venez d'installer ou de mettre à jour) n'est pas en mode FIPS, faites-le basculer dans ce mode. Pour plus d'informations, reportez-vous à la section « Activation du serveur Sentinel pour une exécution en mode FIPS 140-2 » page 133.

---

2 Veillez à ce qu'une instance Collector Manager distante s'exécute en mode FIPS 140-2 et que l'autre continue de s'exécuter en mode non-FIPS.

2a Si le mode FIPS 140-2 n'est activé sur aucune instance Collector Manager distante, vous devez l'activer sur l'un d'eux. Pour plus d'informations, reportez-vous à la section « Activation du mode FIPS 140-2 sur des instances Collector Manager et Correlation Engine distantes » page 134.

2b Mettez à jour le certificat de serveur sur l'instance Collector Manager distante non-FIPS. Pour plus d'informations, reportez-vous à la section « Mise à jour des certificats de serveur dans les instances Collector Manager et Correlation Engine distantes » page 137.

3 Veillez à ce que les deux instances Collector Manager distantes communiquent avec le serveur Sentinel compatible FIPS 140-2.

4 Configurez les instances Correlation Engine distantes (le cas échéant) pour qu'elles s'exécutent en mode FIPS 140-2. Pour plus d'informations, reportez-vous à la section « Activation du mode FIPS 140-2 sur des instances Collector Manager et Correlation Engine distantes » page 134.

5 Configurez les plug-ins Sentinel pour qu'ils s'exécutent en mode FIPS 140-2. Pour plus d'informations, reportez-vous à la section « Configuration des plug-ins Sentinel pour une exécution en mode FIPS 140-2. » page 138.

   5a Déployez les connecteurs qui prennent en charge le mode FIPS 140-2 dans l'instance Collector Manager distante s'exécutant en mode FIPS.

   5b Déployez les connecteurs qui ne prennent pas en charge le mode FIPS 140-2 dans l'instance Collector Manager distante non-FIPS.

8 Ports utilisés

Sentinel utilise divers ports pour la communication externe avec d'autres composants. Pour l'installation d'applicatifs, les ports sont par défaut ouverts au niveau du pare-feu. Toutefois, dans le cas d'une installation traditionnelle, vous devez configurer le système d'exploitation sur lequel vous installez Sentinel afin d'ouvrir les ports sur le pare-feu.

Ports du serveur Sentinel

Le serveur Sentinel utilise les ports suivants pour la communication interne et externe.

Ports locaux

Sentinel utilise les ports suivants pour la communication interne avec la base de données et d'autres processus internes :

Ports	Description
TCP 27017	Utilisé pour la base de données Security Intelligence.
TCP 28017	Utilisé pour la console Web de la base de données Security Intelligence.
TCP 32000	Utilisé pour la communication interne entre le processus wrapper et le processus serveur.
TCP 9200	Utilisé pour la communication avec le service d'indexation des alertes basée sur REST.
TCP 9300	Utilisé pour la communication avec le service d'indexation des alertes basée sur son protocole natif.

Ports réseau

Pour le bon fonctionnement de Sentinel, veillez à ce que les ports suivants soient ouverts au niveau du pare-feu :

Ports	Sens	Obligatoire/ facultatif	Description
TCP 5432	Entrant	Facultatif. Par défaut, ce port écoute uniquement sur l'interface en boucle.	Utilisé pour la base de données PostgreSQL. Il n'est pas nécessaire d'ouvrir ce port par défaut. Ce port doit cependant être ouvert lorsque vous développez des rapports à l'aide du SDK Sentinel. Pour plus d'informations, reportez-vous au site Web SDK de plug-ins Sentinel.

Ports	Sens	Obligatoire/ facultatif	Description
TCP 1099 et 2000	Entrant	Requis	Utilisés par les outils de surveillance pour établir la connexion au processus serveur Sentinel à l'aide de JMX (Java Management Extensions).
TCP 1289	Entrant	Facultatif	Utilisé pour les connexions Audit.
UDP 1514	Entrant	Facultatif	Utilisé pour les messages syslog.
TCP 8443	Entrant	Requis	Utilisé pour les communications HTTPS.
TCP 1443	Entrant	Facultatif	Utilisé pour les messages syslog codés avec SSL.
TCP 61616	Entrant	Facultatif	Utilisé pour les connexions entrantes des instances Collector Manager et Correlation Engine.
TCP 10013	Entrant	Requis	Utilisé par Sentinel Control Center et Solution Designer.
TCP 1468	Entrant	Facultatif	Utilisé pour les messages syslog.
TCP 10014	Entrant	Facultatif	Utilisé par les instances Collector Manager distantes afin d'établir la connexion au serveur par l'intermédiaire du proxy SSL. Ce port n'est toutefois pas courant. Par défaut, les instances Collector Manager distantes utilisent le port SSL 61616 pour établir la connexion au serveur.
TCP 443	Sortant	Facultatif	Si vous utilisez Advisor, le port initialise une connexion Internet avec le service Advisor via la page des mises à jour Advisor.
TCP 8443	Sortant	Facultatif	Si vous utilisez une fédération des données, le port initialise une connexion avec les autres systèmes Sentinel pour effectuer une recherche distribuée.
TCP 389 ou 636	Sortant	Facultatif	Si une authentification LDAP est utilisée, le port initialise une connexion avec le serveur LDAP.
TCP/UDP 111 et TCP/UDP 2049	Sortant	Facultatif	Si le stockage secondaire est configuré pour utiliser NFS.
TCP 137, 138, 139, 445	Sortant	Facultatif	Si le stockage secondaire est configuré pour utiliser CIFS.
TCP JDBC (selon la base de données)	Sortant	Facultatif	En cas de synchronisation des données, le port initialise une connexion avec la base de données cible à l'aide de JDBC. Le port utilisé dépend de la base de données cible.
TCP 25	Sortant	Facultatif	Initialise une connexion avec le serveur de messagerie.
TCP 1290	Sortant	Facultatif	Lorsque Sentinel transfère des événements à un autre système Sentinel, ce port initialise une connexion Sentinel Link à ce système.
UDP 162	Sortant	Facultatif	Lorsque Sentinel transfère des événements au système recevant des trappes SNMP, le port envoie un paquet au récepteur.
UDP 514 ou TCP 1468	Sortant	Facultatif	Ce port est utilisé lorsque Sentinel transfère des événements au système recevant des messages Syslog. Si le port UDP est utilisé, il envoie un paquet au récepteur. Si le port TCP est utilisé, il initialise une connexion avec le récepteur.

Ports	Sens	Obligatoire/ facultatif	Description
TCP 9443	Entrant	Facultatif	Ce port permet à un système Sentinel de recevoir des événements à partir d'autres logiciels SIEM tels que Change Guardian et Secure Configuration Manager.

Ports de l'applicatif du serveur Sentinel

Outre les ports ci-dessus, les ports suivants sont ouverts sur l'applicatif.

Ports	Sens	Obligatoire/ facultatif	Description
TCP 22	Entrant	Requis	Utilisé pour un accès shell sécurisé à l'applicatif Sentinel
TCP 4984	Entrant	Requis	Également utilisé par l'applicatif Sentinel pour le service de mise à jour.
TCP 289	Entrant	Facultatif	Réacheminé vers le port 1289 pour les connexions Audit.
TCP 443	Entrant	Facultatif	Réacheminé vers le port 8443 pour la communication HTTPS.
UDP 514	Entrant	Facultatif	Réacheminé vers le port 1514 pour les messages syslog.
TCP 1290	Entrant	Facultatif	Port Sentinel Link autorisé à se connecter par l'intermédiaire du pare-feu SuSE.
UDP et TCP 40000 - 41000	Entrant	Facultatif	Ports pouvant être utilisés lors de la configuration des serveurs de collecte de données, par exemple syslog. Par défaut, Sentinel n'écoute pas sur ces ports.
TCP 443 ou 80	Sortant	Requis	Initialise une connexion avec l'espace de stockage de la mise à jour logicielle de l'applicatif sur Internet ou un service SMT (Subscription Management Tool) sur votre réseau.
TCP 80	Sortant	Facultatif	Initialise une connexion avec le service SMT.
TCP 7630	Entrant	Requis	Utilisé par HAWK (High Availability Web Konsole).
TCP 9443	Entrant	Requis	Utilisé par la console de gestion de l'applicatif Sentinel.
TCP 1098 et 2000	Entrant	Requis	Utilisés par les outils de surveillance pour établir la connexion au processus serveur Sentinel à l'aide de JMX (Java Management Extensions).

Ports Collector Manager

Collector Manager utilise les ports suivants pour communiquer avec d'autres composants.

Ports réseau

Pour le bon fonctionnement de Collector Manager Sentinel, veillez à ce que les ports suivants soient ouverts au niveau du pare-feu :

Ports	Sens	Obligatoire/ facultatif	Description
TCP 1289	Entrant	Facultatif	Utilisé pour les connexions Audit.
UDP 1514	Entrant	Facultatif	Utilisé pour les messages syslog.
TCP 1443	Entrant	Facultatif	Utilisé pour les messages syslog codés avec SSL.
TCP 1468	Entrant	Facultatif	Utilisé pour les messages syslog.
TCP 1099 et 2000	Entrant	Requis	Utilisés par les outils de surveillance pour établir la connexion au processus serveur Sentinel à l'aide de JMX (Java Management Extensions).
TCP 61616	Sortant	Requis	Initialise une connexion avec le serveur Sentinel.
TCP 8443	Sortant	Requis	Initialise une connexion avec le port du serveur Web Sentinel. Laisse ce port ouvert uniquement pendant l'installation et la configuration de Collector Manager.

Ports de l'applicatif Collector Manager

Outre les ports ci-dessus, les ports suivants sont également ouverts sur l'applicatif Sentinel Collector Manager.

Ports	Sens	Obligatoire/ facultatif	Description
TCP 22	Entrant	Requis	Utilisé pour un accès shell sécurisé à l'applicatif Sentinel
TCP 4984	Entrant	Requis	Également utilisé par l'applicatif Sentinel pour le service de mise à jour.
TCP 289	Entrant	Facultatif	Réacheminé vers le port 1289 pour les connexions Audit.
UDP 514	Entrant	Facultatif	Réacheminé vers le port 1514 pour les messages syslog.
TCP 1290	Entrant	Facultatif	Port Sentinel Link autorisé à se connecter par l'intermédiaire du pare-feu SuSE.
UDP et TCP 40000 - 41000	Entrant	Facultatif	Utilisés pour la configuration des serveurs de collecte de données, tels que syslog. Par défaut, Sentinel n'écoute pas sur ces ports.
TCP 443	Sortant	Requis	Initialise une connexion avec l'espace de stockage de la mise à jour logicielle de l'applicatif sur Internet ou un service SMT (Subscription Management Tool) sur votre réseau.
TCP 80	Sortant	Facultatif	Initialise une connexion avec le service SMT.
TCP 9443	Entrant	Requis	Utilisé par la console de gestion de l'applicatif Sentinel.

Ports	Sens	Obligatoire/ facultatif	Description
TCP 1098 et 2000	Entrant	Requis	Utilisés par les outils de surveillance pour établir la connexion au processus serveur Sentinel à l'aide de JMX (Java Management Extensions).

Ports Correlation Engine

Correlation Engine utilise les ports suivants pour communiquer avec d'autres composants.

Ports réseau

Pour le bon fonctionnement de Sentinel Correlation Engine, veillez à ce que les ports suivants soient ouverts au niveau du pare-feu :

Ports	Sens	Obligatoire/ facultatif	Description
TCP 1099 et 2000	Entrant	Requis	Utilisés par les outils de surveillance pour établir la connexion au processus serveur Sentinel à l'aide de JMX (Java Management Extensions).
TCP 61616	Sortant	Requis	Initialise une connexion avec le serveur Sentinel.
TCP 8443	Sortant	Requis	Initialise une connexion avec le port du serveur Web Sentinel. Laisse ce port ouvert uniquement pendant l'installation et la configuration de Correlation Engine.

Ports de l'applicatif Correlation Engine

Outre les ports ci-dessus, les ports suivants doivent également être ouverts sur l'applicatif Sentinel Correlation Engine.

Ports	Sens	Obligatoire/ facultatif	Description
TCP 22	Entrant	Requis	Utilisé pour un accès shell sécurisé à l'applicatif Sentinel
TCP 4984	Entrant	Requis	Également utilisé par l'applicatif Sentinel pour le service de mise à jour.
TCP 443	Sortant	Requis	Initialise une connexion avec l'espace de stockage de la mise à jour logicielle de l'applicatif sur Internet ou un service SMT (Subscription Management Tool) sur votre réseau.
TCP 80	Sortant	Facultatif	Initialise une connexion avec le service SMT.
TCP 9443	Entrant	Requis	Utilisé par la console de gestion de l'applicatif Sentinel.
TCP 1098 et 2000	Entrant	Requis	Utilisés par les outils de surveillance pour établir la connexion au processus serveur Sentinel à l'aide de JMX (Java Management Extensions).

Ports de stockage évolutif

Pour que SSDM puisse communiquer correctement avec CDH et Elasticsearch, vérifiez que les ports que vous spécifiez lors de la configuration du stockage évolutif sont ouverts au niveau du pare-feu, en plus des ports requis par Cloudera et de ceux répertoriés à la section Ports du serveur Sentinel.

9 Options d'installation

Vous pouvez effectuer une installation traditionnelle de Sentinel ou installer l'applicatif. Ce chapitre fournit des informations sur les deux options d'installation.

Installation traditionnelle

L'installation traditionnelle installe Sentinel sur un système d'exploitation existant, en utilisant le programme d'installation d'applications. Vous pouvez installer Sentinel des manières suivantes :

- **Interactif :** L'installation nécessite la saisie d'informations par l'utilisateur. Pendant l'installation, vous pouvez enregistrer les options d'installation (informations saisies par l'utilisateur ou valeurs par défaut) dans un fichier que vous pouvez utiliser par la suite pour une installation silencieuse. L'installation peut être standard ou personnalisée.

Installation standard	Installation personnalisée
Utilise les valeurs par défaut pour la configuration. L'utilisateur ne doit indiquer que le mot de passe.	Invite à spécifier les valeurs pour la configuration. Vous pouvez sélectionner les valeurs par défaut ou indiquer les valeurs adéquates.
Installation avec la clé d'évaluation par défaut.	Vous permet d'effectuer l'installation avec la clé de licence d'évaluation par défaut ou avec une clé de licence valide.
Vous permet d'indiquer le mot de passe admin et l'utilise en tant que mot de passe par défaut pour les utilisateurs dbauser et appuser.	Vous permet d'indiquer le mot de passe admin. Pour les utilisateurs dbauser et appuser, vous pouvez indiquer un nouveau mot de passe ou utiliser le mot de passe admin.
Installation des ports par défaut pour tous les composants.	Vous permet d'indiquer les ports des différents composants.
Installe Sentinel en mode non-FIPS.	Vous permet d'installer Sentinel en mode FIPS 140-2.
Utilise le stockage traditionnel pour stocker les événements et les données brutes.	Vous permet d'utiliser un stockage évolutif pour stocker les événements et les données brutes.
Authentification des utilisateurs avec la base de données interne.	Permet de configurer l'authentification LDAP pour Sentinel en plus de l'authentification à la base de données. Lorsque vous configurez Sentinel avec l'authentification LDAP, les utilisateurs peuvent se connecter au serveur à l'aide de leurs informations d'identification Novell eDirectory ou Microsoft Active Directory.

Pour plus d'informations sur l'installation interactive, reportez-vous à la « Installation interactive » page 93.

- **Mode silencieux :** si vous souhaitez installer plusieurs serveurs Sentinel dans votre déploiement, vous pouvez enregistrer les options d'installation dans un fichier de configuration pendant l'installation standard ou personnalisée, puis utiliser ce fichier pour exécuter une installation silencieuse. Pour plus d'informations sur l'installation silencieuse, reportez-vous à la « Installation silencieuse » page 99.

Installation de l'applicatif

Le programme d'installation de l'applicatif installe Sentinel et le système d'exploitation SLES 12 SP3 64 bits.

L'applicatif Sentinel est disponible dans les formats suivants :

- image de l'applicatif OVF ;
- Image de l'applicatif ISO

Pour plus d'informations sur l'installation de l'applicatif, reportez-vous au Chapitre 15, « Installation de l'applicatif », page 103.

II Installation de Sentinel

Cette section fournit des informations sur l'installation de Sentinel et de composants supplémentaires.

10 Présentation générale de l'installation

Le programme d'installation par défaut de Sentinel installe les composants suivants sur le serveur Sentinel :

- **Processus serveur Sentinel et serveur Web Sentinel :** Le processus serveur Sentinel traite les demandes des autres composants de Sentinel et permet au système de fonctionner en toute transparence. Il traite des demandes visant à filtrer des données, effectuer des recherches et gérer des tâches administratives impliquant des autorisations et l'authentification des utilisateurs.

  Le serveur Web Sentinel permet d'établir une connexion sécurisée vers l'interface principale de Sentinel.
- **Base de données PostgreSQL :** Sentinel dispose d'une base de données intégrée qui stocke les informations de configuration, les données de ressources et de vulnérabilité, les informations d'identité, l'état des incidents et des workflows Sentinel, etc.
- **Base de données MongoDB :** elle stocke les données de Security Intelligence et d'alertes.
- **Elasticsearch :** Indexe les événements et les alertes pour la recherche et la visualisation.
- **Collector Manager :** il fournit un point flexible de collecte de données pour Sentinel. Le programme d'installation de Sentinel installe Collector Manager par défaut pendant l'installation.
- **Elasticsearch :** Composant de stockage des données facultatif permettant de stocker et d'indexer des données. Par défaut, Sentinel comprend un nœud Elasticsearch. Si vous prévoyez beaucoup d'EPS, plus de 2 500, vous devez déployer des nœuds Elasticsearch supplémentaires dans une grappe.
- **Correlation Engine :** il traite les événements à partir du flux d'événements en temps réel pour déterminer s'ils doivent déclencher l'une des règles de corrélation.
- **Advisor :** fourni par Security Nexus, Advisor est un service facultatif d'abonnement de données qui assure une corrélation au niveau des périphériques entre les événements en temps réel générés par les systèmes de détection d'intrusion et de prévention et par les résultats des analyses de vulnérabilité de l'entreprise. Pour plus d'informations sur Advisor, reportez-vous à la section « Detecting Vulnerabilities and Exploits » (Détection des vulnérabilités et des exploits) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
- **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. Vous pouvez télécharger des mises à jour et des plug-ins supplémentaires sur le site Web des plug-ins Sentinel. Les plug-ins Sentinel incluent notamment les éléments suivants :
  - Collecteurs
  - Connecteurs
  - Règles et opérations de corrélation
  - Rapports
  - Workflows iTRAC
  - Solution packs

11 Liste de contrôle de l'installation

Veillez à avoir effectué les tâches suivantes avant de commencer l'installation :

- ❒ Vérifiez que le matériel et le logiciel sont conformes à la configuration système requise indiquée dans la Chapitre 5, « Configuration du système », page 39.
- ❒ En cas d'installation antérieure de Sentinel, vérifiez qu'il ne reste aucun fichier ni paramètre système de cette installation. Pour plus d'informations, reportez-vous à la section section Annexe B, « Désinstallation », page 233.
- ❒ Si vous prévoyez d'installer la version sous licence, vous devez obtenir votre clé de licence auprès du Service clients .
- ❒ Vérifiez que les ports répertoriés au Chapitre 8, « Ports utilisés », page 65 sont ouverts dans le pare-feu.
- ❒ Pour que le programme d'installation de Sentinel fonctionne correctement, le système doit pouvoir renvoyer le nom d'hôte ou une adresse IP valide. Pour ce faire, ajoutez le nom d'hôte au fichier `/etc/hosts`, sur la ligne contenant l'adresse IP, puis entrez `hostname -f` pour que le nom d'hôte s'affiche correctement.
- ❒ Synchronisez l'heure à l'aide du protocole NTP (Network Time Protocol).
- ❒ Si vous envisagez de déployer Sentinel en configurant le stockage évolutif, veillez à avoir installé CDH et Elasticsearch. Pour plus d'informations sur le déploiement de Sentinel en utilisant un stockage évolutif, reportez-vous à la section « Installation et configuration du stockage évolutif » page 89.
- ❒ **Sur les systèmes RHEL :** Afin d'optimiser les performances, les paramètres de mémoire doivent être correctement configurés pour la base de données PostgreSQL. Le paramètre SHMMAX doit être supérieur ou égal à 1073741824.

  Pour définir la valeur appropriée, ajoutez les informations suivantes dans le fichier `/etc/sysctl.conf` :

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```

- ❒ **Pour les installations traditionnelles :**

  le système d'exploitation du serveur Sentinel doit comprendre au moins les composants Base Server du serveur SLES ou RHEL 6. Sentinel nécessite les versions 64 bits des RPM suivants :

  - bash
  - bc
  - coreutils
  - gettext
  - glibc
  - grep
  - libgcc
  - libstdc

- lsof
- net-tools
- openssl
- python-libs
- sed
- zlib

❒ **Pour Sentinel avec un stockage traditionnel :**

Pour afficher les visualisations d'événement, définissez la mémoire virtuelle en ajoutant la propriété `vm.max_map_count=262144` dans le fichier `/etc/sysctl.conf`.

12 Installation et configuration d'Elasticsearch

Pour l'indexation distribuée et évolutive des événements, vous devez installer Elasticsearch en mode grappe. La grappe Elasticsearch que vous installez pour Sentinel doit être utilisée pour indexer uniquement les données Sentinel.

Conditions préalables

Respectez les conditions préalables suivantes avant d'installer Elasticsearch :

- En fonction de votre taux d'événements par seconde (EPS), déployez Elasticsearch dans un mode en grappe avec le nombre de nœuds et de répliques tels que recommandés à la page Informations techniques pour Sentinel.
- Définissez les descripteurs de fichier en ajoutant les propriétés suivantes au fichier `/etc/security/limits.conf` :

  ```
  elasticsearch hard nofile 65536
  elasticsearch soft nofile 65536
  elasticsearch soft as unlimited
  ```

REMARQUE : Une fois les pré-requis ci-dessus remplis, exécutez la commande `sysctl -p` pour recharger les changements effectués dans les fichiers.

Installation et configuration d'Elasticsearch

Vous devez installer Elasticsearch et les plug-ins requis sur chaque nœud de la grappe Elasticsearch.

Pour installer et configurer Elasticsearch, procédez comme suit :

1. Installez la version JDK prise en charge par Elasticsearch.
2. Téléchargez la version certifiée du RPM Elasticsearch. Pour plus d'informations sur la version certifiée d'Elasticsearch et l'URL de téléchargement, reportez-vous à la page Technical Information for Sentinel (Informations techniques pour Sentinel).
3. Installez Elasticsearch :

   ```
   rpm -i elasticsearch -<version>.rpm
   ```
4. Réalisez les tâches affichées à l'écran dans les instructions post-installation de RPM.

5. Assurez-vous que l'utilisateur Elasticsearch a accès à Java.
6. Configurez le fichier `/etc/elasticsearch/elasticsearch.yml` en mettant à jour ou en ajoutant les informations suivantes :

Propriété et valeur	Remarques
cluster.name: <*nom_grappe_Elasticsearch*>	Le nom de grappe que vous spécifiez doit être identique pour tous les noeuds.
node.name: <*nom_noeud*>	Le nom de noeud doit être unique pour chaque noeud.
network.host: _<*InterfaceRéseau*>:ipv4_	
discovery.zen.ping.unicast.hosts : [<nom de domaine complet du nœud elasticsearch sur le serveur Sentinel>, <*nom de domaine complet du nœud1 elasticsearch*>, <*nom de domaine complet du nœud2 elasticsearch*>, et ainsi de suite]	
thread_pool.bulk.queue_size: 300	
thread_pool.search.queue_size: 10000	Lorsque la taille de la file d'attente des recherches a atteint sa limite, Elasticsearch ignore les requêtes de recherche placées en file d'attente. Vous pouvez augmenter la taille de la file d'attente pour les recherches à l'aide du calcul suivant : threadpool.search.queue_size = nombre moyen de requêtes widget par utilisateur pour un tableau de bord x nombre de partitionnements (par index quotidien) x nombre de jours (durée de la recherche)
index.codec: best_compression	
path.data: ["/<*es1*>", "/<*es2*>"]	Répartissez les données sur plusieurs disques ou emplacements indépendants pour réduire le risque de latence d'E/S de disque. Configurez plusieurs chemins d'accès au stockage des données Elasticsearch. Par exemple /es1, /es2, etc. Pour optimiser les performances et faciliter la gestion, montez chaque chemin sur un disque physique distinct (JBOD).

7. Mettez à jour la taille du segment de mémoire Elasticsearch par défaut dans le fichier `/etc/elasticsearch/jvm.options`.

   La taille du segment de mémoire doit correspondre à 50 % de la mémoire du serveur. Par exemple, sur un noeud Elasticsearch de 24 Go, affectez 12 Go à la taille du segment de mémoire pour optimiser les performances.
8. Répétez toutes les étapes ci-dessus sur chaque noeud de la grappe Elasticsearch.

9 Dans le nœud Elasticsearch du serveur Sentinel, configurez `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` comme suit :

9a Assurez-vous que les valeurs de `cluster.name` et de `discovery.zen.ping.unicast.hosts` dans le fichier `elasticsearch.yml` sont identiques au fichier `elasticsearch.yml` dans le nœud Elasticsearch externe.

9b Indiquez l'adresse IP de localhost suivie de l'adresse IP du nœud Elasticsearch local dans la propriété `network.host` comme suit :

```
network.host : ["127.0.0.1","<adresse IP du nœud Elasticsearch dans Sentinel>"]
```

10 (Conditionnel) Pour Sentinel avec un stockage traditionnel, ajoutez les adresses IP de nœuds Elasticsearch externes à la propriété `ServerList` dans le fichier `/etc/opt/novell/sentinel/config/elasticsearch-index.properties`.

Par exemple : `ServerList=<Elasticsearch IP1>:<Port>,<Elasticsearch IP2>:<Port>`

11 Redémarrez Sentinel :

```
rcsentinel restart
```

12 Redémarrez chaque nœud Elasticsearch :

```
/etc/init.d/elasticsearch start
```

13 Pour optimiser les performances et la stabilité du serveur Sentinel, configurez le nœud Elasticsearch sur le serveur Sentinel en tant que nœud `master-eligible` dédié afin que toutes les données de visualisation des événements soient indexées dans les nœuds Elasticsearch externes :

13a Connectez-vous au serveur Sentinel en tant qu'utilisateur novell.

13b Assurez-vous que toutes les données d'alerte existantes ont été déplacées vers des nœuds Elasticsearch externes.

13c Ouvrez le fichier `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` et ajoutez les informations suivantes :

```
node.master: true
node.data: false
node.ingest: false
search.remote.connect: false
```

13d Redémarrez Elasticsearch :

```
rcsentinel stopSIdb
```

```
rcsentinel startSIdb
```

14 Reportez-vous à la « Sécurisation des données dans Elasticsearch » page 81.

Sécurisation des données dans Elasticsearch

Les nœuds de grappe Elasticsearch sont accessibles à divers clients réseau, notamment les suivants :

- Sentinel : pour récupérer et présenter les données d'événements dans le tableau de bord de visualisation des événements.
- Tâches Spark s'exécutant sur les nœuds NodeManager YARN : pour effectuer l'indexation en masse des événements provenant de Kafka. (pour SSDM)

- Collector Manager : pour effectuer l'indexation en masse d'événements dans Sentinel avec un stockage traditionnel.
- Autres clients externes : pour effectuer des opérations personnalisées telles que les analyses personnalisées.

Sentinel fournit un plug-in de sécurité pour Elasticsearch nommé **elasticsearch-security-plugin** qui authentifie et autorise les accès à Elasticsearch.

Le plug-in utilise un jeton SAML ou une liste blanche pour la validation en fonction de la manière dont les clients se connectent :

- Lorsqu'un client envoie un jeton SAML de pair avec la requête, le plug-in authentifie le jeton par rapport au serveur d'authentification de Sentinel. Une fois l'authentification réussie, le plug-in permet d'accéder uniquement aux événements filtrés pour lesquels le client dispose d'une autorisation.

  Par exemple, le tableau de bord de visualisation des événements (client) affiche uniquement les événements d'Elasticsearch qu'un rôle d'utilisateur est autorisé à afficher.

  Pour plus d'informations sur les rôles et les autorisations, reportez-vous à la section « Creating a Role » (Création d'un rôle) du *Sentinel Administration Guide* (Guide d'administration de Sentinel).
- Lorsqu'un client ne peut pas envoyer de jeton SAML, le plug-in vérifie sa liste blanche de clients autorisés. Si la validation réussit, le plug-in autorise l'accès à tous les événements sans filtrage.
- Lorsqu'un client n'envoie pas de jeton SAML valide ou n'est pas autorisé par la liste blanche, le plug-in le considère comme étant un client illégitime et lui interdit l'accès.

Cette section fournit des informations sur l'installation et la configuration du plug-in de sécurité Elasticsearch :

- « Installation du plug-in de sécurité Elasticsearch » page 82
- « Fournir un accès sécurisé à des clients Elasticsearch supplémentaires » page 83
- « Mise à jour de la configuration du plug-in Elasticsearch » page 85

Installation du plug-in de sécurité Elasticsearch

Vous devez installer le plug-in de sécurité Elasticsearch sur chaque nœud de la grappe Elasticsearch ainsi que sur le nœud Elasticsearch inclus dans Sentinel.

Pour installer le plug-in de sécurité Elasticsearch sur le nœud Elasticsearch inclus dans Sentinel :

1. Connectez-vous au serveur SSDM ou Sentinel principal.
2. Définissez le chemin d'accès pour la variable d'environnement JAVA_HOME comme suit :

   ```
   export JAVA_HOME=/<Sentinel_installation_path>/opt/novell/sentinel/jdk/
   ```

3. Installez le plug-in :

   Pour Linux, connectez-vous sous l'identité de l'utilisateur exécutant Elasticsearch et exécutez la commande suivante :

   ```
   <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/
   elasticsearch-plugin install file://localhost/<Sentinel_installation_path>/
   etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip --
   verbose
   ```

Lorsque vous êtes invité à poursuivre l'installation, entrez `y`.

4. (Conditionnel) Si Elasticsearch n'écoute pas sur le port HTTP par défaut (9200), vous devez mettre à jour le numéro de port Elasticsearch dans chaque entrée du fichier `<chemin_installation_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plug-in/elasticsearch-ip-whitelist.txt`.

   Pour plus d'informations, reportez-vous à la section « Fournir un accès à des clients Elasticsearch à l'aide d'une liste blanche » page 84.

5. Redémarrez les services d'indexation de Sentinel à l'aide de la commande :

```
rcsentinel stopSIdb
rcsentinel startSIdb
```

Pour installer le plug-in de sécurité Elasticsearch sur des nœuds Elasticsearch externes :

Effectuez les opérations suivantes sur chaque nœud de la grappe Elasticsearch :

1. Connectez-vous au serveur SSDM ou Sentinel principal.
2. Copiez le fichier `<chemin_installation_sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip` à un emplacement temporaire sur chaque nœud de la grappe Elasticsearch.
3. Installez le plug-in :

   Pour Linux, connectez-vous sous l'identité de l'utilisateur exécutant Elasticsearch et exécutez la commande suivante :

```
<elasticsearch_install_directory>/bin/elasticsearch-plugin install file://localhost/<full path of elasticsearch-security-plugin*.zip file> --verbose
```

   Lorsque vous êtes invité à poursuivre l'installation, entrez `y`.

4. (Conditionnel) Si Elasticsearch n'écoute pas sur le port HTTP par défaut (9200), vous devez mettre à jour le numéro de port Elasticsearch dans chaque entrée du fichier `<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt`.

   Pour plus d'informations, reportez-vous à la section « Fournir un accès à des clients Elasticsearch à l'aide d'une liste blanche » page 84.

5. Redémarrez Elasticsearch.

Fournir un accès sécurisé à des clients Elasticsearch supplémentaires

Par défaut, les clients approuvés, tels que le serveur SSDM (pour le tableau de bord de visualisation des événements) et YARN NodeManager, le serveur Sentinel (pour le tableau de bord de visualisation des événements) et RCM ont accès à Elasticsearch. Si vous souhaitez utiliser des clients Elasticsearch supplémentaires, vous devez fournir un accès sécurisé à ces clients supplémentaires à l'aide d'un jeton SAML ou d'une liste blanche.

Fournir un accès à des clients Elasticsearch REST à l'aide d'un jeton SAML

Si vous utilisez un client REST pour accéder à Elasticsearch, vous pouvez inclure un jeton SAML dans l'en-tête de requête comme suit :

1. Obtenez un jeton SAML à partir du serveur d'authentification Sentinel. Pour plus d'informations, reportez-vous à la documentation de l'API REST disponible dans Sentinel.

   Cliquez sur **Help** (Aide) > **APIs (API) > Tutorial (Didacticiel) > API Security (Sécurité API) > Obtaining a SAML Token (Logon) (Obtenir un jeton SAML (ouverture de session))**.

2. Utilisez le jeton SAML dans les requêtes REST suivantes : incluez le jeton SAML dans l'en-tête d'autorisation de chaque requête effectuée par le client REST. Indiquez le nom d'en-tête `Authorization` (Autorisation) et la valeur d'en-tête en tant que *<jeton SAML>* obtenue à l'étape 1.

Fournir un accès à des clients Elasticsearch à l'aide d'une liste blanche

Par défaut, Sentinel remplit automatiquement une liste blanche avec les adresses IP des clients Elasticsearch approuvés, tels que le serveur SSDM (pour le tableau de bord de visualisation des événements) et YARN NodeManager, le serveur Sentinel (pour le tableau de bord de visualisation des événements) et RCM. Le plug-in de sécurité Elasticsearch accorde l'accès à Elasticsearch à tous les clients répertoriés dans sa liste blanche.

Pour accorder un accès à des clients supplémentaires qui n'envoient pas de jeton Sentinel valide, vous devez ajouter l'adresse IP du client et le numéro de port HTTP du serveur Elasticsearch à la liste blanche au format `adresse IP:port`. Vous devez vous assurer que les clients externes que vous ajoutez à la liste blanche sont légitimes et dignes de confiance pour empêcher tout accès non autorisé.

Pour mettre à jour la liste blanche, procédez comme suit :

1. Connectez-vous au serveur Sentinel ou au nœud Elasticsearch sous l'identité de l'utilisateur exécutant Elasticsearch.
2. Ajoutez l'entrée <Elasticsearch_Client_IP>:<Target_Elasticsearch_HTTP_Port> dans le fichier :
   - `<chemin_installation_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin//elasticsearch-ip-whitelist.txt` pour le noeud Elasticsearch inclus dans Sentinel.
   - `<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt` pour les nœuds Elasticsearch externes.

   S'il existe plusieurs entrées, ajoutez chaque entrée sur une nouvelle ligne et enregistrez le fichier.
3. Répétez les étapes ci-dessus pour chaque nœud de la grappe Elasticsearch.

Mise à jour de la configuration du plug-in Elasticsearch

Si vous modifiez l'adresse IP/le nom d'hôte et le numéro de port des composants de stockage évolutifs ou le numéro de port et de version Elasticsearch, vous devez mettre à jour les fichiers de configuration du plug-in Elasticsearch en conséquence.

Effectuez les étapes suivantes sur chaque nœud de la grappe Elasticsearch :

1. Connectez-vous au nœud Elasticsearch sous l'identité de l'utilisateur qui exécute Elasticsearch.
2. (Conditionnel) Si vous avez modifié les adresses IP de YARN NodeManager, l'adresse IP de SSDM ou du serveur Sentinel, les adresses IP de RCM ou le numéro de port Elasticsearch, mettez à jour la liste blanche en conséquence afin de vous assurer que le plug-in de sécurité Elasticsearch accorde l'accès aux clients Elasticsearch.

   Si vous configurez SSDM ou Sentinel en mode haute disponibilité, ajoutez des entrées pour l'adresse IP physique de chaque nœud actif et nœud passif de la grappe haute disponibilité.

   Si vous modifiez l'adresse IP physique d'un nœud de la grappe haute disponibilité ou ajoutez un nouveau nœud à la grappe haute disponibilité, mettez à jour la liste blanche avec les adresses IP physiques des nœuds qui ont été modifiés ou qui viennent d'être ajoutés.

   Pour plus d'informations, reportez-vous à la section « Fournir un accès à des clients Elasticsearch à l'aide d'une liste blanche » page 84.
3. (Conditionnel) Si vous avez modifié l'adresse IP de SSDM, l'adresse IP du serveur ou le numéro de port du serveur Web, mettez à jour les propriétés `authServer.host` et `authServer.port` dans les fichiers suivants et redémarrez Elasticsearch :
   - `<chemin_installation_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-configuration.properties` pour le noeud Elasticsearch inclus dans Sentinel.
   - `<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-configuration.properties` pour les nœuds Elasticsearch externes.

   Si vous configurez SSDM ou Sentinel en mode haute disponibilité, définissez la propriété `authServer.host` sur l'adresse IP virtuelle de la grappe haute disponibilité.

   Si vous modifiez l'adresse IP virtuelle de la grappe haute disponibilité, mettez à jour la propriété `authServer.host` par rapport à l'adresse IP virtuelle modifiée.
4. (Conditionnel) Si vous avez mis à niveau Elasticsearch vers une version plus récente, mettez à jour la propriété `elasticsearch.version` dans les fichiers suivants et relancez Elasticsearch :
   - `/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` pour le nœud Elasticsearch inclus dans Sentinel.
   - `<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` pour les nœuds Elasticsearch externes.

Réglage des performances pour Elasticsearch

Sentinel configure automatiquement les paramètres Elasticsearch décrits dans le tableau ci-dessous. Vous pouvez personnaliser les paramètres Elasticsearch selon vos besoins.

Pour personnaliser les paramètres par défaut :

Pour le stockage traditionnel : Ouvrez le fichier `/etc/opt/novell/sentinel/config/elasticsearch-index.properties` et mettez jour les propriétés figurant dans le tableau, le cas échéant.

Pour un stockage évolutif : Dans la page d'accueil SSDM, cliquez sur **Storage** (Stockage) > **Scalable Storage** (Stockage évolutif) > **Advanced Properties** (Propriétés avancées) > **Elasticsearch**.

Tableau 12-1 *Propriétés Elasticsearch*

Propriété	Valeur par défaut	Remarques
elasticsearch.Events.lucenefilter (facultatif)		Spécifiez un filtre pour envoyer uniquement des événements spécifiques à Elasticsearch pour indexation. Par exemple : si vous spécifiez la valeur sev:[3-5], uniquement les événements avec une valeur de gravité comprise entre 3 et 5 sont envoyés à Elasticsearch.
index.fields	id,dt,rv171,msg,ei,evt,xdastaxname,xdasoutcomename,sev,vul,rv32,rv39,rv159,dhn,dip,rv98,dp,fn,rv199,dun,tufname,rv84,rv158,shn,sip,rv76,sun,iufname,sp,iudep,rv198,rv62,st,tid,srcgeo,destgeo,obsgeo,rv145,estz,estzmonth,estzdiy,estzdim,estzdiw,estzhour,estzmin,rv24,tudep,pn,xdasclass,xdasid,xdasreg,xdasprov,iuident,tuident	Indique les champs d'événement que vous voulez qu'Elasticsearch indexe.
es.num.shards	5	Indique le nombre de fragments primaires par index. Vous pouvez augmenter cette valeur par défaut lorsque la taille de fragment dépasse 50 Go.
es.num.replicas	1	Indique le nombre de fragments de réplique que chaque fragment primaire doit comporter. Un minimum de grappe à 2 nœuds est recommandé en prenant en compte la reprise après échec et la haute disponibilité.

Redéploiement du plug-in de sécurité Elasticsearch

Vous devez effectuer un redéploiement : autrement dit, désinstallez et réinstallez le plug-in de sécurité Elasticsearch dans le nœud Elasticsearch inclus dans Sentinel et les nœuds Elasticsearch externes dans les scénarios suivants :

- Ajout ou modification des adresses IP de Collector Manager à distance.
- Désinstallation des instances Collector Manager distantes.
- Activation de la post-installation du stockage évolutif.

Pour redéployer le plug-in de sécurité Elasticsearch :

1. Connectez-vous au serveur Sentinel ou au nœud Elasticsearch sous l'identité de l'utilisateur exécutant Elasticsearch.
2. Désinstallez le plug-in à l'aide de la commande suivante :
   - Pour l'instance d'Elasticsearch incluse dans Sentinel :
     ```
     <chemin_installation_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin remove file://localhost/<chemin_installation_sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
     ```
   - Pour l'instance externe d'Elasticsearch : `<répertoire_installation_elasticsearch> remove file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
3. Réinstallez le plug-in :
   - Pour l'instance d'Elasticsearch incluse dans Sentinel :
     ```
     <chemin_installation_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin install file://localhost/<chemin_installation_sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
     ```
   - Pour l'instance externe d'Elasticsearch : `<répertoire_installation_elasticsearch>/bin/elasticsearch-plugin install file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
4. Redémarrez Elasticsearch à l'aide de la commande suivante :
   - Pour le nœud Elasticsearch inclus dans Sentinel :
     ```
     rcsentinel stopSIdb
     rcsentinel startSIdb
     ```
   - Pour les nœuds Elasticsearch externes :
     ```
     sudo systemctl restart elasticsearch.service
     ```

13 Installation et configuration du stockage évolutif

Veillez à respecter les conditions préalables reprises dans le tableau ci-dessous pour configurer le stockage évolutif comme solution de stockage des données pour Sentinel :

Tableau 13-1 *Conditions préalables pour activer le stockage évolutif*

❒	Tâches	Voir
❒	Déterminez le nombre de grappes de distribution Hadoop et de nœuds de grappe Elasticsearch que vous devez configurer en fonction du taux d'EPS et du nombre de répliques nécessaires. Déterminez la version certifiée de CDH et d'Elasticsearch.	Informations techniques concernant Sentinel.
❒	CDH, Elasticsearch et Sentinel ont leur propre matrice de prise en charge de plates-formes. Passez en revue la matrice de prise en charge de plates-formes de chacun de ces produits et déterminez la plate-forme que vous souhaitez utiliser. Pour Elasticsearch, l'installation du fichier RPM est recommandée, car il contient le script d'initialisation. Elasticsearch sera installé en tant que service et pourra être arrêté et démarré automatiquement lors des redémarrages et mises à niveau sans pour autant écraser les fichiers de configuration. L'installation RPM d'Elasticsearch n'est pas prise en charge sous SLES 11. Par conséquent, déterminez une plate-forme appropriée pour Elasticsearch.	Matrice de prise en charge de CDH dans la documentation Cloudera. Matrice de prise en charge d'Elasticsearch dans la documentation Elasticsearch. Matrice de prise en charge de Sentinel.
❒	Installez et configurez CDH en mode grappe.	« Installation et configuration de CDH » page 90.
❒	Installez et configurez Elasticsearch en mode grappe.	« Installation et configuration d'Elasticsearch » page 79.
❒	Activez le stockage évolutif dans Sentinel.	« Activation du stockage évolutif » page 92

Installation et configuration de CDH

Cette section fournit des informations sur les paramètres spécifiques requis pour Sentinel lors de l'installation et de la configuration de CDH. Pour obtenir des informations détaillées sur l'installation et la configuration de CDH, reportez-vous à la version certifiée détaillée dans la documentation de Cloudera.

Sentinel fonctionne avec Cloudera Express, la version gratuite de CDH. Sentinel fonctionne également avec Cloudera Enterprise, qui nécessite l'achat d'une licence auprès de Cloudera et inclut de nombreuses fonctionnalités non disponibles dans l'édition Cloudera Express. Si vous choisissez de commencer par Cloudera Express et découvrez ensuite que vous avez besoin des fonctionnalités proposées dans Cloudera Enterprise, vous pouvez mettre à niveau la grappe après l'achat de la licence auprès de Cloudera.

Conditions préalables

Avant d'installer CDH, vous devez configurer les hôtes en respectant les conditions préalables suivantes :

- Veillez à respecter les conditions préalables mentionnées dans la documentation de Cloudera.
- Pour de meilleures performances, utilisez le système de fichiers ext4 ou XFS.
- CDH nécessite quelques paquets de système d'exploitation qui ne sont pas installés par défaut. Par conséquent, vous devez monter le DVD du système d'exploitation correspondant. Les instructions d'installation Cloudera vous guident pour déterminer les paquets à installer.
- Pour les systèmes d'exploitation SLES, CDH requiert le paquet `python-psycopg2`. Installez le paquet `python-psycopg2`. Pour plus d'informations, consultez la documentation d'openSUSE.
- Si vous utilisez des machines virtuelles, réservez l'espace disque requis sur le système de fichiers lorsque vous créez des nœuds de machine virtuelle. Par exemple, sous VMware, vous pouvez utiliser le provisioning lourd.
- Assurez-vous que les nœuds de grappe Sentinel et CDH se trouvent dans le même fuseau horaire.
- Définissez le paramètre swappiness de tous les hôtes sur 1 dans le fichier `/etc/sysctl.conf` en ajoutant l'entrée suivante :

  ```
  vm.swappiness=1
  ```

  Pour appliquer ce paramètre immédiatement, exécutez la commande suivante :

  ```
  sysctl -p
  ```

- La version du JDK dans CDH doit au minimum être identique à celle utilisée dans Sentinel. Si la version du JDK disponible dans CDH est antérieure à celle de Sentinel, vous devez suivre les instructions pour installer le JDK manuellement au lieu d'installer le JDK disponible dans l'espace de stockage CDH.

  Installez JDK à l'aide du fichier binaire d'archivage (`.tar.gz`) car l'installation du RPM JDK est problématique lors de l'utilisation du script `manage_spark_jobs.sh` pour soumettre des jobs Spark sous YARN.

  Pour déterminer la version du JDK utilisée dans Sentinel, consultez les Notes de version de Sentinel.

Installation et configuration de CDH

Installez la version certifiée de CDH. Pour plus d'informations sur la version certifiée de CDH, reportez-vous à la page Technical Information for Sentinel (Informations techniques pour Sentinel). Reportez-vous à la version certifiée dans la documentation de Cloudera pour obtenir des instructions d'installation.

Pendant l'installation de CDH, procédez comme suit :

- (Conditionnel) Si l'installation échoue pendant l'installation de la base de données PostgreSQL intégrée, procédez comme suit :

  ```
  mkdir -p /var/run/postgresql
  ```

  ```
  sudo chown cloudera-scm:cloudera-scm /var/run/postgresql
  ```

- Lorsque vous choisissez le type d'installation logiciel dans la fenêtre **Select Repository** (Sélectionner un espace de stockage), veillez à ce que l'option **Use Parcels** (Utiliser les paquets) soit sélectionnée et choisissez Kafka dans **Additional Parcels** (Paquets supplémentaires).
- Lorsque vous ajoutez des services, veillez à activer les services suivants :
  - Cloudera Manager
  - ZooKeeper
  - HDFS
  - HBase
  - YARN
  - Spark
  - Kafka

  REMARQUE : Le serveur d'historique Spark et HDFS NameNode doivent être installés sur le même nœud pour assurer la fiabilité du système. Pour plus d'informations sur l'architecture de stockage évolutif, consultez « Planification du stockage évolutif » page 46.

  Lorsque vous activez les services ci-dessus, configurez la haute disponibilité pour les composants suivants :
  - HBase HMaster
  - HDFS NameNode
  - YARN ResourceManager
- (Conditionnel) Si le programme d'installation ne déploie pas la configuration du client en raison d'un chemin Java manquant, ouvrez une nouvelle session du navigateur et mettez à jour manuellement le chemin d'accès à Java comme suit :

  Cliquez sur **Hosts** (Hôtes) > **All Hosts** (Tous les hôtes) > **Configuration** et spécifiez le chemin d'accès correct dans le champ **Java Home Directory** (Répertoire privé Java).

Activation du stockage évolutif

Vous pouvez activer le stockage évolutif durant ou après l'installation de Sentinel. Lorsque vous activez le stockage évolutif pendant l'installation, Sentinel configure les composants CDH avec les valeurs par défaut. Certaines de ces configurations sont permanentes et ne peuvent pas être modifiées. Par exemple, le nombre de partitions par défaut pour les rubriques Kafka est de 9 et cette valeur ne peut pas être modifiée.

Si vous souhaitez modifier les valeurs par défaut, vous devez activer le stockage évolutif après avoir installé Sentinel, puis configurer les composants CDH selon vos besoins.

Pour les installations traditionnelles, vous pouvez activer le stockage évolutif pendant ou après l'installation de Sentinel. Pour les installations d'applicatifs, vous ne pouvez activer le stockage évolutif qu'après l'installation.

Pour les installations de mise à niveau, le stockage évolutif ne peut être activé qu'après la mise à niveau de Sentinel.

Avant d'activer le stockage évolutif, ayez à portée de main la liste des adresses IP ou des noms d'hôte et numéros de ports des noeuds Kafka, HDFS NameNode, YARN NodeManager, Zookeeper et Elasticsearch. En effet, ces informations sont nécessaires lorsque vous activez un stockage évolutif.

Pour activer le stockage évolutif lors de l'installation de Sentinel, reportez-vous à la « Installation personnalisée du serveur Sentinel » page 94.

Pour activer le stockage évolutif après l'installation ou la mise à niveau, reportez-vous à la section « Enabling Scalable Storage Post-Installation » (Activation du stockage évolutif après l'installation) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

14 Installation traditionnelle

Ce chapitre fournit des informations sur les différentes méthodes d'installation de Sentinel.

Installation interactive

Cette section fournit des informations sur les installations standard et personnalisée.

Installation standard du serveur Sentinel

Procédez comme suit pour effectuer une installation standard :

1. Téléchargez le fichier d'installation de Sentinel sur le site Web des téléchargements :
2. Indiquez sur la ligne de commande la commande suivante pour extraire le fichier d'installation.

   ```
   tar zxvf <install_filename>
   ```

   Remplacez *<nom_fichier_installation>* par le nom réel du fichier d'installation.
3. Accédez au répertoire dans lequel vous avez extrait le programme d'installation :

   ```
   cd <directory_name>
   ```
4. Indiquez la commande suivante pour installer Sentinel :

   ```
   ./install-sentinel
   ```

   ou

   Si vous souhaitez installer Sentinel sur plusieurs systèmes, vous pouvez enregistrer vos options d'installation dans un fichier. Vous pouvez utiliser ce fichier dans le cadre d'une installation sans surveillance de Sentinel sur d'autres systèmes. Pour enregistrer vos options d'installation, entrez la commande suivante :

   ```
   ./install-sentinel -r <response_filename>
   ```
5. Indiquez le numéro de la langue que vous souhaitez utiliser pour l'installation, puis appuyez sur la touche Entrée.

   L'accord de licence utilisateur final s'affiche dans la langue sélectionnée.
6. Appuyez sur la barre d'espacement pour lire l'intégralité de l'accord de licence.
7. Tapez `yes` ou `y` pour accepter la licence et poursuivre l'installation.

Le programme d'installation peut prendre quelques secondes pour charger les paquetages d'installation et afficher un message demandant le type de configuration.

8. Lorsque le système vous y invite, tapez `1` pour sélectionner la configuration standard.

   L'installation utilise la clé de licence d'évaluation par défaut incluse avec le programme d'installation. À tout moment, que ce soit pendant ou après la période d'évaluation, vous pouvez remplacer la clé de la licence d'évaluation par celle que vous avez achetée.

9. Spécifiez le mot de passe de l'administrateur `admin`.
10. Confirmez le mot de passe.

    Ce mot de passe est utilisé par les utilisateurs `admin`, `dbauser` et `appuser`.

    L'installation de Sentinel se termine et le serveur démarre. Après l'installation, le démarrage de tous les services peut prendre quelques minutes, car le système effectue une initialisation unique. Patientez jusqu'à la fin de l'installation avant de vous connecter au serveur.

Pour accéder à l'interface principale de Sentinel, indiquez l'adresse URL suivante dans votre navigateur Web :

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

où *IP_AddressOrDNS_Sentinel_server* est l'adresse IP ou le nom DNS du serveur Sentinel et *8443* le port par défaut du serveur Sentinel.

Installation personnalisée du serveur Sentinel

Si vous souhaitez installer Sentinel en utilisant une configuration personnalisée, vous pouvez personnaliser votre installation Sentinel en indiquant votre clé de licence, en définissant un mot de passe différent, en spécifiant d'autres ports, etc.

1. Si vous souhaitez activer le stockage évolutif, veillez à respecter les conditions préalables mentionnées au Chapitre 13, « Installation et configuration du stockage évolutif », page 89.
2. Téléchargez le fichier d'installation de Sentinel sur le site Web des téléchargements :
3. Indiquez sur la ligne de commande la commande suivante pour extraire le fichier d'installation.

   `tar zxvf <install_filename>`

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

4. Indiquez la commande suivante à la racine du répertoire extrait pour l'installation de Sentinel :

   `./install-sentinel`

   ou

   Si vous souhaitez utiliser cette configuration personnalisée pour installer Sentinel sur plusieurs systèmes, vous pouvez enregistrer vos options d'installation dans un fichier. Vous pouvez utiliser ce fichier dans le cadre d'une installation sans surveillance de Sentinel sur d'autres systèmes. Pour enregistrer vos options d'installation, entrez la commande suivante :

   `./install-sentinel -r <response_filename>`

5. Indiquez le numéro de la langue que vous souhaitez utiliser pour l'installation, puis appuyez sur la touche Entrée.

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

6. Appuyez sur la barre d'espacement pour lire l'intégralité de l'accord de licence.
7. Tapez `yes` ou `y` pour accepter l'accord de licence et poursuivre l'installation.

Le programme d'installation peut prendre quelques secondes pour charger les paquetages d'installation et afficher un message demandant le type de configuration.

8 Indiquez `2` pour effectuer une configuration personnalisée de Sentinel.

9 Indiquez `1` pour utiliser la clé de licence d'évaluation par défaut.

ou

Saisissez `2` afin d'entrer la clé de licence achetée pour Sentinel.

10 Indiquez le mot de passe de l'utilisateur administrateur `admin` et confirmez-le en le ressaisissant.

11 Indiquez le mot de passe de l'utilisateur de base de données `dbauser` et confirmez-le en le ressaisissant.

Le compte `dbauser` correspond à l'identité utilisée par Sentinel pour interagir avec la base de données. Le mot de passe que vous saisissez ici peut être utilisé pour les tâches de maintenance de base de données, y compris la réinitialisation du mot de passe admin en cas de perte ou d'oubli.

12 Indiquez le mot de passe de l'utilisateur d'application `appuser` et confirmez-le en le ressaisissant.

13 Changez les assignations de port pour les services Sentinel en saisissant le numéro souhaité, puis en indiquant le numéro du nouveau port.

14 Après avoir modifié les ports, tapez `7` lorsque vous avez terminé.

15 Saisissez `1` pour authentifier les utilisateurs qui utilisent uniquement la base de données interne.

ou

Si vous avez configuré un annuaire LDAP dans votre domaine, saisissez `2` pour authentifier les utilisateurs à l'aide de l'authentification d'annuaires LDAP.

La valeur par défaut est de `1`.

16 ***Pour que Sentinel utilise le mode FIPS 140-2***, entrez `y`.

16a Spécifiez un mot de passe fort pour la base de données keystore, puis confirmez-le.

REMARQUE : le mot de passe doit contenir au minimum sept caractères. Le mot de passe doit contenir au moins trois des classes de caractères suivantes : chiffres, minuscules ASCII, majuscules ASCII, caractères non alphanumériques ASCII et caractères non-ASCII.

Si la première lettre est une majuscule ASCII ou que le dernier caractère est un chiffre, ils ne sont pas comptés.

16b Si vous souhaitez insérer des certificats externes dans la base de données keystore pour établir une relation de confiance, appuyez sur `y`, puis spécifiez le chemin du fichier de certificat. Dans le cas contraire, appuyez sur `n`.

16c Terminez la configuration du mode FIPS 140-2 en effectuant les tâches mentionnées au Chapitre 24, « Fonctionnement de Sentinel en mode FIPS 140-2 », page 135.

17 ***Si vous souhaitez activer le stockage évolutif***, entrez `yes` ou `y`.

IMPORTANT : une fois le stockage évolutif activé, vous ne pouvez pas restaurer la configuration, à moins de réinstaller Sentinel.

17a Indiquez les adresses IP ou les noms d'hôte et numéros de port des composants du stockage évolutif.

17b (Conditionnel) Si vous souhaitez quitter la configuration du stockage évolutif et procéder à l'installation de Sentinel, entrez `no` ou `n`.

17c Une fois que l'installation de Sentinel est terminée, effectuez la configuration du stockage évolutif mentionnée à la section « Configuration post-installation pour le stockage évolutif » page 96.

L'installation de Sentinel se termine et le serveur démarre. Après l'installation, le démarrage de tous les services peut prendre quelques minutes, car le système effectue une initialisation unique. Patientez jusqu'à la fin de l'installation avant de vous connecter au serveur.

Pour accéder à l'interface principale de Sentinel, indiquez l'adresse URL suivante dans votre navigateur Web :

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

où <*IP_AddressOrDNS_Sentinel_server*> est l'adresse IP ou le nom DNS du serveur Sentinel et *8443* le port par défaut du serveur Sentinel.

Configuration post-installation pour le stockage évolutif

1. Connectez-vous au serveur SSDM.
2. Effacez le cache de votre navigateur pour afficher la version de Sentinel que vous avez installée.
3. Pour afficher les événements et les alertes, ajoutez le nœud Elasticsearch inclus dans SSDM à la grappe Elasticsearch que vous avez configurée pour un stockage évolutif :

   Dans le nœud Elasticsearch local, ouvrez `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` et ajoutez les informations suivantes :

   - cluster.name: <*nom_grappe_Elasticsearch*>
   - node.name: <*nom_noeud*>
   - discovery.zen.ping.unicast.hosts: ["<*FQDN noeud1 Elasticsearch*>", "<*FQDN noeud2 Elasticsearch*>", etc."]

   Dans tous les noeuds Elasticsearch externes, ouvrez `/etc/elasticsearch/elasticsearch.yml` et effectuez la mise à jour

   discovery.zen.ping.unicast.hosts: ["<*FQDN noeud1 Elasticsearch*>", "<*FQDN noeud2 Elasticsearch*>", etc."]

   REMARQUE : Assurez-vous que les valeurs des paramètres dans le fichier local `elasticsearch.yml` et le fichier `elasticsearch.yml` dans les nœuds Elasticsearch externes sont identiques, à l'exception de `network.host` et `node.name` étant donné que ces valeurs sont spécifiques au nœud.

4. Redémarrez les services d'indexation en utilisant la commande :

   ```
   rcsentinel stopSIdb
   rcsentinel startSIdb
   ```

5. Terminez la configuration de stockage évolutif comme indiqué dans les sections suivantes :
   - « Sécurisation des données dans Elasticsearch » page 81

- Performance Tuning Guidelines (Conseils d'optimisation des performances)·du *Sentinel Administration Guide* (Guide d'administration de Sentinel)
- Processing Data (Traitement des données) du *Sentinel Administration Guide* (Guide d'administration de Sentinel)

Installation de Collector Manager et de Correlation Engine

Par défaut, Sentinel installe une instance de Collector Manager et de Correlation Engine. Pour les environnements de production, configurez un déploiement distribué, car il isole les composants de collecte de données sur un ordinateur distinct, ce qui permet de gérer les pointes de trafic et les autres anomalies tout en garantissant une stabilité maximale du système. Pour en savoir plus sur les avantages liés à l'installation de composants supplémentaires, reportez-vous à la « Avantages des déploiements distribués » page 49.

IMPORTANT : vous devez installer l'instance supplémentaire de Collector Manager ou de Correlation Engine sur des systèmes distincts. Veillez également à ne pas les installer sur le système où se trouve déjà le serveur Sentinel.

Liste de contrôle pour l'installation : Veillez à avoir effectué les tâches suivantes avant de commencer l'installation.

- Vérifiez que votre matériel et vos logiciels satisfont aux conditions de la configuration minimale requise. Pour plus d'informations, reportez-vous à la Chapitre 5, « Configuration du système », page 39.
- Synchronisez l'heure à l'aide du protocole NTP (Network Time Protocol).
- Collector Manager requiert une connectivité réseau vers le port de bus de messages (61616) sur le serveur Sentinel Avant d'installer Collector Manager, vérifiez que tous les paramètres réseau et du pare-feu sont définis pour pouvoir communiquer sur ce port.

Pour installer Collector Manager et Correlation Engine, procédez comme suit :

1. Lancez l'interface principale de Sentinel en indiquant l'adresse URL suivante dans le navigateur Web :

   `https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

   où <*IP_AddressOrDNS_Sentinel_server*> est l'adresse IP ou le nom DNS du serveur Sentinel et *8443* le port par défaut du serveur Sentinel.

   Connectez-vous avec le nom d'utilisateur et le mot de passe indiqués pendant l'installation du serveur Sentinel.
2. Dans la barre d'outils, cliquez sur **Téléchargements**.
3. Cliquez sur **Télécharger le programme d'installation** sous l'installation requise.
4. Cliquez sur **Enregistrer le fichier** pour enregistrer le programme d'installation à l'emplacement souhaité.
5. Indiquez la commande suivante pour extraire le fichier d'installation.

   `tar zxvf <install_filename>`

   Remplacez <*nom_fichier_installation*> par le nom réel du fichier d'installation.
6. Accédez au répertoire dans lequel vous avez extrait le programme d'installation.
7. Spécifiez la commande suivante pour installer Collector Manager ou Correlation Engine :

   Pour Collector Manager :

```
./install-cm
```

Pour Correlation Engine :

```
./install-ce
```

ou

Si vous souhaitez installer Collector Manager ou Correlation Engine sur plusieurs systèmes, vous pouvez enregistrer vos options d'installation dans un fichier. Vous pouvez utiliser ce fichier dans le cadre d'une installation sans surveillance de sur d'autres systèmes. Pour enregistrer vos options d'installation, entrez la commande suivante :

Pour Collector Manager :

```
./install-cm -r <response_filename>
```

Pour Correlation Engine :

```
./install-ce -r <response_filename>
```

8 Indiquez le numéro de la langue que vous souhaitez utiliser pour l'installation.

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

9 Appuyez sur la barre d'espacement pour lire l'intégralité de l'accord de licence.

10 Tapez `yes` ou `y` pour accepter l'accord de licence et poursuivre l'installation.

Le programme d'installation peut prendre quelques secondes pour charger les paquetages d'installation et afficher un message demandant le type de configuration.

11 Lorsque vous y êtes invité, indiquez l'option appropriée pour procéder à la configuration standard ou personnalisée.

12 Entrez le nom d'hôte par défaut du serveur de communication ou l'adresse IP de la machine sur laquelle Sentinel est installé.

13 (Conditionnel) Si vous avez opté pour une configuration personnalisée, précisez :

13a le numéro de port du canal de communication avec le serveur Sentinel ;

13b le numéro de port du serveur Web Sentinel.

14 Lorsque vous êtes invité à accepter le certificat, exécutez la commande ci-dessous sur le serveur Sentinel pour vérifier le certificat :

En mode FIPS :

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.activemqkeystore.jks
```

En mode non-FIPS :

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/nonfips_backup/.activemqkeystore.jks
```

Comparez le résultat obtenu pour ce certificat avec celui du certificat du serveur Sentinel affiché à l'Étape 12.

REMARQUE : Si le certificat ne correspond pas, l'installation s'arrête. Exécutez le programme d'installation à nouveau et vérifiez les certificats.

---

15 Acceptez le certificat si le résultat obtenu correspond à celui du certificat du serveur Sentinel.

16 Indiquez les informations d'identification de tout utilisateur disposant d'un rôle d'administrateur. Entrez le nom d'utilisateur et le mot de passe.

17 (Conditionnel) Si vous avez opté pour la configuration personnalisée, saisissez `yes` ou `y` pour activer le mode FIPS 140-2 dans Sentinel et procéder à la configuration FIPS.

18 (Conditionnel) Si votre environnement utilise une authentification forte ou à plusieurs facteurs, vous devez fournir l'ID client Sentinel et le secret client Sentinel. Pour plus d'informations sur les méthodes d'authentification, reportez-vous à la section « Authentication Methods » (Méthodes d'authentification) du *Sentinel Administrator Guide* (Guide de l'administrateur Sentinel).

Pour récupérer l'ID client Sentinel et le secret client Sentinel, accédez à l'URL suivante :

`https://Nomhote:port/SentinelAuthServices/oauth/clients`

Où :

- *Nomhote* est le nom d'hôte du serveur Sentinel.
- *Port* est le port qu'utilise Sentinel (généralement 8443).

L'URL indiquée se base sur votre session Sentinel actuelle pour récupérer l'ID client Sentinel et le secret client Sentinel.

19 (Conditionnel) Si vous avez activé la visualisation des événements, vous devez ajouter Collector Manager à la liste blanche Elasticsearch. Pour plus d'informations, reportez-vous à la section « Fournir un accès à des clients Elasticsearch à l'aide d'une liste blanche » page 84.

20 Procédez à l'installation comme indiqué jusqu'à la fin de la procédure d'installation.

Installation silencieuse

L'installation silencieuse ou sans surveillance est utile si vous devez installer plusieurs serveurs Sentinel, ou plusieurs instances de Collector Manager ou Correlation Engine dans votre déploiement. Dans ce type de scénario, vous pouvez enregistrer les paramètres d'installation au cours de l'installation interactive, puis exécuter le fichier enregistré sur d'autres serveurs.

Pour effectuer une installation en mode silencieux, vérifiez que vous avez enregistré les paramètres d'installation dans un fichier. Pour obtenir des informations sur la création du fichier de réponses, reportez-vous à la « Installation standard du serveur Sentinel » page 93 ou « Installation personnalisée du serveur Sentinel » page 94 et à la « Installation de Collector Manager et de Correlation Engine » page 97.

Pour activer le mode FIPS 140-2, veillez à ce que le fichier de réponses inclue les paramètres suivants :

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

Pour effectuer une installation silencieuse, procédez comme suit :

1 Téléchargez les fichiers d'installation sur le site Web de téléchargement .

2 Connectez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez installer Sentinel, Collector Manager ou Correlation Engine.

3 Entrez la commande suivante pour extraire les fichiers d'installation du fichier TAR :

```
tar -zxvf <install_filename>
```

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

4 Indiquez la commande suivante pour effectuer l'installation en mode silencieux :

Pour le serveur Sentinel :

```
./install-sentinel -u <response_file>
```

Pour Collector Manager :

```
./install-cm -u <response_file>
```

Pour Correlation Engine :

```
./install-ce -u <response_file>
```

L'installation se poursuit et utilise les valeurs stockées dans le fichier de réponses.

Si vous avez installé un serveur Sentinel, le démarrage de tous les services après l'installation peut prendre quelques minutes, car le système effectue une initialisation unique. Patientez jusqu'à la fin de l'installation avant de vous connecter au serveur.

5 **(Conditionnel) Si vous avez choisi d'activer le mode FIPS 140-2 pour le serveur Sentinel,**

configurez-le en suivant la procédure mentionnée au Chapitre 24, « Fonctionnement de Sentinel en mode FIPS 140-2 », page 135.

Installation de Sentinel en tant qu'utilisateur non-root

Si la stratégie de votre organisation ne vous permet pas d'exécuter l'installation complète de Sentinel en tant qu'utilisateur `root`, vous pouvez installer Sentinel en tant qu'utilisateur `non-root`, c'est-à-dire en tant qu'utilisateur `novell`. Au cours de cette installation, les premières étapes sont effectuées en tant qu'utilisateur `root`. Vous procédez ensuite à l'installation de Sentinel en tant qu'utilisateur `novell` créé par l'utilisateur `root`. Enfin, l'utilisateur `root` termine l'installation.

Si vous installez Sentinel en tant qu'utilisateur `non-root`, vous devez procéder en tant qu'utilisateur « novell ». Les installations non-root autres que celles de l'utilisateur novell ne sont pas prises en charge bien que l'installation se déroule correctement.

REMARQUE : Lorsque vous installez Sentinel dans un répertoire existant, autre que celui par défaut, assurez-vous que l'utilisateur « novell » dispose des autorisations de propriété sur ce répertoire. Exécutez la commande suivante pour lui assigner ces autorisations :

```
chown novell:novell <non-default installation directory>
```

---

1 Téléchargez les fichiers d'installation sur le site Web de téléchargement .

2 Entrez la commande suivante dans la ligne de commande pour extraire les fichiers d'installation du fichier tar :

```
tar -zxvf <install_filename>
```

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

3 Connectez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez installer Sentinel en tant que `root`.

4 Entrez la commande suivante :

```
./bin/root_install_prepare
```

Une liste des commandes à exécuter avec des privilèges root s'affiche. Si vous souhaitez que l'utilisateur non-root installe Sentinel à un emplacement différent de l'emplacement par défaut, indiquez l'option --location avec la commande. Par exemple :

```
./bin/root_install_prepare --location=/foo
```

La valeur que vous transmettez à l'option `--location foo` est ajoutée au début des chemins d'accès aux répertoires.

Cette opération crée également un groupe `novell` ainsi qu'un utilisateur `novell` s'ils n'existent pas encore.

5 Acceptez la liste de commandes.

Les commandes affichées sont exécutées.

6 Entrez la commande suivante pour adopter l'identité de l'utilisateur non-root que vous venez de créer, à savoir `novell` :

```
su novell
```

7 (Conditionnel) Pour effectuer une installation interactive :

7a Indiquez la commande appropriée en fonction du composant en cours d'installation :

Composant	Commande
un serveur Sentinel ;	**Emplacement par défaut :** `./install-sentinel`
	Emplacement personnalisé : `./install-sentinel --location=/foo`
Collector Manager	**Emplacement par défaut :** `./install-cm`
	Emplacement personnalisé : `./install-cm --location=/foo`
Correlation Engine	**Emplacement par défaut :** `./install-ce`
	Emplacement personnalisé : `./install-cm --location=/foo`

7b Passez à l'Étape 9.

8 (Conditionnel) Pour effectuer une installation en mode silencieux, vérifiez que vous avez enregistré les paramètres d'installation dans un fichier. Pour obtenir des informations sur la création du fichier de réponses, reportez-vous à la « Installation standard du serveur Sentinel » page 93 ou à la « Installation personnalisée du serveur Sentinel » page 94.

Pour effectuer une installation en mode silencieux :

8a Indiquez la commande appropriée en fonction du composant en cours d'installation :

Composant	Commande
un serveur Sentinel ;	**Emplacement par défaut :** `./install-sentinel -u <fichier_réponse>`
	Emplacement personnalisé : `./install-sentinel --location=/foo -u <fichier_réponse>`
Collector Manager	**Emplacement par défaut :** `./install-cm -u <fichier_réponse>`
	Emplacement personnalisé : `./install-cm --location=/foo -u <fichier_réponse>`
Correlation Engine	**Emplacement par défaut :** `./install-ce -u <fichier_réponse>`
	Emplacement personnalisé : `./install-ce --location=/foo -u <fichier_réponse>`

L'installation se poursuit et utilise les valeurs stockées dans le fichier de réponses.

8b Passez au Étape 12.

9 Indiquez le numéro de la langue que vous souhaitez utiliser pour l'installation.

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

10 Lisez l'accord de licence utilisateur final et tapez `yes` ou `y` pour l'accepter et poursuivre l'installation.

   Le processus démarre en installant tous les paquetages RPM. Cette installation peut prendre quelques secondes.

11 Vous êtes invité à spécifier le mode d'installation.

   - Si vous choisissez de passer à une configuration standard, suivez les étapes Étape 8 à Étape 10 dans la « Installation standard du serveur Sentinel » page 93.
   - Si vous choisissez de passer à une configuration personnalisée, suivez les étapes Étape 8 à Étape 15 dans la « Installation personnalisée du serveur Sentinel » page 94.

12 Connectez-vous en tant qu'utilisateur `root` et indiquez la commande suivante pour terminer l'installation :

   ```
   ./bin/root_install_finish
   ```

   L'installation de Sentinel se termine et le serveur démarre. Après l'installation, le démarrage de tous les services peut prendre quelques minutes, car le système effectue une initialisation unique. Patientez jusqu'à la fin de l'installation avant de vous connecter au serveur.

Pour accéder à l'interface principale de Sentinel, indiquez l'adresse URL suivante dans votre navigateur Web :

`https://`*`IP_AddressOrDNS_Sentinel_server`*`:`*`8443`*`/sentinel/views/main.html`

où *IP_AddressOrDNS_Sentinel_server* est l'adresse IP ou le nom DNS du serveur Sentinel et *8443* le port par défaut du serveur Sentinel.

15 Installation de l'applicatif

L'applicatif Sentinel est un applicatif logiciel prêt à l'emploi basé sur l'infrastructure d'applicatif commune Micro Focus. Il associe un système d'exploitation SLES 12 SP3 renforcé et le service de mise à jour du logiciel Sentinel. L'expérience utilisateur est simple et transparente, et vous pouvez tirer bénéfice de vos investissements existants. L'applicatif Sentinel inclut une interface utilisateur Web pour configurer et surveiller l'applicatif.

L'image de l'applicatif Sentinel est compressée aux deux formats ISO et OVF, qui peuvent être déployés dans les environnements virtuels. Pour plus d'informations sur les plates-formes de virtualisation prises en charge, consultez le site Web des informations techniques concernant Sentinel.

Conditions préalables

Assurez-vous que l'environnement où vous prévoyez d'installer Sentinel en tant qu'applicatif ISO répond aux conditions préalables suivantes :

- Avant d'installer l'applicatif Sentinel, consultez les nouvelles fonctionnalités et les problèmes connus dans les notes de version du SLES certifié.
- (Conditionnel) Si vous installez l'applicatif ISO Sentinel sur du matériel sans système d'exploitation, téléchargez l'image du disque ISO de l'applicatif à partir du site de support et créez un DVD.
- Vérifiez que le disque dur dispose d'un espace disponible minimal de 50 Go pour que le programme d'installation propose une partition automatique.
- Assurez-vous que votre système dispose d'au moins 4 Go de mémoire pour que l'installation s'exécute correctement. Si la mémoire disponible est inférieure à 4 Go, l'installation échoue. Si la mémoire est supérieure à 4 Go mais inférieure aux 24 Go recommandés, le programme d'installation affiche un message vous indiquant que la mémoire dont vous disposez est inférieure aux recommandations.

Installation de l'applicatif ISO Sentinel

Cette section fournit des informations sur l'installation de Sentinel, des instances Collector Manager et Correlation Engine à l'aide de l'image de l'applicatif ISO. Ce format d'image vous permet de générer un format d'image de disque plein qui peut être déployé directement sur du matériel physique (sans système d'exploitation) ou virtuel (machine virtuelle désinstallée d'un hyperviseur) à l'aide d'une image DVD ISO de démarrage.

Installation de Sentinel

Pour installer l'applicatif ISO Sentinel :

1. Téléchargez l'image de l'applicatif virtuel ISO à partir du site Web de téléchargement .
2. (Conditionnel) Si vous utilisez un hyperviseur :

   Configurez la machine virtuelle à l'aide de l'image de l'applicatif virtuel ISO et mettez-la sous tension.

   ou

   Gravez l'image ISO sur un DVD, configurez la machine virtuelle à l'aide du DVD, puis mettez-la sous tension.
3. (Conditionnel) Si vous installez l'applicatif Sentinel sur du matériel sans système d'exploitation :
   - **3a** Démarrez la machine physique à l'aide du DVD à partir de l'unité DVD.
   - **3b** Suivez les instructions de l'assistant d'installation qui s'affichent à l'écran.
   - **3c** Sélectionnez **Install sentinel server <*version*>** (Installer le serveur Sentinel <version>).
4. Sélectionnez la langue de votre choix.
5. Sélectionnez la disposition du clavier.
6. Cliquez sur **Suivant**.
7. Lisez et acceptez l'accord de licence du logiciel SUSE Enterprise Server. Cliquez sur **Suivant**
8. Lisez et acceptez l'accord de licence de l'applicatif du serveur Sentinel. Cliquez sur **Suivant**
9. Définissez les mots de passe, la configuration NTP et le fuseau horaire de l'applicatif Sentinel.

   Définissez les informations d'identification de l'utilisateur `vaadmin` pour la connexion à la console de gestion de l'applicatif Sentinel.

   REMARQUE : après l'installation, vous pouvez modifier la configuration NTP et le fuseau horaire en procédant comme suit :

   - Accédez à l'invite de commande et entrez `yast->Network Services->NTP Configuration`.
   - Accédez à la console de gestion de l'applicatif Sentinel et cliquez sur **Heure**.

   Si l'heure n'est pas immédiatement synchronisée après l'installation, exécutez la commande suivante pour redémarrer NTP :

   ```
   rcntp restart
   ```

   ---
10. Dans la page des paramètres réseau de l'applicatif du serveur Sentinel, indiquez le nom d'hôte et le nom de domaine. Sélectionnez **Static IP Address** (Adresse IP statique) ou **DHCP IP Address** (Adresse IP DHCP).
11. Cliquez sur **Suivant**.
12. (Conditionnel) Si vous avez sélectionné **Static IP Address** (Adresse IP statique) à l'étape 10, spécifiez les paramètres de connexion réseau.
13. Cliquez sur **Suivant**.
14. Définissez le mot de passe de l'utilisateur Sentinel `admin`, puis cliquez sur **Suivant**.

    L'applicatif est installé.
15. Prenez note de l'adresse IP de l'applicatif qui s'affiche dans la console.
16. Connectez-vous en tant qu'utilisateur `root` à la console pour vous connecter à l'applicatif.

Entrez le nom d'utilisateur `root`, puis spécifiez le mot de passe que vous avez défini à l'Étape 9.

17 Passez à la section « Configuration post-installation de l'applicatif » page 108.

Installation de Collector Manager et Correlation Engine

La procédure d'installation de Collector Manager et de Correlation Engine est similaire à la procédure d'installation de Sentinel, si ce n'est que vous devez télécharger le fichier d'applicatif ISO approprié à partir du site Web de téléchargement.

1 Suivez la procédure des étapes 1 à 13 de la « Installation de Sentinel » page 104.

   L'installation vérifie si la mémoire et l'espace disque disponibles sont suffisants. Si la mémoire disponible est inférieure à 1 Go, le programme d'installation ne vous permet pas de poursuivre et le bouton **Suivant** est grisé.

2 Spécifiez la configuration suivante pour Collector Manager ou Correlation Engine :

   - **Nom d'hôte ou adresse IP du serveur Sentinel :** indiquez le nom d'hôte ou l'adresse IP du serveur Sentinel auquel Collector Manager ou Correlation Engine doit se connecter.
   - **Port du canal de communication Sentinel :** indiquez le numéro de port du canal de communication avec le serveur Sentinel. Le numéro de port par défaut est `61616`.
   - **Port du serveur Web Sentinel :** indiquez le numéro de port du serveur Web Sentinel. Le numéro de port par défaut est 8443.
   - **User name with Administrator role (Nom d'utilisateur ayant un rôle d'administrateur) :** spécifiez le nom d'utilisateur de tout utilisateur disposant d'un rôle d'administrateur.
   - **Password for user with Administrator role (Mot de passe de l'utilisateur ayant un rôle d'administrateur) :** spécifiez le mot de passe de l'utilisateur que vous avez indiqué dans le champ ci-dessus.

3 (Conditionnel) Si votre environnement utilise une authentification forte ou à plusieurs facteurs, vous devez fournir l'ID client Sentinel et le secret client Sentinel. Pour plus d'informations sur les méthodes d'authentification, reportez-vous à la section « Authentication Methods » (Méthodes d'authentification) du *Sentinel Administrator Guide* (Guide de l'administrateur Sentinel).

   Pour récupérer l'ID client Sentinel et le secret client Sentinel, accédez à l'URL suivante :

   `https://Nomhote:port/SentinelAuthServices/oauth/clients`

   Où :

   - *Nomhote* est le nom d'hôte du serveur Sentinel.
   - *Port* est le port qu'utilise Sentinel (généralement 8443).

   L'URL indiquée se base sur votre session Sentinel actuelle pour récupérer l'ID client Sentinel et le secret client Sentinel.

4 Cliquez sur **Suivant**.

5 Acceptez le certificat lorsque vous y êtes invité.

6 Prenez note de l'adresse IP de l'applicatif qui s'affiche dans la console.

   La console affiche un message indiquant que cet applicatif est Sentinel Collector Manager ou Correlation Engine (en fonction du choix que vous avez effectué), ainsi que l'adresse IP de ce dernier. La console affiche également l'adresse IP de l'interface utilisateur du serveur Sentinel.

7 Effectuez les opérations de l'Étape 16 à l'Étape 17 de la « Installation de Sentinel » page 104.

Installation de l'applicatif OVF Sentinel

Cette section fournit des informations sur l'installation de Sentinel, Collector Manager et Correlation Engine en tant qu'image d'applicatif OVF.

Le format OVF est un format standard de machine virtuelle, pris en charge par la plupart des hyperviseurs, directement ou par le biais d'une conversion simple. Sentinel prend en charge l'applicatif OVF avec deux hyperviseurs certifiés, mais vous pouvez également l'utiliser avec d'autres hyperviseurs.

- « Installation de Sentinel » page 106
- « Installation de Collector Manager et Correlation Engine » page 107

Installation de Sentinel

Pour installer l'applicatif OVF Sentinel :

1. Téléchargez l'image de l'applicatif virtuel OVF à partir du site Web de téléchargement .
2. Dans la console de gestion de votre hyperviseur, importez le fichier image OVF en tant que nouvelle machine virtuelle. Autorisez l'hyperviseur à convertir l'image OVF au format natif si vous y êtes invité.
3. Passez en revue les ressources matérielles virtuelles allouées à votre nouvelle machine virtuelle pour vous assurer qu'elles répondent aux exigences de Sentinel.
4. Mettez la machine virtuelle sous tension.
5. Sélectionnez la langue de votre choix.
6. Sélectionnez la disposition du clavier.
7. Cliquez sur **Suivant**.
8. Lisez et acceptez l'accord de licence du logiciel SUSE Enterprise Server. Cliquez sur **Suivant**.
9. Lisez et acceptez l'accord de licence de l'applicatif du serveur Sentinel. Cliquez sur **Suivant**.
10. Définissez les mots de passe, la configuration NTP et le fuseau horaire de l'applicatif Sentinel.

    Définissez les informations d'identification de l'utilisateur `vaadmin` pour la connexion à la console de gestion de l'applicatif Sentinel.

    REMARQUE : après l'installation, vous pouvez modifier la configuration NTP et le fuseau horaire en procédant comme suit :

    - Accédez à l'invite de commande et entrez `yast->Network Services->NTP Configuration`.
    - Accédez à la console de gestion de l'applicatif Sentinel et cliquez sur **Heure**.

    Si l'heure n'est pas immédiatement synchronisée après l'installation, exécutez la commande suivante pour redémarrer NTP :

    ```
    rcntp restart
    ```

    ---

11. Dans la page des paramètres réseau de l'applicatif du serveur Sentinel, indiquez le nom d'hôte et le nom de domaine. Sélectionnez **Static IP Address** (Adresse IP statique) ou **DHCP IP Address** (Adresse IP DHCP).
12. Cliquez sur **Suivant**.
13. (Conditionnel) Si vous avez sélectionné **Static IP Address** (Adresse IP statique) à l'étape 11, spécifiez les paramètres de connexion réseau.

14 Cliquez sur **Suivant**.

15 Définissez le mot de passe admin de Sentinel, puis cliquez sur **Suivant**.

Après l'installation, le démarrage de tous les services peut prendre quelques minutes, car le système effectue une initialisation unique. Patientez jusqu'à la fin de l'installation avant de vous connecter au serveur.

16 Prenez note de l'adresse IP de l'applicatif qui s'affiche dans la console. Utilisez la même adresse IP pour accéder à l'interface principale de Sentinel.

Installation de Collector Manager et Correlation Engine

Pour installer Collector Manager ou Correlation Engine sur un serveur VMware ESX en tant qu'image d'applicatif OVF :

1 Suivez la procédure des étapes 1 à 14 de la « Installation de Sentinel » page 106.

L'installation vérifie si la mémoire et l'espace disque disponibles sont suffisants. Si la mémoire disponible est inférieure à 1 Go, le programme d'installation ne vous permet pas de poursuivre et le bouton **Suivant** est grisé.

2 Indiquez le nom d'hôte/l'adresse IP du serveur Sentinel auquel le Collector Manager doit se connecter.

3 Indiquez le numéro de port du serveur de communication. Le port par défaut est `61616`.

4 Indiquez les informations d'identification de tout utilisateur disposant d'un rôle d'administrateur. Entrez le nom d'utilisateur et le mot de passe.

5 (Conditionnel) Si votre environnement utilise une authentification forte ou à plusieurs facteurs, vous devez fournir l'ID client Sentinel et le secret client Sentinel. Pour plus d'informations sur les méthodes d'authentification, reportez-vous à la section « Authentication Methods » (Méthodes d'authentification) du *Sentinel Administrator Guide* (Guide de l'administrateur Sentinel).

Pour récupérer l'ID client Sentinel et le secret client Sentinel, accédez à l'URL suivante :

`https://Nomhote:port/SentinelAuthServices/oauth/clients`

Où :

- *Nomhote* est le nom d'hôte du serveur Sentinel.
- *Port* est le port qu'utilise Sentinel (généralement 8443).

L'URL indiquée se base sur votre session Sentinel actuelle pour récupérer l'ID client Sentinel et le secret client Sentinel.

6 Cliquez sur **Suivant**.

7 Acceptez le certificat.

8 Cliquez sur **Suivant** pour terminer l'installation.

Une fois l'installation terminée, le programme d'installation affiche un message indiquant que cet applicatif est Sentinel Collector Manager ou Sentinel Correlation Engine (en fonction du choix que vous avez effectué), ainsi que l'adresse IP de ce dernier. Ce message indique également l'adresse IP de l'interface utilisateur du serveur Sentinel.

Configuration post-installation de l'applicatif

Après avoir installé Sentinel, vous devez effectuer une configuration supplémentaire pour permettre à l'applicatif de fonctionner correctement.

Enregistrement pour obtenir les mises à jour

Vous devez enregistrer l'applicatif Sentinel auprès du canal de mise à jour de l'applicatif pour recevoir les dernières mises à jour du système d'exploitation et de Sentinel. Pour enregistrer l'applicatif, vous devez d'abord obtenir un code d'enregistrement ou une clé d'activation auprès du Service clients .

Enregistrement à l'aide de la console de gestion de l'applicatif Sentinel

Si vous utilisez SLES 12 SP3, vous pouvez vous enregistrer pour recevoir les mises à jour à l'aide de la console de gestion de l'applicatif Sentinel.

1. Lancez l'applicatif Sentinel en effectuant l'une des opérations suivantes :
   - Connectez-vous à Sentinel, puis cliquez sur **Sentinel Main** (Sentinel - Principal) > **Appliance** (Applicatif).
   - Indiquez l'URL suivante dans votre navigateur Web : `https://<adresse_IP>:9443`.
2. Connectez-vous en tant qu'utilisateur `vaadmin` ou `root`.
3. Cliquez sur **Online Update** (Mise à jour en ligne) > **Register Now** (S'enregistrer maintenant).
4. Dans le champ **Adresse électronique**, indiquez l'ID d'adresse électronique via lequel vous souhaitez recevoir les mises à jour.
5. Dans le champ **Clé d'activation**, entrez le code d'enregistrement.
6. Cliquez sur **Register** (S'enregistrer) pour terminer le processus d'enregistrement.

Enregistrement à l'aide de commandes

Si vous utilisez SLES 11 SP4 ou SLES 12 SP3, vous pouvez vous enregistrer à l'aide de commandes.

Pour s'enregistrer afin de recevoir les mises à jour :

1. Connectez-vous au serveur Sentinel en tant qu'utilisateur `root`.
2. Spécifiez les commandes suivantes :
   - Pour enregistrer un serveur, indiquez : `suse_register -a regcode-sentinel="<code_enregistrement>" -a email="<ID_message_électronique>"`
   - Pour enregistrer Collector Manager, indiquez : `suse_register -a regcode-sentinel-collector="<code_enregistrement>" -a email="<ID_message_électronique>"`

- Pour enregistrer Correlation Engine, indiquez : `suse_register -a regcode-sentinel-correlation ="<code_enregistrement>" -a email="<ID_message_électronique>"`
- Pour enregistrer Sentinel en haute disponibilité, indiquez : `suse_register -a regcode-sentinel-ha ="<code_enregistrement>" -a email="<ID_message_électronique>"`

Pour le paramétrage des e-mails, indiquez l'ID e-mail sur lequel vous souhaitez recevoir des mises à jour.

Création de partitions pour le stockage traditionnel

Les informations de cette section s'appliquent uniquement si vous souhaitez utiliser le stockage traditionnel comme solution de stockage des données.

Nous vous recommandons de créer des partitions distinctes pour stocker les données Sentinel sur une partition différente de celle qui contient les fichiers exécutables, de configuration et du système d'exploitation. L'isolation des données variables présente l'avantage de faciliter la sauvegarde et la récupération des ensembles de fichiers en cas d'altération et d'offrir un degré de protection supplémentaire si la partition du disque venait à être saturée. Pour plus d'informations sur la planification de vos partitions, reportez-vous à la « Planification du stockage traditionnel » page 43. Vous pouvez ajouter des partitions dans l'applicatif et déplacer un répertoire dans cette nouvelle partition à l'aide de l'outil YaST.

Utilisez la procédure suivante pour créer une partition et déplacer les fichiers de données de leur répertoire actuel vers la partition que vous venez de créer :

1. Connectez-vous à Sentinel avec l'identité d'un utilisateur `root`.
2. Exécutez la commande suivante pour arrêter Sentinel sur l'applicatif :

   ```
   /etc/init.d/sentinel stop
   ```
3. Entrez la commande suivante pour prendre l'identité de l'utilisateur `novell` :

   ```
   su -novell
   ```
4. Déplacez le contenu du répertoire `/var/opt/novell/sentinel` dans un emplacement temporaire.
5. Changez d'utilisateur et choisissez l'identité `root`.
6. Saisissez la commande suivante pour accéder à YaST2 Control Center :

   ```
   yast
   ```
7. Sélectionnez **Système > Partitionneur**.
8. Lisez l'avertissement et sélectionnez **Oui** pour ajouter la nouvelle partition inutilisée.

   Pour plus d'informations sur la création des partitions, reportez-vous à la section Using the YaST Partitioner (Utilisation du partitionneur YaST) dans la *documentation de SLES 11*.
9. Montez la nouvelle partition à l'emplacement `/var/opt/novell/sentinel`.
10. Entrez la commande suivante pour prendre l'identité de l'utilisateur `novell` :

    ```
    su -novell
    ```
11. Replacez dans la nouvelle partition le contenu du répertoire de données que vous avez stocké temporairement à l'Étape 4 dans `/var/opt/novell/sentinel`.
12. Exécutez la commande suivante pour redémarrer l'applicatif Sentinel :

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

Configuration du stockage évolutif

Pour activer et configurer le stockage évolutif comme solution de stockage des données, reportez-vous à la section « Configuring Scalable Storage (Configuration du stockage évolutif) du » Sentinel Administration Guide (Guide d'administration de NetIQ Sentinel).

Configuration de l'applicatif avec l'outil SMT (Subscription Management Tool)

Dans les environnements sécurisés où l'applicatif doit s'exécuter sans accès direct à Internet, vous devez le configurer à l'aide de l'outil SMT (Subscription Management Tool). Il vous permet en effet de mettre à niveau l'applicatif vers les dernières versions de Sentinel lorsqu'elles sont disponibles. L'outil SMT est un système proxy de paquetage intégré à Customer Center et offre les fonctions essentielles de Customer Center.

- « Conditions préalables » page 110
- « Configuration de l'applicatif » page 111
- « Mise à niveau de l'applicatif » page 111

Conditions préalables

Avant de configurer l'applicatif avec SMT, veillez à respecter les conditions préalables suivantes :

- Procurez-vous les informations d'identification du Customer Center pour obtenir des mises à jour de Sentinel. Pour plus d'informations sur l'obtention des informations d'identification, contactez le support technique.
- Vérifiez que SLES 11 SP3 est installé avec les paquets suivants sur l'ordinateur sur lequel vous souhaitez installer SMT :
  - htmldoc
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - perl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - yum-metadata-parser
  - createrepo
  - perl-DBI
  - apache2-prefork
  - libapr1
  - perl-Data-ShowTable
  - perl-Net-Daemon
  - perl-Tie-IxHash
  - fltk
  - libapr-util1
  - perl-PIRPC
  - apache2-mod_perl

- apache2-utils
- apache2
- perl-DBD-mysql

- Installez SMT et configurez le serveur SMT. Pour plus d'informations, reportez-vous aux sections suivantes de la documentation de SMT :
  - Installation de l'outil SMT
  - Configuration du serveur SMT
  - Mise en miroir de l'installation et mise à jour des espaces de stockage à l'aide de l'outil SMT
- Installez l'utilitaire `wget` sur l'ordinateur de l'applicatif.

Configuration de l'applicatif

Procédez comme suit pour configurer l'applicatif avec SMT :

1. Activez les espaces de stockage de l'applicatif en exécutant les commandes suivantes sur le serveur SMT :

   ```
   smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64
   ```

   ```
   smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64
   ```

   ```
   smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64
   ```

2. Configurez l'applicatif avec SMT en suivant les étapes décrites à la section « Configuring Clients to Use SMT » (Configuration des clients pour l'utilisation de SMT) dans la documentation de SMT.

Mise à niveau de l'applicatif

Pour plus d'informations sur la mise à niveau de l'applicatif, consultez la « Mise à niveau de Sentinel » page 161.

16 Installation de collecteurs et de connecteurs supplémentaires

Par défaut, tous les collecteurs et connecteurs disponibles s'installent en même temps que Sentinel. Pour installer un nouveau collecteur ou connecteur publié après la sortie de Sentinel, utilisez les informations fournies dans les sections suivantes.

Installation d'un collecteur

Procédez comme suit pour installer un collecteur :

1. Téléchargez le collecteur approprié sur le site Web des plug-ins Sentinel.
2. Depuis **l'interface principale de Sentinel**, cliquez sur le menu déroulant **admin**, puis sur **Applications**.
3. Cliquez sur **Démarrer Control Center** pour lancer Sentinel Control Center.
4. Dans la barre d'outils, cliquez sur **Gestion de source d'événements** > **Vue en direct**, puis cliquez sur **Outils** > **Importer le plug-in**.
5. Accédez au fichier de collecteur que vous avez téléchargé à l'Étape 1 et sélectionnez-le, puis cliquez sur **Suivant**.
6. Suivez les instructions des autres messages qui apparaissent, puis cliquez sur **Terminer**.

Pour configurer le collecteur, reportez-vous à la documentation propre à ce collecteur sur le site Web des plug-ins Sentinel.

Installation d'un connecteur

Procédez comme suit pour installer un connecteur :

1. Téléchargez le connecteur approprié sur le site Web des plug-ins Sentinel.
2. Depuis **l'interface principale de Sentinel**, cliquez sur le menu déroulant **admin**, puis sur **Applications**.
3. Cliquez sur **Démarrer Control Center** pour lancer Sentinel Control Center.
4. Dans la barre d'outils, sélectionnez **Gestion de source d'événements** > **Vue en direct**, puis cliquez sur **Outils** > **Importer le plug-in**.
5. Accédez au fichier de connecteur que vous avez téléchargé à l'Étape 1 et sélectionnez-le, puis cliquez sur **Suivant**.
6. Suivez les instructions des autres messages qui apparaissent, puis cliquez sur **Terminer**.

Pour configurer le connecteur, reportez-vous à la documentation propre à ce connecteur sur le site Web des plug-ins Sentinel.

17 Vérification de l'installation

Vous pouvez contrôler que l'installation a réussi en procédant de l'une des manières suivantes :

- Vérifiez la version de Sentinel :

  ```
  /etc/init.d/sentinel version
  ```

- Vérifiez si les services Sentinel sont actifs et s'ils fonctionnent en mode FIPS ou non-FIPS :

  ```
  /etc/init.d/sentinel status
  ```

- Vérifiez si les services Web sont actifs et en cours d'exécution :

  ```
  netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  Le numéro de port par défaut est 8443.

- Lancez Sentinel :

  1. Démarrez un navigateur Web pris en charge.
  2. Indiquez l'URL de Sentinel :

     ```
     https://IP_AddressOrDNS_Sentinel_server:8443
     ```

     où *IP_AddressOrDNS_Sentinel_server* est l'adresse IP ou le nom DNS du serveur Sentinel et *8443* le port par défaut du serveur Sentinel.
  3. Connectez-vous à l'aide du nom d'administrateur et du mot de passe spécifiés pendant l'installation. Le nom d'utilisateur par défaut est admin.

IV Configuration de Sentinel

Cette section fournit des informations sur la configuration de Sentinel et des plug-ins prêts à l'emploi.

18 Configuration de l'heure

L'heure d'un événement est déterminante pour son traitement dans Sentinel. Elle est importante pour la génération de rapports et l'audit, ainsi que pour le traitement en temps réel. Cette section fournit des explications sur l'heure dans Sentinel ainsi que sur la configuration de cette dernière et la gestion des fuseaux horaires.

Présentation de l'heure dans Sentinel

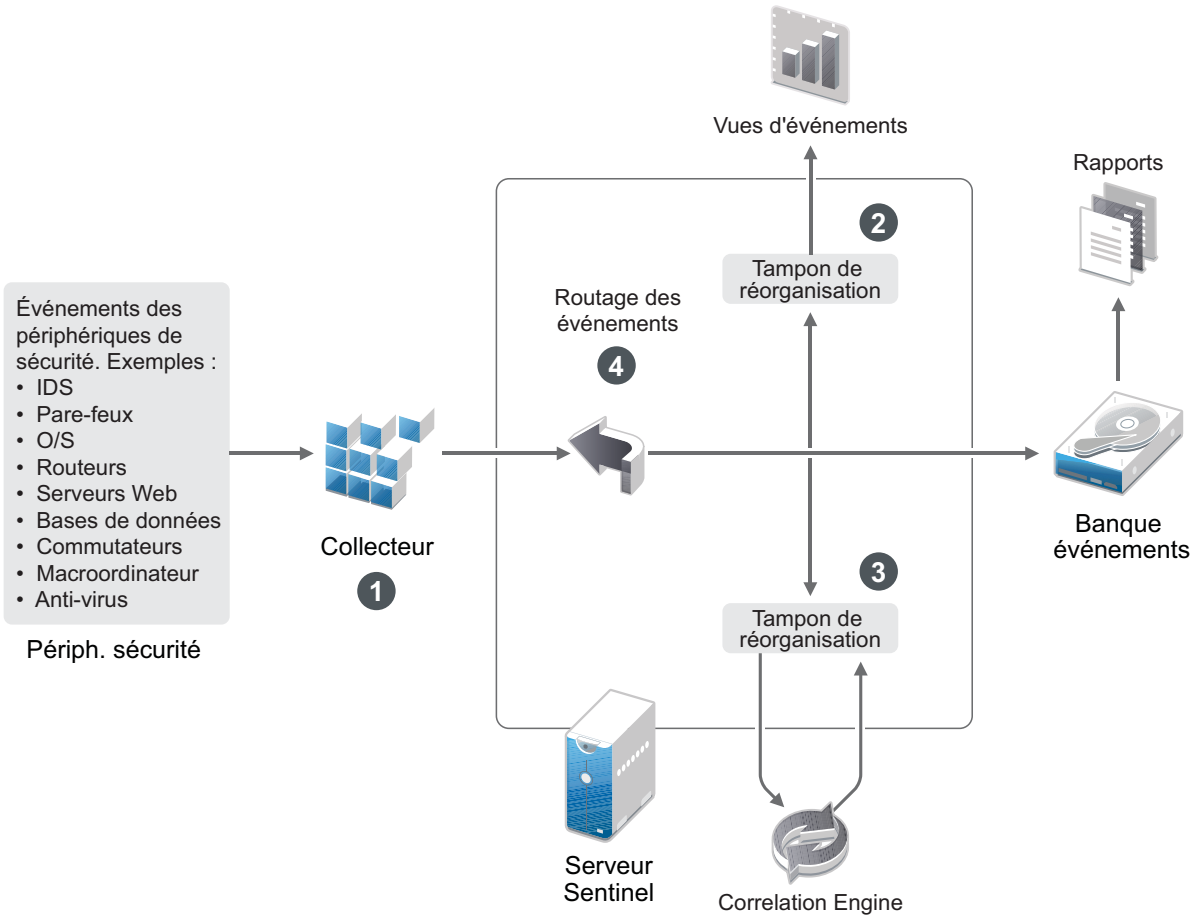
Sentinel est un système distribué constitué de plusieurs processus disséminés sur l'ensemble de votre réseau. En outre, la source d'événements peut être à l'origine d'un certain retard. Pour pallier cela, les processus Sentinel reclassent les événements dans l'ordre chronologique avant de les traiter.

Chaque événement contient trois champs horaires :

- **Heure de l'événement :** il s'agit de l'heure de l'événement utilisée notamment par les rapports, les recherches et moteurs d'analyse.
- **Heure de traitement par Sentinel :** heure à laquelle Sentinel a collecté les données partir du périphérique basée sur l'heure système de Collector Manager.
- **Heure de l'événement pour l'observateur :** tampon horaire dans lequel le périphérique place les données. Le tampon horaire des données n'est pas toujours fiable et peut être très différent de l'heure de traitement par Sentinel, notamment lorsque le périphérique fournit les données par lots.

L'illustration suivante décrit la manière dont Sentinel procède avec une configuration de stockage traditionnel :

Figure 18-1 *Heure Sentinel*



1. Par défaut, l'heure d'un événement est définie sur l'heure de traitement par Sentinel. L'idéal est toutefois que l'heure de l'événement corresponde à celle de l'observateur si cette dernière est disponible et fiable. Il est recommandé de configurer la collecte de données sur **Faire confiance à heure de la source d'événements** si l'heure du périphérique est disponible, exacte et correctement analysée par le collecteur. Le collecteur définit l'heure de l'événement pour la faire correspondre à celle de l'observateur.
2. Les événements dont l'heure diffère de maximum 5 minutes (d'avance ou de retard) par rapport à celle du serveur sont traités normalement par les vues d'événement. Les événements dont l'heure a plus de 5 minutes d'avance par rapport à l'heure du serveur ne s'affichent pas dans les vues d'événement, mais sont insérés dans la banque d'événements. Les événements dont l'heure a plus de 5 minutes d'avance et qui remontent à moins de 24 heures s'affichent dans les graphiques, mais pas dans les données d'événement correspondant à ce graphique. Il est par conséquent nécessaire de forer vers le bas pour récupérer ces événements de la banque d'événements.
3. Les événements sont triés à 30 secondes d'intervalle afin que instances Correlation Engine puisse les traiter dans l'ordre chronologique. Si l'heure de l'événement a plus de 30 secondes de retard par rapport à celle du serveur, Correlation Engine ne traite pas les événements.
4. Si l'heure de l'événement a plus de 5 minutes de retard par rapport à l'heure système de Collector Manager, Sentinel achemine directement les événements vers la banque d'événements, en ignorant les systèmes en temps réel tels que Correlation Engine et Security Intelligence.

Configuration de l'heure dans Sentinel

Correlation Engine traite les flux d'événements classés par heure et détecte les modèles dans les événements, ainsi que les schémas temporaires dans les flux. Toutefois, le périphérique qui génère l'événement n'inclut pas toujours l'heure dans ses messages de journal.

Pour configurer l'heure afin de garantir le bon fonctionnement de Sentinel, vous avez deux possibilités :

- Configurez NTP sur Collector Manager et désélectionnez l'option **Faire confiance à l'heure de la source d'événements** pour la source d'événements dans le gestionnaire des sources d'événements. Sentinel utilise Collector Manager en tant que source horaire des événements.
- Sélectionnez **Faire confiance à l'heure de la source d'événements** sur la source d'événements dans le gestionnaire des sources d'événements. Sentinel utilise l'heure du message du journal comme heure correcte.

Pour changer ce paramètre sur la source d'événements :

1. Connectez-vous à la fonctionnalité Gestion de source d'événements.

   Pour plus d'informations, reportez-vous à la section « Accessing Event Source Management (Accès à la gestion des sources d'événements) » du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
2. Cliquez avec le bouton droit sur la source d'événements dont vous souhaitez modifier le paramètre d'heure, puis sélectionnez **Éditer**.
3. Sélectionnez ou désélectionnez l'option **Faire confiance à l'heure de la source d'événements** au bas de l'onglet **Général**.
4. Cliquez sur **OK** pour enregistrer la modification.

Configuration de la limite de délai pour les événements

Lorsque Sentinel reçoit des événements depuis des sources d'événements, il peut y avoir un délai entre leur génération et le moment où Sentinel les traite. Sentinel stocke les événements qui présentent des délais importants dans des partitions distinctes. Si de nombreux événements enregistrent des délais importants, cela peut indiquer qu'une source d'événements est mal configurée. Cela peut également affecter les performances de Sentinel lorsqu'il tente de traiter les événements en retard. Ces délais pouvant être dus à une configuration incorrecte et le stockage de ces événements n'étant, dès lors, peut-être pas souhaitable, Sentinel vous permet de configurer une limite de délai acceptable pour les événements entrants. Le routeur d'événements supprime les événements qui dépassent le délai limite. Indiquez la limite de délai dans la propriété suivante du fichier `configuration.properties` :

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

Vous pouvez également définir la journalisation périodique d'une liste dans le fichier journal du serveur Sentinel afin d'afficher les sources d'événements à partir desquelles les événements reçus sont différés au-delà d'une certaine limite. Pour consigner ces informations, indiquez le seuil dans la propriété suivante du fichier `configuration.properties` :

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

Gestion des fuseaux horaires

La gestion des fuseaux horaires peut s'avérer très complexe dans un environnement distribué. Par exemple, une source d'événements peut se trouver dans un premier fuseau horaire, Collector Manager dans un deuxième, le serveur Sentinel de l'interface dorsale dans un troisième et le client qui consulte les données dans un quatrième. Si vous ajoutez les difficultés liées à l'heure d'été et également au fait que de nombreuses sources d'événements n'indiquent pas le fuseau horaire dans lequel elles sont définies (c'est le cas notamment de toutes les sources syslog), vous pouvez vous trouver devant un grand nombre de problèmes à résoudre. Sentinel est adaptable : vous pouvez représenter correctement l'heure exacte à laquelle les événements se produisent, puis comparer ces événements à ceux d'autres sources du même fuseau horaire ou d'un autre.

En général, les sources d'événements signalent les tampons horaires de trois manières :

- La source d'événements signale l'heure en temps UTC. Par exemple, tous les événements standard du journal des événements Windows sont signalés en temps UTC.
- La source d'événements signale l'heure dans l'heure locale, mais indique toujours le fuseau horaire dans le tampon horaire. Par exemple, certaines sources d'événements qui suivent la norme RFC3339 dans la structuration des tampons horaires indiquent le fuseau horaire sous forme de décalage ; d'autres sources signalent les fuseaux horaires sous forme d'identifiants longs (Amériques//New York par exemple) ou d'identifiants courts (EST par exemple), ce qui peut provoquer des conflits et des résolutions inadéquates.
- La source d'événements indique l'heure locale, mais pas le fuseau horaire. Malheureusement, le format syslog, extrêmement courant, suit ce modèle.

Pour ce premier scénario, vous pouvez toujours calculer en temps UTC absolu l'heure à laquelle l'événement est survenu (dans la mesure où un protocole de synchronisation est utilisé), ce qui vous permet de comparer facilement l'heure de cet événement à celle de toute autre source d'événements dans le monde. En revanche, vous ne pouvez pas déterminer automatiquement l'heure locale à laquelle l'événement s'est produit. C'est pour cette raison que Sentinel permet aux clients de définir manuellement le fuseau horaire d'une source d'événements : il suffit de modifier le noeud de la source d'événements dans le gestionnaire des sources d'événements et d'indiquer le fuseau horaire adéquat. Cette information n'a aucune incidence sur le calcul des heures DeviceEventTime ou EventTime, mais elle est placée dans le champ ObserverTZ et sert au calcul de différents champs ObserverTZ, ObserverTZHour par exemple. Ces champs sont toujours exprimés dans l'heure locale.

Dans le second scénario, si les identifiants de fuseau horaire ou des décalages sont utilisés au format long, vous pouvez convertir facilement l'heure en temps UTC, ce qui vous permet d'obtenir l'heure UTC canonique absolue (stockée dans le champ DeviceEventTime) et également de calculer les champs ObserverTZ en heure locale. En cas d'utilisation d'identifiants de fuseau horaire courts, des conflits risquent de survenir.

Le troisième scénario implique que l'administrateur définisse manuellement le fuseau horaire de toutes les sources concernées de manière à ce que Sentinel puisse calculer correctement le temps UTC. Si la modification du noeud de la source d'événements dans le gestionnaire des sources d'événements n'indique pas le fuseau horaire correctement, le champ DeviceEventTime (et probablement le champ EventTime également) peuvent être incorrects, de même que le champ ObserverTZ et les champs associés.

En général, le collecteur d'un type de source d'événements donné (Microsoft Windows par exemple) connaît la méthode de présentation des tampons horaires qu'utilise cette source et s'ajuste en conséquence. Les bonnes pratiques consistent à définir manuellement le fuseau horaire de tous les noeuds de source d'événements dans le gestionnaire des sources d'événements, sauf si vous savez que la source d'événements signale les heures dans l'heure locale et indique toujours le fuseau horaire dans le tampon horaire.

La présentation de la source d'événements pour le tampon horaire est traitée au niveau du collecteur et de Collector Manager. Les champs DeviceEventTime et EventTime sont stockés en temps UTC, tandis que les champs ObserverTZ sont stockés sous la forme de chaînes définies dans l'heure locale de la source d'événements. Ces informations sont envoyées par Collector Manager au serveur Sentinel et sont stockées dans la banque d'événements. Le fuseau horaire de Collector Manager et du serveur Sentinel ne devrait pas avoir d'incidence sur ce processus ni sur les données stockées. Toutefois, si un client affiche l'événement dans un navigateur Web, l'heure de l'événement au format UTC est convertie au format d'heure locale du navigateur Web, afin que tous les événements soient présentés aux clients en utilisant le fuseau horaire local. Si les utilisateurs souhaitent connaître l'heure locale de la source, ils peuvent consulter les champs ObserverTZ.

19 Sécurisation des données dans Elasticsearch

Sentinel utilise Kibana, un tableau de bord d'analyse et de recherche basé sur le navigateur, qui vous aide à visualiser les événements et les alertes dans des tableaux de bord. Sentinel stocke et indexe les alertes dans Elasticsearch. Vous pouvez configurer Sentinel pour également stocker et indexer les événements dans Elasticsearch afin de tirer parti des fonctions de visualisation d'événements. Les tableaux de bord Sentinel accèdent aux données à partir d'Elasticsearch pour présenter des événements et des alertes dans des tableaux de bord. Pour vous assurer que les tableaux de bord affichent uniquement les données que le rôle d'un utilisateur est autorisé à afficher et pour empêcher tout accès non autorisé aux données dans Elasticsearch, vous devez installer le plug-in de sécurité Elasticsearch. Pour plus d'informations, reportez-vous à la section « Sécurisation des données dans Elasticsearch » page 81.

20 Activation de la visualisation des événements

Dans une configuration de stockage évolutif, les visualisations d'événements sont disponibles par défaut. Dans une configuration de stockage traditionnelle, les visualisations d'événements sont disponibles uniquement si vous avez activé le magasin de données de visualisation (Elasticsearch) pour stocker et indexer des données.

Conditions préalables

Pour une indexation évolutive et distribuée des événements dans des environnements de production, vous devez configurer des nœuds Elasticsearch supplémentaires dans un mode en grappe. Pour installer et configurer Elasticsearch dans un mode en grappe, reportez-vous à la section « Installation et configuration d'Elasticsearch » page 79.

Activation de la visualisation des événements

Pour activer la visualisation des événements :

1. Connectez-vous au serveur Sentinel en tant qu'utilisateur novell.
2. Ouvrez le fichier `/etc/opt/novell/sentinel/config/configuration.properties`.
3. Définissez `eventvisualization.traditionalstorage.enabled` sur `true`.
4. Rafraîchissez l'interface utilisateur après quelques minutes pour afficher les visualisations d'événements.

   Vous devriez maintenant voir tous les tableaux de bord activés dans l'interface utilisateur **My Sentinel**. Lancez un tableau de bord quelconque, le tableau de bord Recherche de menaces par exemple, puis cliquez sur **Rechercher**. Le tableau de bord affiche tous les événements générés au cours de la dernière heure.
5. (Facultatif) Les tableaux de bord de visualisation des événements affichent uniquement les événements traités une fois que vous avez activé la visualisation des événements. Pour afficher les événements figurant dans le stockage basé sur les fichiers, vous devez migrer les données à partir du stockage basé sur les fichiers vers Elasticsearch. Pour plus d'informations, reportez-vous à la section Chapitre 33, « Migration de données vers Elasticsearch », page 185.

REMARQUE : L'activation ou la désactivation de la visualisation des événements génère une exception, étant donné qu'elle redémarre les services d'indexation de Sentinel. Cette exception est normale et vous pouvez l'ignorer.

---

21 Modification de la configuration après l'installation

Après l'installation de Sentinel, si vous souhaitez entrer la clé de licence valide, changer le mot de passe ou modifier les ports assignés, vous pouvez exécuter le script `configure.sh` pour effectuer ces modifications. Le script est disponible dans le dossier `/opt/novell/sentinel/setup`.

1. Arrêtez Sentinel à l'aide de la commande suivante :

   ```
   rcsentinel stop
   ```

2. Indiquez dans la ligne de commande la commande suivante pour exécuter le script `configure.sh` :

   ```
   ./configure.sh
   ```

3. Indiquez `1` pour effectuer une configuration standard ou `2` pour effectuer une configuration personnalisée de Sentinel.
4. Appuyez sur la barre d'espacement pour lire l'intégralité de l'accord de licence.
5. Tapez `yes` ou `y` pour accepter l'accord de licence et poursuivre l'installation.

   L'installation peut prendre quelques secondes à charger les paquetages d'installation.
6. Indiquez `1` pour utiliser la clé de licence d'évaluation par défaut.

   ou

   Saisissez `2` afin d'entrer la clé de licence achetée pour Sentinel.
7. Déterminez si vous souhaitez conserver le mot de passe existant pour l'utilisateur administrateur `admin`.
   - Si vous souhaitez conserver le mot de passe existant, saisissez `1`, puis passez à l'Étape 8.
   - Si vous souhaitez modifier le mot de passe existant, saisissez `2`, indiquez le nouveau mot de passe, confirmez-le, puis passez à l'Étape 8.

     L'utilisateur `admin` est l'identité utilisée pour effectuer des tâches d'administration par le biais de l'interface principale de Sentinel, notamment la création d'autres comptes utilisateur.
8. Déterminez si vous souhaitez conserver le mot de passe existant pour l'utilisateur de base de données `dbauser`.
   - Si vous souhaitez conserver le mot de passe existant, saisissez `1`, puis passez à l'Étape 9.
   - Si vous souhaitez modifier le mot de passe existant, saisissez `2`, indiquez le nouveau mot de passe, confirmez-le, puis passez à l'Étape 9.

   Le compte `dbauser` correspond à l'identité utilisée par Sentinel pour interagir avec la base de données. Le mot de passe que vous saisissez ici peut être utilisé pour les tâches de maintenance de base de données, y compris la réinitialisation du mot de passe admin en cas de perte ou d'oubli.
9. Déterminez si vous souhaitez conserver le mot de passe existant pour l'utilisateur d'application `appuser`.
   - Si vous souhaitez conserver le mot de passe existant, saisissez `1`, puis passez à l'Étape 10.

- Si vous souhaitez modifier le mot de passe existant, saisissez 2, indiquez le nouveau mot de passe, confirmez-le, puis passez à l'Étape 10.

  Le compte `appuser` est une identité interne qu'utilise le processus Java de Sentinel pour établir la connexion et interagir avec la base de données. Le mot de passe que vous indiquez ici permet d'effectuer des tâches sur la base de données.

10 Changez les assignations de port pour les services Sentinel en saisissant le numéro souhaité, puis en indiquant le numéro du nouveau port.

11 Après avoir modifié les ports, tapez 7 lorsque vous avez terminé.

12 Saisissez 1 pour authentifier les utilisateurs qui utilisent uniquement la base de données interne.

ou

Si vous avez configuré un annuaire LDAP dans votre domaine, saisissez 2 pour authentifier les utilisateurs à l'aide de l'authentification d'annuaires LDAP.

La valeur par défaut est de 1.

22 Configuration des plug-ins prêts à l'emploi

Sentinel a été préinstallé avec les plug-ins Sentinel par défaut disponibles au moment de la sortie du logiciel.

Ce chapitre fournit des informations sur la configuration des plug-ins prêts à l'emploi.

Consultation des plug-ins préinstallés

Vous pouvez consulter la liste des plug-ins préinstallés dans Sentinel. Vous pouvez également afficher les versions des plug-ins et d'autres métadonnées pour vous aider à déterminer si vous disposez de la version la plus récente.

Pour afficher les plug-ins installés sur votre serveur Sentinel, procédez comme suit :

1. Connectez-vous en tant qu'administrateur à l'interface principale de Sentinel à l'adresse `https://<adresse IP>:8443`, 8443 étant le port par défaut du serveur Sentinel.
2. Cliquez sur **Plug-ins** > **Catalogue**.

Configuration de la collecte des données

Pour plus d'informations sur la configuration de Sentinel en vue de la collecte de données, reportez-vous à la section « Collecting and Routing Event Data » (Collecte et routage des données d'événement) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Configuration des Solution Packs

L'application Sentinel est livrée avec une large gamme de contenus prêts à l'emploi et très utiles que vous pouvez utiliser immédiatement pour répondre à de nombreux besoins d'analyse. La plupart du contenu de Sentinel provient des packs préinstallés suivants : Sentinel Core Solution Pack et Solution Pack for ISO 27000 Series. Pour plus d'informations, reportez-vous à la section « Using Solution Packs » (Utilisation de Solution Packs) du manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel 7.0.1).

Les Solution Packs permettent de regrouper et de trier le contenu en contrôles ou ensembles de stratégies qui sont traités en tant qu'unité. Les contrôles de ces Solution Packs sont préinstallés pour vous fournir ce contenu prêt à l'emploi, ce qui ne vous empêche toutefois pas de devoir les implémenter et les tester formellement à l'aide de l'interface principale de Sentinel.

Si une certaine rigueur s'impose et que vous devez prouver que Sentinel fonctionne correctement, vous pouvez utiliser le processus d'attestation formel intégré dans l'ensemble Solution Packs. Ce processus d'attestation exécute et teste les contrôles Sentinel Pack comme si vous le faisiez à partir d'un autre ensemble Solution Pack. Dans le cadre de ce processus, la personne chargée de l'exécution et celle responsable des tests attestent qu'elles ont effectué ces tâches ; ces attestations s'intègrent alors dans un suivi d'audit qui peut être examiné pour démontrer qu'un contrôle donné a été déployé correctement.

Cette attestation peut être réalisée à l'aide de Solution Manager. Pour plus d'informations sur l'exécution et le test des contrôles, reportez-vous à la section « Installing and Managing Solution Packs » (Installation et gestion des Solution Packs) du manuel *Sentinel User Guide* (Guide de l'utilisateur NetIQ Sentinel).

Configuration d'opérations et d'intégrateurs

Pour plus d'informations sur la configuration des plug-ins prêts à l'emploi, reportez-vous à la documentation relative aux plug-ins sur le site Web des plug-ins Sentinel.

23 Activation du mode FIPS 140-2 dans une installation Sentinel existante

Ce chapitre fournit des informations sur l'activation du mode FIPS 140-2 dans une installation existante de Sentinel.

REMARQUE : Ces instructions partent du principe que Sentinel est installé dans le répertoire `/opt/novell/sentinel`. Les commandes doivent être exécutées en tant qu'utilisateur `novell`.

Activation du serveur Sentinel pour une exécution en mode FIPS 140-2

Pour configurer le serveur Sentinel afin qu'il s'exécute en mode FIPS 140-2 :

1. Connectez-vous au serveur Sentinel.
2. Modifiez votre nom d'utilisateur et utilisez l'identité `novell` (`su novell`).
3. Accédez au répertoire bin de Sentinel.
4. Exécutez le script `convert_to_fips.sh`, puis suivez les instructions qui s'affichent à l'écran.
5. (Conditionnel) Si votre environnement utilise une authentification forte ou à plusieurs facteurs, vous devez exécuter le script `create_mfa_fips_keys.sh` et suivre les instructions qui s'affichent à l'écran.

   REMARQUE : Pendant l'exécution du script, le mot de passe de la base de données nss est requis.

   ---
6. (Conditionnel) Si votre environnement utilise une authentification forte ou à plusieurs facteurs, vous devez fournir l'ID client Sentinel et le secret client Sentinel. Pour plus d'informations sur les méthodes d'authentification, reportez-vous à la section « Authentication Methods » (Méthodes d'authentification) du *Sentinel Administrator Guide* (Guide de l'administrateur Sentinel).

   Pour récupérer l'ID client Sentinel et le secret client Sentinel, accédez à l'URL suivante :

   `https://Nomhote:port/SentinelAuthServices/oauth/clients`

   Où :

   - *Nomhote* est le nom d'hôte du serveur Sentinel.
   - *Port* est le port qu'utilise Sentinel (généralement 8443).

   L'URL indiquée se base sur votre session Sentinel actuelle pour récupérer l'ID client Sentinel et le secret client Sentinel.
7. Redémarrez le serveur Sentinel.
8. Terminez la configuration du mode FIPS 140-2 en effectuant les tâches mentionnées au Chapitre 24, « Fonctionnement de Sentinel en mode FIPS 140-2 », page 135.

Activation du mode FIPS 140-2 sur des instances Collector Manager et Correlation Engine distantes

Le mode FIPS 140-2 doit être activé sur les instances Collector Manager et Correlation Engine distantes si vous souhaitez utiliser des communications certifiées FIPS lorsque le serveur Sentinel est exécuté en mode FIPS 140-2.

Pour configurer une instance Collector Manager ou Correlation Engine distante afin qu'elle s'exécute en mode FIPS 140-2 :

1. Connectez-vous au système distant Collector Manager ou Correlation Engine.
2. Modifiez votre nom d'utilisateur et utilisez l'identité `novell` (`su novell`).
3. Accédez au répertoire bin. L'emplacement par défaut est : `/opt/novell/sentinel/bin`.
4. Exécutez le script `convert_to_fips.sh`, puis suivez les instructions qui s'affichent à l'écran.
5. Redémarrez Collector Manager ou Correlation Engine.
6. Terminez la configuration du mode FIPS 140-2 en effectuant les tâches mentionnées au Chapitre 24, « Fonctionnement de Sentinel en mode FIPS 140-2 », page 135.

24 Fonctionnement de Sentinel en mode FIPS 140-2

Ce chapitre fournit des informations sur la configuration et le fonctionnement de Sentinel en mode FIPS 140-2.

Configuration du service Advisor en mode FIPS 140-2

Le service Advisor utilise une connexion HTTPS sécurisée pour télécharger son flux à partir du serveur Advisor. Le certificat utilisé par le serveur pour la communication sécurisée doit être ajouté à la base de données keystore FIPS de Sentinel.

Pour vérifier la réussite de l'enregistrement avec la base de données de gestion des ressources :

1. Téléchargez le certificat à partir du serveur Advisor et enregistrez le fichier sous `advisor.cer`.
2. Importez le certificat de serveur Advisor dans le keystore FIPS de Sentinel.

   Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

Configuration de la recherche distribuée en mode FIPS 140-2

Cette section fournit des informations sur la configuration de la recherche distribuée en mode FIPS 140-2.

Scénario 1 : les serveurs Sentinel source et cible sont en mode FIPS 140-2

Pour pouvoir effectuer des recherches distribuées sur plusieurs serveurs Sentinel s'exécutant en mode FIPS 140-2, vous devez ajouter les certificats utilisés pour la communication sécurisée dans le keystore FIPS.

1. Connectez-vous à l'ordinateur source de la recherche distribuée.
2. Accédez au répertoire du certificat :

   `cd <sentinel_install_directory>/config`
3. Copiez le certificat source (`sentinel.cer`) à un emplacement temporaire sur l'ordinateur cible.

4 Importez le certificat source dans le keystore FIPS cible de Sentinel.

   Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

5 Connectez-vous à l'ordinateur cible de la recherche distribuée.

6 Accédez au répertoire du certificat :

```
cd /etc/opt/novell/sentinel/config
```

7 Copiez le certificat cible (`sentinel.cer`) à un emplacement temporaire sur l'ordinateur source.

8 Importez le certificat du système cible dans le keystore FIPS Sentinel source.

9 Redémarrez les services Sentinel sur les ordinateurs source et cible.

Scénario 2 : le serveur Sentinel source est en mode non-FIPS et le serveur Sentinel cible est en mode FIPS 140-2

Vous devez convertir le keystore du serveur Web sur l'ordinateur source au format du certificat, puis exporter le certificat vers l'ordinateur cible.

1 Connectez-vous à l'ordinateur source de la recherche distribuée.

2 Créez le keystore du serveur Web dans le certificat au format (`.cer`) :

```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
password -file <certificate_name.cer>
```

3 Copiez le certificat source (`Sentinel.cer`) de la recherche distribuée à un emplacement temporaire sur l'ordinateur cible de la recherche distribuée.

4 Connectez-vous à l'ordinateur cible de la recherche distribuée.

5 Importez le certificat source dans le keystore FIPS cible de Sentinel.

   Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

6 Redémarrez les services Sentinel sur l'ordinateur cible.

Scénario 3 : le serveur Sentinel source est en mode FIPS et le serveur Sentinel cible est en mode non-FIPS

1 Connectez-vous à l'ordinateur cible de la recherche distribuée.

2 Créez le keystore du serveur Web dans le certificat au format (.cer) :

```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
password -file <certificate_name.cer>
```

3 Copiez le certificat à un emplacement temporaire sur l'ordinateur source de la recherche distribuée.

4 Importez le certificat cible dans le keystore FIPS Sentinel source.

   Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

5 Redémarrez les services Sentinel sur l'ordinateur source.

Configuration de l'authentification LDAP en mode FIPS 140-2

Pour configurer l'authentification LDAP pour des serveurs Sentinel exécutés en mode FIPS 140-2 :

1. Procurez-vous le certificat de serveur LDAP auprès de l'administrateur LDAP ou utilisez une commande. Par exemple,

   ```
   openssl s_client -connect <LDAP server IP>:636
   ```

   Copiez ensuite le texte renvoyé (à l'exception des lignes de début (BEGIN) et de fin (END) dans un fichier.
2. Importez le certificat de serveur LDAP dans le keystore FIPS de Sentinel.

   Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.
3. Accédez à l'**interface principale de Sentinel** en tant qu'utilisateur au rôle d'administrateur et procédez à la configuration de l'authentification LDAP.

   Pour plus d'informations, reportez-vous à la section « LDAP Authentication Against a Single LDAP Server Or Domain » (Authentification LDAP par rapport à un seul serveur ou domaine LDAP) du *Sentinel Administration Guide* (Guide d'administration de Sentinel).

REMARQUE : vous pouvez également configurer l'authentification LDAP pour un serveur Sentinel utilisant le mode FIPS 140-2 en exécutant le script `ldap_auth_config.sh` contenu dans le répertoire `/opt/novell/sentinel/setup`.

Mise à jour des certificats de serveur dans les instances Collector Manager et Correlation Engine distantes

Pour configurer des instances Collector Manager et Correlation Engine distantes existantes afin qu'elles communiquent avec un serveur Sentinel exécuté en mode FIPS 140-2, vous pouvez faire basculer le système distant en mode FIPS 140-2 ou mettre à jour le certificat de serveur Sentinel sur le système distant et laisser Collector Manager ou Correlation Engine en mode non-FIPS. Les instances Collector Manager distantes en mode FIPS peuvent ne pas être compatibles avec les sources d'événements ne prenant pas en charge FIPS ou nécessitant un des connecteurs Sentinel ne prenant pas encore en charge ce mode.

Si vous n'avez pas l'intention d'activer le mode FIPS 140-2 sur l'instance Collector Manager ou Correlation Engine distante, vous devez copier le dernier certificat de serveur Sentinel sur le système distant afin de permettre à Collector Manager ou Correlation Engine de communiquer avec le serveur Sentinel.

Pour mettre à jour le certificat de serveur Sentinel dans l'instance Collector Manager ou Correlation Engine distante :

1. Connectez-vous à l'ordinateur distant Collector Manager ou Correlation Engine.
2. Modifiez votre nom d'utilisateur et utilisez l'identité `novell` (`su novell`).
3. Accédez au répertoire bin. L'emplacement par défaut est : `/opt/novell/sentinel/bin`.
4. Exécutez le script `updateServerCert.sh` et suivez les instructions qui s'affichent à l'écran.

Configuration des plug-ins Sentinel pour une exécution en mode FIPS 140-2.

Cette section fournit des informations sur la configuration de divers plug-ins Sentinel à exécuter en mode FIPS 140-2.

REMARQUE : ces instructions sont fournies en partant du principe que vous avez installé Sentinel dans le répertoire `/opt/novell/sentinel`. Exécutez toutes les commandes en tant qu'utilisateur `novell`.

Connecteur Agent Manager

N'effectuez la procédure suivante que si vous avez sélectionné l'option **Codé (HTTPS)** lors de la configuration des paramètres de réseautique du serveur de source d'événements Agent Manager.

Pour configurer le connecteur Agent Manager pour qu'il s'exécute en mode FIPS 140-2 :

1. Ajoutez ou modifiez le serveur de source d'événements Agent Manager. Faites défiler les écrans de configuration jusqu'à ce que la fenêtre Sécurité s'affiche. Pour plus d'informations, reportez-vous au *Agent Manager Connector Guide* (Guide du connecteur Agent Manager).
2. Sélectionnez l'une des options disponibles dans le champ *Type d'authentification du client*. Le type d'authentification du client détermine dans quelle mesure le serveur SSL de source d'événements Agent Manager vérifie l'identité des sources d'événements Agent Manager qui tentent d'envoyer des données.
   - **Ouvert :** autorise toutes les connexions SSL provenant des agents Agent Manager. N'effectue aucune validation ni authentification du certificat client.
   - **Strict :** vérifie que le certificat est un certificat X.509 valide et contrôle également que le certificat client est approuvé par le serveur de source d'événements. Les nouvelles sources doivent être explicitement ajoutées à Sentinel (ce qui permet d'éviter que des sources malveillantes envoient des données non autorisées).

     Si l'option **Strict** est activée, vous devez importer le certificat de chaque nouveau client Agent Manager dans le keystore FIPS de Sentinel. Lorsque Sentinel est exécuté en mode FIPS 140-2, vous ne pouvez pas importer le certificat client à l'aide de l'interface ESM (Event Source Management).

     Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

REMARQUE : en mode FIPS 140-2, le serveur de source d'événements Agent Manager utilise la paire de clés du serveur Sentinel. L'importation de la paire de clés du serveur n'est dès lors pas nécessaire.

3 Si l'authentification serveur est activée dans les agents, ces derniers doivent en outre être configurés pour approuver le certificat du serveur Sentinel ou Collector Manager distant selon l'emplacement sur lequel le connecteur est déployé.

Emplacement du certificat du serveur Sentinel : `/etc/opt/novell/sentinel/config/sentinel.cer`

Emplacement du certificat Collector Manager distant : `/etc/opt/novell/sentinel/config/rcm.cer`

REMARQUE : lors de l'utilisation de certificats personnalisés ayant reçu la signature numérique d'une autorité de certification (CA), l'agent Agent Manager doit approuver le fichier de certificat approprié.

Connecteur (JDBC) de base de données

N'effectuez la procédure suivante que si vous avez sélectionné l'option *SSL* lors de la configuration de la connexion de base de données.

Pour configurer le connecteur de base de données pour qu'il s'exécute en mode FIPS 140-2 :

1 Avant de configurer le connecteur, téléchargez le certificat à partir du serveur de base de données et enregistrez le fichier sous `database.cert` dans le répertoire `/etc/opt/novell/sentinel/config` du serveur Sentinel.

Pour plus d'informations, reportez-vous à la documentation relative à la base de données.

2 Importez le certificat dans le keystore FIPS de Sentinel.

Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

3 Configurez le connecteur.

Connecteur Sentinel Link

N'effectuez la procédure suivante que si vous avez sélectionné l'option **Codé (HTTPS)** lors de la configuration des paramètres de réseautique du serveur de source d'événements Sentinel Link.

Pour configurer le connecteur Sentinel Link pour qu'il s'exécute en mode FIPS 140-2 :

1 Ajoutez ou modifiez le serveur de source d'événements Sentinel Link. Faites défiler les écrans de configuration jusqu'à ce que la fenêtre Sécurité s'affiche. Pour plus d'informations, reportez-vous au *Sentinel Link Connector Guide* (Guide du connecteur Sentinel Link).

2 Sélectionnez l'une des options disponibles dans le champ *Type d'authentification du client*. Le type d'authentification du client détermine dans quelle mesure le serveur SSL de source d'événements Sentinel Link vérifie l'identité des sources d'événements Sentinel Link (intégrateurs Sentinel Link) qui tentent d'envoyer des données.

- **Ouvert :** autorise toutes les connexions SSL provenant des clients (intégrateurs Sentinel Link). N'effectue aucune validation ni authentification du certificat de l'intégrateur.

- **Strict :** vérifie que le certificat de l'intégrateur est un certificat X.509 valide et contrôle également que le certificat de l'intégrateur est approuvé par le serveur de source d'événements. Pour plus d'informations, reportez-vous à la documentation relative à la base de données.

  Si l'option **Strict** est activée :

  - Si l'intégrateur Sentinel Link est en mode FIPS 140-2, vous devez copier le fichier `/etc/opt/novell/sentinel/config/sentinel.cer` présent sur la machine Sentinel de l'expéditeur sur celle du récepteur. Importez ce certificat dans le keystore FIPS Sentinel du récepteur.

    REMARQUE : lors de l'utilisation de certificats personnalisés ayant reçu la signature numérique d'une autorité de certification (CA), vous devez importer le fichier de certificat personnalisé approprié.

  - Si l'intégrateur Sentinel Link n'est pas en mode FIPS, vous devez importer le certificat personnalisé de l'intégrateur dans le keystore FIPS Sentinel du récepteur.

    REMARQUE : si l'expéditeur est Sentinel Log Manager (en mode non-FIPS) et que le récepteur est Sentinel en mode FIPS 140-2, le certificat serveur à importer auprès de l'expéditeur est le fichier `/etc/opt/novell/sentinel/config/sentinel.cer` de la machine Sentinel du récepteur.

  Lorsque Sentinel est exécuté en mode FIPS 140-2, vous ne pouvez pas importer le certificat client à l'aide de l'interface ESM (Event Source Management). Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

REMARQUE : en mode FIPS 140-2, le serveur de source d'événements Sentinel Link utilise la paire de clés du serveur Sentinel. L'importation de la paire de clés du serveur n'est dès lors pas nécessaire.

Connecteur Syslog

N'effectuez la procédure suivante que si vous avez sélectionné le protocole **SSL** lors de la configuration des paramètres de réseautique du serveur de source d'événements Syslog.

Pour configurer le connecteur Syslog pour qu'il s'exécute en mode FIPS 140-2 :

1. Ajoutez ou modifiez le serveur de source d'événements Syslog. Faites défiler les écrans de configuration jusqu'à ce que la fenêtre Réseautique s'affiche. Pour plus d'informations, reportez-vous au *Syslog Connector Guide* (Guide du connecteur Syslog).
2. Cliquez sur **Paramètres**.
3. Sélectionnez l'une des options disponibles dans le champ *Type d'authentification du client*. Le type d'authentification du client détermine dans quelle mesure le serveur SSL de source d'événements Syslog vérifie l'identité des sources d'événements Syslog qui tentent d'envoyer des données.
   - **Ouvert :** autorise toutes les connexions SSL provenant des clients (sources d'événements). N'effectue aucune validation ni authentification du certificat client.
   - **Strict :** vérifie que le certificat est un certificat X.509 valide et contrôle également que le certificat client est approuvé par le serveur de source d'événements. Les nouvelles sources doivent être explicitement ajoutées à Sentinel (ce qui permet d'éviter que des sources malveillantes envoient des données à Sentinel).

Si l'option **Strict** est activée, vous devez importer le certificat de chaque client Syslog dans le keystore FIPS de Sentinel.

Lorsque Sentinel est exécuté en mode FIPS 140-2, vous ne pouvez pas importer le certificat client à l'aide de l'interface ESM (Event Source Management).

Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

REMARQUE : en mode FIPS 140-2, le serveur de source d'événements Syslog utilise la paire de clés du serveur Sentinel. L'importation de la paire de clés du serveur n'est dès lors pas nécessaire.

---

4 Si l'authentification serveur est activée dans le client Syslog, ce dernier doit approuver le certificat du serveur Sentinel ou de l'instance Collector Manager distante selon l'emplacement sur lequel le connecteur est déployé.

Le fichier de certificat du serveur Sentinel se trouve à l'emplacement :`/etc/opt/novell/sentinel/config/sentinel.cer`.

Le fichier de certificat de l'instance Collector Manger distante se trouve à l'emplacement `/etc/opt/novell/sentinel/config/rcm.cer`.

REMARQUE : lors de l'utilisation de certificats personnalisés ayant reçu la signature numérique d'une autorité de certification (CA), le client doit approuver le fichier de certificat approprié.

Connecteur Windows Event (WMI)

Pour configurer le connecteur Windows Event (WMI) pour qu'il s'exécute en mode FIPS 140-2 :

1 Ajoutez ou modifiez le connecteur Windows Event. Faites défiler les écrans de configuration jusqu'à ce que la fenêtre Sécurité s'affiche. Pour plus d'informations, reportez-vous au guide *Windows Event (WMI) Connector Guide* [Guide du connecteur Windows Event (WMI)].

2 Cliquez sur **Paramètres**.

3 Sélectionnez l'une des options disponibles dans le champ *Type d'authentification du client*. Le type d'authentification du client détermine dans quelle mesure le connecteur Windows Event vérifie l'identité des services de collecte des événements Windows (WECS) du client qui tentent d'envoyer des données.

- **Ouvert :** autorise toutes les connexions SSL provenant des services WECS du client. N'effectue aucune validation ni authentification du certificat client.
- **Strict :** vérifie que le certificat est un certificat X.509 valide et contrôle également que le certificat WECS client a été signé par une autorité de certification. Les nouvelles sources doivent être explicitement ajoutées à Sentinel (ce qui permet d'éviter que des sources malveillantes envoient des données à Sentinel).

  Si l'option **Strict** est activée, vous devez importer le certificat des services WECS du client dans le keystore FIPS de Sentinel. Lorsque Sentinel est exécuté en mode FIPS 140-2, vous ne pouvez pas importer le certificat client à l'aide de l'interface ESM (Event Source Management).

  Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

REMARQUE : en mode FIPS 140-2, le serveur de source d'événements Windows utilise la paire de clés du serveur Sentinel. L'importation de la paire de clés du serveur n'est dès lors pas nécessaire.

4 Si l'authentification serveur est activée dans le client Windows, ce dernier doit approuver le certificat du serveur Sentinel ou de l'instance Collector Manager distante selon l'emplacement sur lequel le connecteur est déployé.

Le fichier de certificat du serveur Sentinel se trouve à l'emplacement :`/etc/opt/novell/sentinel/config/sentinel.cer`.

Le fichier de certificat de l'l'instance Collector Manager distante se trouve à l'emplacement `/etc/opt/novell/sentinel/config/rcm.cer`.

REMARQUE : lors de l'utilisation de certificats personnalisés ayant reçu la signature numérique d'une autorité de certification (CA), le client doit approuver le fichier de certificat approprié.

5 Si vous souhaitez synchroniser automatiquement les sources d'événements ou compléter la liste de sources d'événements à l'aide d'une connexion Active Directory, vous devez importer le certificat du serveur Active Directory dans le keystore FIPS de Sentinel.

Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

Intégrateur Sentinel Link

N'effectuez la procédure suivante que si vous avez sélectionné l'option **Codé (HTTPS)** lors de la configuration des paramètres réseau de l'intégrateur Sentinel Link.

Pour configurer l'intégrateur Sentinel Link pour qu'il s'exécute en mode FIPS 140-2 :

1 Lorsque l'intégrateur Sentinel Link est en mode FIPS 140-2, une authentification serveur est obligatoire?. Avant de configurer l'instance d'intégrateur, importez le certificat du serveur Sentinel Link dans le keystore FIPS de Sentinel :

- **Si Sentinel Link Connector est en mode FIPS 140-2** :

  Si le connecteur est déployé sur le serveur Sentinel, vous devez copier le fichier `/etc/opt/novell/sentinel/config/sentinel.cer` présent sur la machine Sentinel du destinataire sur celle de l'expéditeur.

  S'il est déployé sur une instance Collector Manager distante, vous devez copier le fichier `/etc/opt/novell/sentinel/config/rcm.cer` présent sur la machine Collector Manager distante du destinataire sur sa machine Sentinel.

  Importez ce certificat dans le keystore FIPS Sentinel de l'expéditeur.

  REMARQUE : lors de l'utilisation de certificats personnalisés ayant reçu la signature numérique d'une autorité de certification (CA), vous devez importer le fichier de certificat personnalisé approprié.

- Si Sentinel Link Connector n'est pas en mode FIPS :

  Importez le certificat personnalisé du serveur Sentinel Link dans le keystore FIPS Sentinel de l'expéditeur.

  REMARQUE : Lorsque l'intégrateur Sentinel Link est en mode FIPS 140-2 et que le connecteur Sentinel Link Connector n'utilise pas le mode FIPS, utilisez la paire de clés personnalisée du serveur sur le connecteur, et non la paire de clés interne du serveur.

Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

2 Configurez l'instance d'intégrateur.

REMARQUE : en mode FIPS 140-2, l'intégrateur Sentinel Link utilise la paire de clés du serveur Sentinel. L'importation de la paire de clés de l'intégrateur n'est pas nécessaire.

Intégrateur LDAP

Pour configurer l'intégrateur LDAP pour qu'il s'exécute en mode FIPS 140-2 :

1 Avant de configurer l'instance d'intégrateur, téléchargez le certificat à partir du serveur LDAP et enregistrez le fichier sous `ldap.cert` dans le répertoire `/etc/opt/novell/sentinel/config` du serveur Sentinel.

Par exemple, utilisez

```
openssl s_client -connect <LDAP server IP>:636
```

Copiez ensuite le texte renvoyé (à l'exception des lignes de début (BEGIN) et de fin (END) dans un fichier.

2 Importez le certificat dans le keystore FIPS de Sentinel.

Pour plus d'informations sur l'importation du certificat, reportez-vous à la section « Importation de certificats dans une base de données keystore FIPS » page 145.

3 Configurez l'instance d'intégrateur.

Intégrateur SMTP

L'intégrateur SMTP Integrator prend en charge le mode FIPS 140-2 à partir de la version 2011.1r2. Aucune modification de la configuration n'est requise.

Intégrateur Syslog

N'effectuez la procédure suivante que si vous avez sélectionné l'option Encrypted (SSL) (Chiffré [SSL]) lors de la configuration des paramètres réseau de l'intégrateur Syslog.

Pour configurer l'intégrateur Syslog pour qu'il s'exécute en mode FIPS 140-2, procédez comme suit :

1 Lorsque l'intégrateur Syslog est en mode FIPS 140-2, l'authentification du serveur est obligatoire. Avant de configurer l'instance d'intégrateur, importez le certificat du serveur Syslog dans le keystore FIPS de Sentinel :

- **Si le connecteur Syslog est en mode FIPS 140-2 :** si le connecteur est déployé sur le serveur Sentinel, vous devez copier le fichier `/etc/opt/novell/sentinel/config/sentinel.cer` présent sur le serveur Sentinel du destinataire sur celui de l'expéditeur.

  S'il est déployé sur une instance Collector Manager distante, vous devez copier le fichier `/etc/opt/novell/sentinel/config/rcm.cer` présent sur l'ordinateur Collector Manager distant du destinataire sur son ordinateur Sentinel.

  Importez ce certificat dans le keystore FIPS Sentinel de l'expéditeur.

REMARQUE : lors de l'utilisation de certificats personnalisés ayant reçu la signature numérique d'une autorité de certification (CA), vous devez importer le fichier de certificat personnalisé approprié.

- **Si le connecteur Syslog n'est pas en mode FIPS :** vous devez importer le certificat personnalisé du serveur Syslog dans le keystore FIPS Sentinel de l'expéditeur.

  REMARQUE : lorsque l'intégrateur Syslog est en mode FIPS 140-2 et que le connecteur Syslog n'utilise pas le mode FIPS, utilisez la paire de clés personnalisée du serveur sur le connecteur, et non la paire de clés interne du serveur.

Pour importer des certificats dans la base de données keystore FIPS :

1. Copiez le fichier de certificat à un emplacement temporaire sur le serveur Sentinel ou sur une instance Collector Manager distante.
2. Accédez au répertoire `/opt/novell/sentinel/bin`.
3. Exécutez la commande suivante pour importer le certificat dans la base de données keystore FIPS, puis suivez les instructions qui s'affichent à l'écran :

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

4. Entrez `yes` ou `y` lorsque vous êtes invité à redémarrer le serveur Sentinel ou une instance Collector Manager distante.

2 Configurez l'instance d'intégrateur.

REMARQUE : en mode FIPS 140-2, l'intégrateur Syslog utilise la paire de clés du serveur Sentinel. Il est inutile d'importer la paire de clés de l'intégrateur.

Utilisation de connecteurs non compatibles FIPS avec Sentinel en mode FIPS 140-2

Cette section fournit des informations sur la façon d'utiliser des connecteurs non compatibles FIPS avec un serveur Sentinel en mode FIPS 140-2. Cette approche est recommandée si certaines sources ne sont pas compatibles avec FIPS ou si vous souhaitez collecter des événements à partir de connecteurs ne prenant pas en charge FIPS dans votre environnement.

Pour utiliser des connecteurs non-FIPS avec Sentinel en mode FIPS 140-2 :

1 Installez une instance Collector Manager en mode non-FIPS à connecter au serveur Sentinel en mode FIPS 140-2.

Pour plus d'informations, reportez-vous à la section Partie III, « Installation de Sentinel », page 73.

2 Déployez les connecteurs non-FIPS expressément sur l'instance Collector Manager distante non-FIPS.

REMARQUE : certains problèmes connus se produisent lorsque des connecteurs non-FIPS tels que le connecteur d'audit et le connecteur de fichier sont déployés sur une instance Collector Manager distante non-FIPS connecté à un serveur Sentinel en mode FIPS 140-2. Pour plus d'informations sur les problèmes connus, reportez-vous aux notes de version de Sentinel .

Importation de certificats dans une base de données keystore FIPS

Pour pouvoir établir des communications sécurisées (SSL) à partir des composants qui détiennent des certificats vers Sentinel, vous devez insérer des certificats dans la base de données keystore FIPS de Sentinel. Vous ne pouvez pas télécharger de certificats à l'aide de l'interface utilisateur Sentinel lorsque le mode FIPS 140-2 est activé. Vous devez les importer manuellement dans la base de données keystore FIPS.

Pour les sources d'événements qui utilisent des connecteurs déployés sur une instance Collector Manager distante, vous devez importer les certificats dans la base de données keystore FIPS de l'instance Collector Manager distante et non sur le serveur Sentinel central.

Pour importer des certificats dans la base de données keystore FIPS :

1. Copiez le fichier de certificat à un emplacement temporaire sur le serveur Sentinel ou sur une instance Collector Manager distante.
2. Accédez au répertoire bin de Sentinel. L'emplacement par défaut est : `/opt/novell/sentinel/bin`.
3. Exécutez la commande suivante pour importer le certificat dans la base de données keystore FIPS, puis suivez les instructions qui s'affichent à l'écran.

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

4. Entrez `yes` ou `y` lorsque vous êtes invité à redémarrer le serveur Sentinel ou une instance Collector Manager distante.

Rétablissement de Sentinel en mode non-FIPS

Cette section fournit des informations sur la procédure de rétablissement de Sentinel et de ses composants en mode non-FIPS.

- « Rétablissement du serveur Sentinel en mode non-FIPS » page 145
- « Restauration des instances Collector Manager ou Correlation Engine distantes en mode non-FIPS » page 146

Rétablissement du serveur Sentinel en mode non-FIPS

Vous ne pouvez rétablir le mode non-FIPS d'un serveur Sentinel exécuté en mode FIPS 140-2 que si vous avez effectué une sauvegarde de votre serveur Sentinel avant la conversion en mode FIPS 140-2.

REMARQUE : lors du rétablissement d'un serveur Sentinel en mode non-FIPS, vous perdez les événements, les données d'incident ainsi que les changements apportés à la configuration de votre serveur Sentinel après la conversion pour une exécution en mode FIPS 140-2. Le système Sentinel récupéré sera celui d'avant la conversion en mode FIPS. Avant de rétablir le mode non-FIPS, vous devez effectuer une sauvegarde du système actuel en vue d'une utilisation ultérieure.

Pour rétablir votre serveur Sentinel en mode non-FIPS :

1. Connectez-vous au serveur Sentinel en tant qu'utilisateur `root`.
2. Modifiez votre nom d'utilisateur et utilisez l'identité `novell`.

3 Accédez au répertoire bin de Sentinel. L'emplacement par défaut est : `/opt/novell/sentinel/bin`.

4 Exécutez la commande suivante pour rétablir votre serveur Sentinel en mode non-FIPS, et suivez les instructions qui s'affichent à l'écran :

```
./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'
```

Par exemple, si le nom du fichier de sauvegarde est `non-fips20130124191111359034887.tar.gz`, exécutez la commande suivante :

```
./backup_util.sh -f non-fips20130124191111359034887.tar.gz -m 'restore'
```

5 Redémarrez le serveur Sentinel.

Restauration des instances Collector Manager ou Correlation Engine distantes en mode non-FIPS

Vous pouvez restaurer des instances Collector Manager ou Correlation Engine distantes en mode non-FIPS.

Pour restaurer une instance Collector Manager ou Correlation Engine distante en mode non-FIPS, procédez comme suit :

1 Connectez-vous au système distant de l'instance Collector Manager ou Correlation Engine distante.

2 Modifiez votre nom d'utilisateur et utilisez l'identité `novell` (`su novell`).

3 Accédez au répertoire bin. L'emplacement par défaut est : `/opt/novell/sentinel/bin`.

4 Exécutez le script `revert_to_nonfips.sh`, puis suivez les instructions qui s'affichent à l'écran.

5 Redémarrez l'instance Collector Manager ou Correlation Engine distante.

25 Ajout d'une bannière de consentement

Sentinel vous permet désormais d'afficher une bannière de consentement avant la connexion. Vous pouvez spécifier le contenu de la bannière, selon vos besoins. Après avoir ajouté la bannière de consentement, vous devez accepter les termes de cette dernière chaque fois que vous vous connectez à Sentinel.

Pour ajouter une bannière de consentement :

1. Connectez-vous au serveur Sentinel en tant qu'utilisateur `novell`.
2. Accédez à l'emplacement `/<chemin_installation_sentinel>/var/opt/novell/sentinel/3rdparty/jetty/webapps/ROOT/siemdownloads`.
3. Ajoutez un fichier texte avec le nom `USER_AGREEMENT.txt`.
4. Entrez le texte de l'accord utilisateur.
5. Enregistrez le fichier.
6. Lancez Sentinel pour afficher la bannière de consentement.

Sentinel affiche désormais la bannière de consentement sur l'écran de connexion.

REMARQUE : Vous devez sauvegarder manuellement le fichier `USER_AGREEMENT.txt` avant de mettre à niveau Sentinel.

V Mise à niveau de Sentinel

Cette section fournit des informations sur la mise à niveau de Sentinel et d'autres composants.

26 Liste de contrôle pour la mise en œuvre

Avant d'effectuer la mise à niveau de Sentinel, consultez la liste de contrôle suivante :

Tableau 26-1 *Liste de contrôle pour la mise en œuvre*

❒	Tâches	Voir
❒	Veillez à ce que les ordinateurs sur lesquels vous installez Sentinel et ses composants disposent de la configuration requise.	Site Web des informations techniques concernant Sentinel
❒	Consultez les notes de version du système d'exploitation pris en charge pour comprendre les problèmes connus.	Notes de version SUSE
❒	Consultez les notes de version de Sentinel afin de comprendre les nouvelles fonctionnalités et les problèmes connus.	Notes de version de Sentinel
❒	Effectuez les tâches mentionnées au chapitre Conditions préalables.	Chapitre 27, « Conditions préalables », page 153

27 Conditions préalables

Enregistrement des informations de configuration personnalisées

Enregistrement des paramètres du fichier server.conf

Si vous avez défini des valeurs personnalisées pour les paramètres de configuration dans le fichier `server.conf`, enregistrez ces valeurs dans des fichiers distincts avant la mise à niveau.

Pour enregistrer vos informations de configuration personnalisées, procédez comme suit :

1. Connectez-vous au serveur Sentinel en tant qu'utilisateur `novell` et accédez au répertoire `/etc/opt/novell/sentinel/config/`.
2. Créez un fichier de configuration nommé `server-custom.conf` et ajoutez-y vos paramètres de configuration personnalisés.

Sentinel applique la configuration personnalisée enregistrée dans ces fichiers de configuration pendant la mise à niveau.

Enregistrement des paramètres du fichier jetty-ssl

Sentinel 8.1 est fourni avec une mise à jour de Jetty. Cette mise à jour inclut des modifications de la structure de fichiers.

Si vous avez modifié le fichier `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml` dans une version antérieure de Sentinel, par exemple pour exclure un chiffrement, enregistrez ces modifications dans un fichier distinct avant de mettre Sentinel à niveau.

Une fois terminée la mise à niveau de Sentinel, copiez ces modifications dans le fichier `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl-context.xml` et redémarrez Sentinel.

Période de conservation étendue des données d'association des événements

À partir de Sentinel 7.4.4, la période de conservation par défaut des données d'association d'événement est de 14 jours. En cas mise à niveau depuis une version antérieure, la période de conservation que vous aviez définie pour ces associations sera remplacée par 14 jours. Pour l'éviter, vous pouvez définir la période de conservation voulue en ajoutant une propriété dans le fichier `configuration.properties`. Pour plus d'informations, reportez-vous à la section « Configuring the

Retention Period for the Event Associations Data » (Configuration de la période de conservation des données d'association d'événements) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Configuration préalable à la mise à niveau pour SSDM

La mise à niveau mettra à jour des fichiers liés aux applications Spark. Pour utiliser les mises à jour de fichiers, vous devez redémarrer la tâche Spark et réinitialiser tous les points de contrôle Spark des rubriques Kafka. Pour prévenir toute perte de données consécutive à la réinitialisation du point de contrôle de rubrique Kafka, vous devez suspendre l'acheminement des données depuis les gestionnaires des collecteurs vers Kafka avant la mise à niveau de SSDM. Tant que l'acheminement des données est suspendu, les données sont stockées dans le gestionnaire des collecteurs Collector Manager. Une fois que l'application Spark a terminé le traitement des données acheminées à Kafka avant la suspension, le point de contrôle peut être réinitialisé en toute sécurité et sans perte de données.

Pour suspendre l'acheminement des événements du gestionnaire des collecteurs à Kafka :

1. Dans l'interface principale de Sentinel, cliquez sur **Stockage** > **Stockage évolutif** > **Configuration avancée** > **Kafka**.
2. Ajoutez la propriété suivante et définissez-la sur vrai :

   ```
   pause.events.tokafka
   ```
3. Cliquez sur **Enregistrer**.

Intégration à Change Guardian

Sentinel est compatible avec Change Guardian 4.2 et versions ultérieures. Pour recevoir des événements de Change Guardian, vous devez d'abord mettre à niveau le serveur Change Guardian, les agents et l'éditeur de stratégie vers la version 4.2 ou une version ultérieure pour que Sentinel continue à recevoir des événements de Change Guardian après la mise à niveau.

28 Mise à niveau de l'installation traditionnelle de Sentinel

Mise à niveau de Sentinel

Procédez comme suit pour mettre à niveau le serveur Sentinel :

1. Sauvegardez votre configuration, puis créez une exportation ESM.

   Pour plus d'informations sur la sauvegarde des données, reportez-vous à la section « Backing Up and Restoring Data (Sauvegarde et restauration des données) » du manuel *Sentinel Administration Guide (Guide d'administration de NetIQ Sentinel 7.1)*.
2. (Conditionnel) Si vous avez personnalisé les paramètres de configuration dans les fichiers `server.xml`, `collector_mgr.xml` ou `correlation_engine.xml`, assurez-vous d'avoir créé les fichiers de propriétés appropriés nommés avec l'ID obj-component pour vous assurer que les personnalisations sont conservées après la mise à niveau. Pour plus d'informations, consultez la section « Maintaining Custom Settings in XML Files » (Conservation des paramètres personnalisés dans les fichiers XML) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
3. Téléchargez la dernière version du programme d'installation sur le site Web de téléchargement .
4. Connectez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez mettre à niveau Sentinel.
5. Entrez la commande suivante pour extraire les fichiers d'installation du fichier TAR :

   ```
   tar xfz <install_filename>
   ```

   Remplacez *<nom_fichier_installation>* par le nom réel du fichier d'installation.
6. Accédez au répertoire dans lequel le fichier d'installation a été extrait.
7. Indiquez la commande suivante pour mettre à niveau Sentinel :

   ```
   ./install-sentinel
   ```
8. Pour continuer dans la langue de votre choix, sélectionnez le numéro en regard de la langue.

   L'accord de licence utilisateur final s'affiche dans la langue sélectionnée.
9. Lisez l'accord de licence utilisateur final et tapez `Oui` ou `o` pour l'accepter, puis poursuivez l'installation.
10. Le script d'installation détecte qu'une version antérieure du produit existe déjà et vous demande si vous souhaitez mettre à niveau le produit. Pour procéder à la mise à niveau, appuyez sur `o`.

    Le processus démarre en installant tous les paquetages RPM. Cette installation peut prendre quelques secondes.

11 Videz le cache de votre navigateur Web pour afficher la dernière version de Sentinel.

12 Effacez le cache de Java Web Start sur les ordinateurs clients afin d'utiliser la dernière version des applications Sentinel.

   Vous pouvez effacer le cache de Java Web Start à l'aide de la commande `javaws -clearcache` ou du centre Java Control Center. Pour plus d'informations, consultez le fichier http://www.java.com/en/download/help/plugin_cache.xml.

13 (Conditionnel) Si la base de données PostgreSQL a été mise à niveau vers une version majeure (8.0 vers 9.0 ou 9.0 vers 9.1, par exemple), effacez les anciens fichiers PostgreSQL de la base de données. Pour savoir si la base de données PostgreSQL a été mise à niveau, consultez les notes de version de Sentinel.

   13a Modifiez votre nom d'utilisateur et utilisez l'identité novell.

   ```
   su novell
   ```

   13b Accédez au dossier `bin` :

   ```
   cd /opt/novell/sentinel/3rdparty/postgresql/bin
   ```

   13c Supprimez tous les anciens fichiers postgreSQL à l'aide de la commande suivante :

   ```
   ./delete_old_cluster.sh
   ```

14 Pour mettre à niveau les systèmes Collector Manager et Correlation Engine distantes, reportez-vous à la « Mise à niveau de Collector Manager ou Correlation Engine » page 158.

15 (Conditionnel) Si vous utilisez l'authentification Kerberos, activez AES256 dans votre environnement runtime Java étant donné que le dossier `java` est remplacé par les fichiers par défaut au cours de la mise à niveau. Pour activer AES256 dans votre environnement runtime Java, procédez comme suit :

   15a Téléchargez Java Cryptography Extension (JCE) 8 à l'emplacement suivant : `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

   15b Extrayez les deux `fichiers *.jar` et copiez-les dans le répertoire `/opt/novell/sentinel/jdk/jre/lib/security`.

   15c (Conditionnel) Si vous exécutez Sentinel dans un environnement à haute disponibilité, répétez cette procédure sur tous les nœuds de la grappe.

   15d Redémarrez Sentinel.

Mise à niveau de Sentinel en tant qu'utilisateur non-root

Si la stratégie de votre organisation ne vous permet pas d'exécuter la mise à niveau complète de Sentinel en tant qu'utilisateur `root`, vous pouvez effectuer la mise à niveau en tant qu'utilisateur non-root. Dans cette mise à niveau, les premières étapes sont effectuées en tant qu'utilisateur `root`, les étapes suivantes peuvent être effectuées par un autre utilisateur créé par l'utilisateur `root`.

1 Sauvegardez votre configuration, puis créez une exportation ESM.

   Pour plus d'informations sur la sauvegarde des données, reportez-vous à la section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

2 (Conditionnel) Si vous avez personnalisé les paramètres de configuration dans les fichiers `server.xml`, `collector_mgr.xml` ou `correlation_engine.xml`, assurez-vous d'avoir créé les fichiers de propriétés appropriés nommés avec l'ID obj-component pour vous assurer que les

personnalisations sont conservées après la mise à niveau. Pour plus d'informations, reportez-vous à la section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

3. Téléchargez les fichiers d'installation sur le site Web de téléchargement .
4. Entrez la commande suivante dans la ligne de commande pour extraire les fichiers d'installation du fichier tar :

   ```
   tar -zxvf <install_filename>
   ```

   Remplacez *<nom_fichier_installation>* par le nom réel du fichier d'installation.
5. Connectez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez mettre à niveau Sentinel.
6. Extrayez le RPM `squashfs` depuis les fichiers d'installation de Sentinel.
7. Installez le fichier `squashfs` sur le serveur Sentinel.

   ```
   rpm -Uvh <install_filename>
   ```
8. Entrez la commande suivante pour adopter l'identité de l'utilisateur non-root `novell` que vous venez de créer : `novell` :

   ```
   su novell
   ```
9. (Conditionnel) Pour effectuer une mise à niveau interactive :

   9a Entrez la commande suivante :

   ```
   ./install-sentinel
   ```

   Pour mettre à niveau Sentinel à un emplacement différent de l'emplacement par défaut, indiquez l'option --location avec la commande. Par exemple :

   ```
   ./install-sentinel --location=/foo
   ```

   9b Passez au Étape 11.
10. (Conditionnel) Pour effectuer une mise à niveau silencieuse, indiquez la commande suivante :

    ```
    ./install-sentinel -u <response_file>
    ```

    L'installation se poursuit et utilise les valeurs stockées dans le fichier de réponses. La mise à niveau de Sentinel est terminée.
11. Indiquez le numéro de la langue que vous souhaitez utiliser pour la mise à niveau.

    L'accord de licence utilisateur final s'affiche dans la langue sélectionnée.
12. Lisez l'accord de licence utilisateur final et tapez `yes` ou `y` pour l'accepter et poursuivre la mise à niveau.

    Le processus démarre en installant tous les paquetages RPM. Cette installation peut prendre quelques secondes.
13. Videz le cache de votre navigateur Web pour afficher la dernière version de Sentinel.
14. Effacez le cache de Java Web Start sur les ordinateurs clients afin d'utiliser la dernière version des applications Sentinel.

    Vous pouvez effacer le cache de Java Web Start à l'aide de la commande `javaws -clearcache` ou du centre Java Control Center. Pour plus d'informations, consultez le fichier http://www.java.com/en/download/help/plugin_cache.xml.

15 (Conditionnel) Si la base de données PostgreSQL a été mise à niveau vers une version majeure (8.0 vers 9.0 ou 9.0 vers 9.1, par exemple), effacez les anciens fichiers PostgreSQL de la base de données. Pour savoir si la base de données PostgreSQL a été mise à niveau, consultez les notes de version de Sentinel.

15a Connectez-vous en tant qu'utilisateur novell.

```
su novell
```

15b Accédez au dossier `bin` :

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

15c Supprimez tous les anciens fichiers postgreSQL à l'aide de la commande suivante :

```
./delete_old_cluster.sh
```

16 (Conditionnel) Si vous utilisez l'authentification Kerberos, activez AES256 dans votre environnement runtime Java étant donné que le dossier `java` est remplacé par les fichiers par défaut au cours de la mise à niveau. Pour activer AES256 dans votre environnement runtime Java, procédez comme suit :

16a Téléchargez Java Cryptography Extension (JCE) 8 à l'emplacement suivant : `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

16b Extrayez les deux `fichiers *.jar` et copiez-les dans le répertoire `/opt/novell/sentinel/jdk/jre/lib/security`.

16c (Conditionnel) Si vous exécutez Sentinel dans un environnement à haute disponibilité, répétez cette procédure sur tous les nœuds de la grappe.

16d Redémarrez Sentinel.

Mise à niveau de Collector Manager ou Correlation Engine

Procédez comme suit pour mettre à niveau Collector Manager ou Correlation Engine :

1 Sauvegardez votre configuration, puis créez une exportation ESM.

Pour plus d'informations, reportez-vous à la section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

2 Accédez à l'**interface principale de Sentinel** en tant qu'utilisateur au rôle d'administrateur.

3 Sélectionnez **Téléchargements**.

4 Cliquez sur **Télécharger le programme d'installation** dans la section du programme d'installation Collector Manager.

5 Enregistrez le fichier du programme d'installation sur le serveur respectif Collector Manager ou Correlation Engine.

6 Copiez le fichier à un emplacement temporaire.

7 Dézippez le contenu du fichier.

8 Exécutez le script suivant :

Pour Collector Manager :

```
./install-cm
```

Pour Correlation Engine :

```
./install-ce
```

9 Suivez les instructions affichées pour terminer l'installation.

10 (Conditionnel) Pour les installations personnalisées, exécutez la commande ci-dessous pour synchroniser les configurations du serveur Sentinel, Collector Manager et Correlation Engine :

```
/opt/novell/sentinel/setup/configure.sh
```

Mise à niveau du système d'exploitation

Cette version de Sentinel comprend un ensemble de commandes à utiliser lors de la procédure de mise à niveau du système d'exploitation. Ces commandes veillent à ce que Sentinel fonctionne correctement après avoir mis à niveau le système d'exploitation.

REMARQUE : Vous devez mettre à niveau Sentinel avant de mettre à niveau le système d'exploitation.

Procédez comme suit pour mettre à niveau votre système d'exploitation :

1 Sur le serveur Sentinel sur lequel vous souhaitez mettre à niveau votre système d'exploitation, connectez-vous sous l'une des identités suivantes :

- Utilisateur `root`
- Utilisateur non-root

2 Ouvrez une invite de commande et accédez au répertoire dans lequel le fichier d'installation Sentinel a été extrait.

3 Arrêtez les services Sentinel :

```
rcsentinel stop
```

4 (Conditionnel) Si Sentinel était en mode FIPS avant la mise à niveau du système d'exploitation, les fichiers de base de données NSS doivent être mis à niveau manuellement par la commande suivante :

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Suivez les instructions affichées pour mettre à niveau la base de données NSS.

Octroyez toutes les autorisations à l'utilisateur `novell` sur les fichiers suivants :

```
cert9.db
key4.db
pkcs11.txt
```

5 Mettez à niveau votre système d'exploitation.

6 (Conditionnel) Si vous utilisez Mozilla Network Security Services (NSS) 3.29, deux fichiers RPM dépendants `libfreebl3-hmac` et `libsoftokn3-hmac` ne sont pas installés. Installez manuellement les fichiers RPM suivants : `libfreebl3-hmac` et `libsoftokn3-hmac`.

7 (Conditionnel) Pour RHEL 7.*x*, exécutez la commande suivante pour vérifier s'il y a des erreurs dans la base de données RPM :

```
rpm -qa --dbpath <install_location>/rpm | grep novell
```

Exemple : `# rpm -qa --dbpath /custom/rpm | grep novell`

7a S'il y a des erreurs, exécutez la commande suivante pour réparer les erreurs :

`rpm --rebuilddb --dbpath <install_location>/rpm`

Exemple : `# rpm --rebuilddb --dbpath /custom/rpm`

7b Exécutez la commande indiquée à l'étape 7 pour vous assurer qu'il n'y a pas d'erreurs.

8 Répétez cette procédure pour les instances suivantes :

- Instances Collector Manager
- Instances Correlation Engine
- Instances NetFlow Collector Manager

9 Redémarrez le service Sentinel :

`rcsentinel restart`

Cette étape n'est pas applicable à Sentinel HA.

29 Mise à niveau de l'applicatif Sentinel

Les procédures décrites dans ce chapitre vous guident tout au long de la mise à niveau de l'applicatif Sentinel. Vous pouvez choisir de mettre à niveau Sentinel sans mettre à niveau le système d'exploitation SLES ou de mettre à niveau à la fois Sentinel et le système d'exploitation SLES. Étant donné que l'applicatif Sentinel 8.2 inclut désormais SLES 12 SP.3, le canal de mises à jour de SLES 11 est désormais obsolète et sera supprimé lorsque SUSE mettra fin à la prise en charge générale de SLES 11. Par conséquent, vous devez effectuer une mise à niveau vers l'applicatif Sentinel 8.2, lequel inclut le système d'exploitation SLES 12 SP3, pour continuer à recevoir les mises à jour du système d'exploitation. Vous devez effectuer la mise à niveau de Sentinel avant celle du système d'exploitation.

Mise à niveau de Sentinel

Mise à niveau de Sentinel via le canal de mise à jour de l'applicatif

Vous pouvez mettre à niveau Sentinel à l'aide de Zypper. Zypper est un gestionnaire de paquetages par ligne de commande qui sert à mettre à niveau l'applicatif de manière interactive. Quand la mise à niveau exige l'intervention de l'utilisateur, par exemple si le contrat de licence utilisateur final est modifié, vous devez utiliser Zypper pour mettre à niveau l'applicatif Sentinel.

Pour mettre à niveau l'applicatif via le canal de mise à jour de l'applicatif :

1. Sauvegardez votre configuration, puis créez une exportation ESM.

   Pour plus d'informations, reportez-vous à la section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
2. (Conditionnel) Si vous avez personnalisé les paramètres de configuration dans les fichiers `server.xml`, `collector_mgr.xml` ou `correlation_engine.xml`, assurez-vous d'avoir créé les fichiers de propriétés appropriés nommés avec l'ID obj-component pour vous assurer que les personnalisations sont conservées après la mise à niveau. Pour plus d'informations, consultez la section « Maintaining Custom Settings in XML Files » (Conservation des paramètres personnalisés dans les fichiers XML) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
3. Connectez-vous à la console d'applicatif en tant qu'utilisateur `root`.
4. Exécutez la commande suivante :

   ```
   /usr/bin/zypper patch
   ```

5. (Conditionnel) Si le programme d'installation affiche un message indiquant que vous devez résoudre une dépendance pour le paquet OpenSSH, entrez l'option appropriée pour mettre à niveau le paquet OpenSSH vers une version antérieure.
6. (Conditionnel) Si le programme d'installation affiche un message indiquant un changement dans l'architecture ncgOverlay, entrez l'option appropriée pour accepter le changement d'architecture.
7. (Conditionnel) Si le programme d'installation affiche un message indiquant que vous devez résoudre une dépendance pour certains paquets d'applicatifs, entrez l'option appropriée pour désinstaller les paquets dépendants.
8. Entrez `Y` pour continuer.
9. Entrez `Yes` pour accepter l'accord de licence.
10. Redémarrez l'applicatif Sentinel.
11. (Conditionnel) Si Sentinel est installé sur un port personnalisé ou si Collector Manager ou Correlation Engine est en mode FIPS, exécutez la commande suivante :

    ```
    /opt/novell/sentinel/setup/configure.sh
    ```
12. Videz le cache de votre navigateur Web pour afficher la dernière version de Sentinel.
13. Effacez le cache de Java Web Start sur les ordinateurs clients afin d'utiliser la dernière version des applications Sentinel.

    Vous pouvez effacer le cache de Java Web Start à l'aide de la commande `javaws -clearcache` ou du centre Java Control Center. Pour plus d'informations, consultez le fichier http://www.java.com/en/download/help/plugin_cache.xml.
14. (Conditionnel) Si la base de données PostgreSQL a été mise à niveau vers une version majeure (8.0 vers 9.0 ou 9.0 vers 9.1, par exemple), effacez les anciens fichiers PostgreSQL de la base de données. Pour savoir si la base de données PostgreSQL a été mise à niveau, consultez les notes de version de Sentinel.

    14a Connectez-vous en tant qu'utilisateur novell.

    ```
    su novell
    ```

    14b Accédez au dossier `bin` :

    ```
    cd /opt/novell/sentinel/3rdparty/postgresql/bin
    ```

    14c Supprimez tous les anciens fichiers postgreSQL à l'aide de la commande suivante :

    ```
    ./delete_old_cluster.sh
    ```
15. (Conditionnel) Pour mettre à niveau Collector Manager ou Correlation Engine, suivez la procédure de l'Étape 3 à l'Étape 11.
16. (Conditionnel) Si vous utilisez l'authentification Kerberos, activez AES256 dans votre environnement runtime Java étant donné que le dossier `java` est remplacé par les fichiers par défaut au cours de la mise à niveau. Pour activer AES256 dans votre environnement runtime Java, procédez comme suit :

    16a Téléchargez Java Cryptography Extension (JCE) 8 à l'emplacement suivant : `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

    16b Extrayez les deux `fichiers *.jar` et copiez-les dans le répertoire `/opt/novell/sentinel/jdk/jre/lib/security`.

    16c Redémarrez Sentinel.
17. (Conditionnel) Si vous exécutez Sentinel dans un environnement à haute disponibilité, répétez cette procédure sur tous les nœuds de la grappe.

18 (Facultatif) Pour mettre à niveau le système d'exploitation, reportez-vous à « Mise à niveau du système d'exploitation » page 164

19 Redémarrez Sentinel.

Mise à niveau de Sentinel à l'aide de SMT

Dans les environnements sécurisés où l'applicatif doit s'exécuter sans accès direct à Internet, vous pouvez le configurer à l'aide de l'outil SMT (Subscription Management Tool). Cet outil vous permet de le mettre à niveau vers les dernières versions disponibles.

1 Veillez à configurer l'applicatif avec SMT.

Pour plus d'informations, reportez-vous à la section « Configuration de l'applicatif avec l'outil SMT (Subscription Management Tool) » page 110.

2 Sauvegardez votre configuration, puis créez une exportation ESM.

Pour plus d'informations, reportez-vous à la section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

3 (Conditionnel) Si vous avez personnalisé les paramètres de configuration dans les fichiers `server.xml`, `collector_mgr.xml` ou `correlation_engine.xml`, assurez-vous d'avoir créé les fichiers de propriétés appropriés nommés avec l'ID obj-component pour vous assurer que les personnalisations sont conservées après la mise à niveau. Pour plus d'informations, consultez la section « Maintaining Custom Settings in XML Files » (Conservation des paramètres personnalisés dans les fichiers XML) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

4 Connectez-vous à la console d'applicatif en tant qu'utilisateur `root`.

5 Rafraîchissez l'espace de stockage pour la mise à niveau :

```
zypper ref -s
```

6 Vérifiez si l'applicatif est activé pour la mise à niveau :

```
zypper lr
```

7 (Facultatif) Recherchez les mises à jour disponibles pour l'applicatif :

```
zypper lu
```

8 (Facultatif) Recherchez les paquetages disponibles pour l'applicatif :

```
zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
```

9 Mettez à jour l'applicatif :

```
zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
```

10 Redémarrez l'applicatif.

```
rcsentinel restart
```

11 (Conditionnel) Si Sentinel est installé sur un port personnalisé ou si Collector Manager ou Correlation Engine est en mode FIPS, exécutez la commande suivante :

```
/opt/novell/sentinel/setup/configure.sh
```

12 (Conditionnel) Pour mettre à niveau Collector Manager ou Correlation Engine, suivez la procédure de l'Étape 4 à l'Étape 11.

13 (Conditionnel) Si vous utilisez l'authentification Kerberos, activez AES256 dans votre environnement runtime Java étant donné que le dossier `java` est remplacé par les fichiers par défaut au cours de la mise à niveau. Pour activer AES256 dans votre environnement runtime Java, procédez comme suit :

13a Téléchargez Java Cryptography Extension (JCE) 8 à l'emplacement suivant : `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

13b Extrayez les deux `fichiers *.jar` et copiez-les dans le répertoire `/opt/novell/sentinel/jdk/jre/lib/security`.

13c Redémarrez Sentinel.

14 (Conditionnel) Si vous exécutez Sentinel dans un environnement à haute disponibilité, répétez cette procédure sur tous les nœuds de la grappe.

15 (Facultatif) Pour mettre à niveau le système d'exploitation, reportez-vous à « Mise à niveau du système d'exploitation » page 164.

16 Redémarrez Sentinel.

Mise à niveau du système d'exploitation

Vous devez mettre à niveau le système d'exploitation après avoir mis à niveau Sentinel. Une fois le système d'exploitation mis à niveau, vous devez configurer l'applicatif de manière à exploiter les nouvelles fonctionnalités du gestionnaire de l'applicatif Sentinel. Le gestionnaire de l'applicatif Sentinel fournit une interface utilisateur Web simple qui permet de configurer et de gérer l'applicatif. Il remplace la fonctionnalité WebYast existante.

Pour mettre à niveau le système d'exploitation et configurer l'applicatif :

1 Mettez à niveau Sentinel. Pour plus d'informations, reportez-vous à la « Mise à niveau de Sentinel » page 161.

2 Arrêtez les services Sentinel :

```
rcsentinel stop
```

3 (Conditionnel) Si Sentinel était en mode FIPS avant la mise à niveau du système d'exploitation, les fichiers de base de données NSS doivent être mis à niveau manuellement par la commande suivante :

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Suivez les instructions affichées pour mettre à niveau la base de données NSS.

Octroyez toutes les autorisations à l'utilisateur `novell` sur les fichiers suivants :

```
cert9.db
key4.db
pkcs11.txt
```

4 (Conditionnel) Si vous utilisez Mozilla Network Security Services (NSS) 3.29, deux fichiers RPM dépendants `libfreebl3-hmac` et `libsoftokn3-hmac` ne sont pas installés. Installez manuellement les fichiers RPM suivants : `libfreebl3-hmac` et `libsoftokn3-hmac`.

5 Téléchargez le programme d'installation de SLES 12 SP3 ainsi que l'utilitaire de post-mise à niveau à partir du site Web Micro Focus Patch Finder. Pour Sentinel HA, téléchargez également le fichier SLES 12 SP3 HA.

6 Suivez les instructions d'installation pour mettre à niveau le système d'exploitation. Pour Sentinel HA, lorsque vous êtes invité à installer d'autres produits complémentaires, sélectionnez l'emplacement dans lequel vous avez téléchargé le fichier SLES 12 SP3 HA et effectuez la mise à niveau.

   Pour plus d'informations sur la mise à niveau vers SLES 12 SP3, reportez-vous à la documentation SLES.

7 Au cours du processus de mise à niveau, SLES renomme le fichier `/etc/sysctl.conf` en `/etc/sysctl.conf.rpmsave` en tant que sauvegarde et crée un fichier `/etc/sysctl.conf`. Une fois la mise à niveau effectuée, copiez le contenu du fichier `/etc/sysctl.conf.rpmsave` dans le fichier `/etc/sysctl.conf`. Ouvrez le fichier `sysctl.conf` et recherchez `# Added by sentinel vm.max_map_count`. Déplacez ce paramètre vers la ligne suivante comme suit :

   remplacez

   ```
   net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count : 65530
   vm.max_map_count = 262144
   ```

   par

   ```
   net.core.wmem_max = 67108864
   # Added by sentinel vm.max_map_count : 65530
   vm.max_map_count = 262144
   ```

8 (Conditionnel) Pour Sentinel HA, suivez la procédure mentionnée dans les sections suivantes :

   - « Configuration des cibles iSCSI » page 218
   - « Configuration des initiateurs iSCSI » page 219
   - « Configuration de la grappe HA » page 220

9 Pour configurer l'applicatif, exécutez l'utilitaire post-mise à niveau à partir de l'invite de commande :

   9a Décompressez le fichier :

   `tar -xvf <nom du fichier du programme d'installation de l'utilitaire post-mise à niveau>.tar.gz`

   9b Accédez au répertoire dans lequel vous avez extrait l'utilitaire :

   `cd <nom du fichier du programme d'installation de l'utilitaire post-mise à niveau>`

   9c Pour configurer l'applicatif, exécutez le script suivant :

   `./appliance_SLESISO_post_upgrade.sh`

   REMARQUE : n'exécutez pas ce script à distance, car il implique la reconfiguration du réseau.

   9d Suivez les instructions affichées à l'écran pour terminer la configuration.

   Ce script reconfigure les paquetages installés et configure des paquetages pour la gestion de l'applicatif.

10 Utilisez votre code d'enregistrement existant, enregistrez-vous à nouveau pour recevoir les mises à jour de Sentinel et les dernières mises à jour du système d'exploitation. Pour plus d'informations, reportez-vous à la section « Enregistrement pour obtenir les mises à jour » page 108.

30 Configurations après mise à niveau

Ce chapitre inclut les configurations ultérieures à la mise à niveau.

Sécurisation des données dans Elasticsearch

Sentinel utilise Kibana, un tableau de bord d'analyse et de recherche basé sur le navigateur, qui vous aide à visualiser les événements et les alertes dans des tableaux de bord. Sentinel stocke et indexe les alertes dans Elasticsearch. Vous pouvez configurer Sentinel pour également stocker et indexer les événements dans Elasticsearch afin de tirer parti des fonctions de visualisation d'événements. Les tableaux de bord Sentinel accèdent aux données à partir d'Elasticsearch pour présenter des événements et des alertes dans des tableaux de bord. Pour vous assurer que les tableaux de bord affichent uniquement les données que le rôle d'un utilisateur est autorisé à afficher et pour empêcher tout accès non autorisé aux données dans Elasticsearch, vous devez installer le plug-in de sécurité Elasticsearch. Pour plus d'informations, reportez-vous à la section « Sécurisation des données dans Elasticsearch » page 81.

Configuration de visualisations d'événements

Sentinel fournit des visualisations d'événements qui présentent les données dans des graphiques, des tableaux et des assignations. Ces visualisations facilitent la visualisation et l'analyse de gros volumes de données tels que les événements, les événements de flux IP et les alertes. Vous pouvez également créer vos propres visualisations et tableaux de bord.

Sentinel tire parti de Kibana, un tableau de bord d'analyse et de recherche basé sur un navigateur, qui vous aide à rechercher et à analyser des événements. Kibana accède aux données de la zone de stockage des données de visualisation (Elasticsearch) pour présenter les événements dans des tableaux de bord. Par défaut, Sentinel comprend un nœud Elasticsearch. Vous devez activer la visualisation des événements pour stocker et indexer les événements dans Elasticsearch. Pour plus d'informations, reportez-vous à la section « Configuration de la zone de stockage de visualisation » page 45.

REMARQUE : Certains des tableaux de bord Sentinel qui tirent parti de Kibana ne se chargent pas après la mise à niveau vers Sentinel 8.2. Ce problème se produit parce que les versions d'Elasticsearch et de Kibana ont été mises à niveau dans Sentinel 8.2 et le fichier d'index Kibana existant n'est pas compatible avec les versions actualisées d'Elasticsearch et de Kibana. Pour résoudre ce problème, vous devez supprimer manuellement le fichier d'index Kibana existant et recréer un nouveau fichier d'index Kibana. Pour plus d'informations, reportez-vous à l'article de la base de connaissances 7022736.

Configuration de la collecte de données de flux IP

Sentinel tire désormais parti des instances ArcSight SmartConnector qui vous permettent de contrôler votre réseau d'entreprise en collectant les données de flux IP en plus des données NetFlow. Les instances SmartConnector collectent les données de flux IP en tant qu'événements, qui permettent d'effectuer les opérations suivantes :

- Utiliser des instances Collector Manager existantes pour collecter les données de flux IP. Vous n'avez plus besoin d'instances Collector Manager NetFlow pour collecter les données NetFlow.
- Exploiter les données de flux IP dans plusieurs domaines de Sentinel, tels que les visualisations, le routage d'événement, les fédération de données, les rapports et la corrélation.
- Appliquer les stratégies de conservation des données aux données de flux IP, ce qui vous permet d'enregistrer ces données pour la durée souhaitée.

Une fois que vous avez mis à niveau Sentinel, vous pouvez continuer à utiliser les fonctions de NetFlow ou choisir de configurer la collecte des données de flux IP. Toutefois, avec la disponibilité de la capacité de collecte et de visualisation des données de flux IP, les capacités NetFlow précédemment disponibles, y compris les vues NetFlow, sont désormais obsolètes et seront supprimées à l'avenir pour une expérience utilisateur optimale.

Une fois que vous activez la collecte de données de flux IP :

- Les données de flux IP seront collectées en tant qu'événements et par conséquent prises en considération pour le nombre d'événements par seconde.
- Vous perdrez toutes les données NetFlow collectées avant l'activation du flux IP. Le système NetFlow obsolète présentait une période maximale de conservation de 3 jours. Vous pouvez conserver les événements de flux IP aussi longtemps que nécessaire.
- Vous ne pouvez pas migrer les données NetFlow collectées avant l'activation du flux IP vers la capacité de flux IP.
- Vous ne pouvez pas rétablir la configuration, sauf si vous installez de nouveau Sentinel.
- Vous serez déconnecté de Sentinel Main et il vous faudra vous vous reconnecter.

Pour configurer la collecte des données de flux IP :

1. Installez et configurez ArcSight SmartConnector. Lors de la configuration, veillez à configurer les instances SmartConnector pertinentes qui collectent les données de flux IP.

   Pour plus d'informations sur la configuration d'instances SmartConnector, consultez la documentation du collecteur CEF universel générique sur le site Web des plug-ins Sentinel.
2. Dans **Sentinel Main** > **Collecte** > **Flux IP**, sélectionnez **Collecter les données de flux IP**, puis cliquez sur **Activer**.

REMARQUE : Étant donné que les événements de flux IP sont à présent envoyés à Collector Manager, vous n'avez plus besoin d'utiliser des instances Collector Manager NetFlow. Par conséquent, vous pouvez désinstaller les instances Collector Manager NetFlow existantes. Pour plus d'informations, reportez-vous à la section « Désinstallation de NetFlow Collector Manager » page 234.

Configuration du gestionnaire de données évolutif de Sentinel après la mise à niveau

Installer le plug-in de sécurité Elasticsearch

En plus des nœuds Elasticsearch externes, Sentinel inclut désormais un nœud Elasticsearch local par défaut pour la visualisation des données. Par conséquent, vous devez installer un plug-in Elasticsearch pour l'instance Elasticsearch locale. Pour plus d'informations, reportez-vous à la section « Installation du plug-in de sécurité Elasticsearch » page 82.

Comme les instances Elasticsearch et Kibana utilisées dans Sentinel sont mises à niveau, vous devez redéployer tous les plug-ins de sécurité Elasticsearch dans les nœuds Elasticsearch existants. Pour plus d'informations sur le redéploiement du plug-in de sécurité Elasticsearch, reportez-vous à la section « Redéploiement du plug-in de sécurité Elasticsearch » page 86.

Mise à jour des applications Spark sur YARN

Pendant la mise à niveau de Sentinel, certains fichiers d'application Spark subissent aussi une mise à jour. Vous devez suivre la procédure ci-dessous pour revalider les applications Spark avec ces fichiers mis à jour :

1. Connectez-vous au serveur SSDM en tant qu'utilisateur `novell` et copiez les fichiers sur le serveur d'historique Spark où est installé HDFS NameNode :

   ```
   cd /etc/opt/novell/sentinel/scalablestore
   ```

   ```
   scp SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties
   log4j.properties manage_spark_jobs.sh
   root@<noeuf_hdfs>:<répertoire_de_destination>
   ```

   où *<répertoire_de_destination>* est le répertoire dans lequel vous voulez placer les copies des fichiers. Assurez-vous aussi que l'utilisateur `hdfs` dispose de toutes les autorisations pour ce répertoire.

2. Connectez-vous au serveur *<noeud_hdfs>* en tant qu'utilisateur root et modifiez le propriétaire des fichiers copiés en utilisateur `hdfs` :

   ```
   cd <répertoire_de_destination>
   ```

   ```
   chown hdfs SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties
   log4j.properties manage_spark_jobs.sh
   ```

   Assignez l'autorisation d'exécution au script `manage_spark_jobs.sh`.

3. Assurez-vous que les tâches Spark ont terminé le traitement de toutes les données:

Accédez à l'interface utilisateur Web ResourceManager de YARN et affichez chaque application Sentinel Spark. Les données d'application de lecture en continu Spark afficheront une chute de la fréquence d'entrée jusqu'à zéro lorsque toutes les données auront été traitées à partir de Kafka.

4 Exécutez la commande suivante pour arrêter le traitement des données :

```
./manage_spark_jobs.sh stop
```

5 Effacez le point de contrôle de traitement des données :

```
sudo -u hdfs hadoop fs -rm -R -skipTrash  /spark/checkpoint
```

où `/spark/checkpoint` est le répertoire du point de contrôle.

6 Exécutez le script suivant pour renvoyer les tâches Spark :

```
./manage_spark_jobs.sh start
```

La soumission par les commandes ci-dessus dure un certain temps.

7 (Facultatif) Exécutez la commande suivante pour vérifier l'état des tâches Spark envoyées :

```
./manage_spark_jobs.sh status
```

8 Relancez l'acheminement de Kafka à Spark pour commencer à traiter les événements :

8a Dans l'interface principale de Sentinel, cliquez sur **Stockage** > **Stockage évolutif** > **Configuration avancée** > **Kafka** .

8b Définissez la propriété suivante sur fausse :

```
pause.events.tokafka
```

8c Cliquez sur **Enregistrer**.

Activation des fonctions de Sentinel

Quand vous effectuez une mise à niveau depuis SSDM 8.0.*x.x*, certaines fonctions apparues dans Sentinel 8.1 ou une version ultérieure ne sont pas disponibles par défaut. Vous devez les activer manuellement dans le fichier `/etc/opt/novell/sentinel/config/ui-configuration.properties`.

1 Connectez-vous au serveur Sentinel en tant qu'utilisateur `novell`.

2 Ouvrez le fichier `/etc/opt/novell/sentinel/config/ui-configuration.properties`.

3 Modifiez les propriétés suivantes sur fausses :

```
alerts.hideUI
solutionDesigner.launcher.hideUI
correlation.hideUI
scc.configurations.solutionPacks.hideUI
people.hideUI
permission.knowledgeBase.hideUI
scc.menuBarItem.toolsMenu.hideUI
scc.toolBarItem.peopleBrowser.hideUI
integration.hideUI
```

4 Rafraîchissez le navigateur Sentinel.

Mise à jour des tableaux de bord et des visualisations dans SSDM

Vous devez mettre à jour les tableaux de bord et les visualisations après la mise à niveau de SSDM, afin que les améliorations incluses dans la version la plus récente puissent leur être appliquées.

Lorsque vous mettez à niveau SSDM, par défaut, les tableaux de bord et les visualisations ne sont pas mis à jour. Toutefois, vous pouvez les mettre à jour manuellement après la mise à niveau. Vous pouvez mettre à jour les tableaux de bord et les visualisations en supprimant ceux qui existent, puis en exécutant le script `load_kibana_data.sh`, qui installe les visualisations et les tableaux de bord les plus récents.

IMPORTANT : si vous effectuez cette mise à jour, les personnalisations apportées aux tableaux de bord et aux visualisations seront perdues.

Pour mettre à jour les tableaux de bord et les visualisations, procédez comme suit :

1. Connectez-vous à l'interface Web SSDM et accédez à la visualisation des événements.
2. À partir de la visualisation des événements, accédez à **Paramètres** > **Objets** > **Tableaux de bord**.
3. Sélectionnez les tableaux de bord à mettre à jour, puis cliquez sur **Supprimer**.
4. Cliquez sur **Visualisations**. Sélectionnez les visualisations à mettre à jour, puis cliquez sur **Supprimer**.
5. Déconnectez-vous de l'interface Web SSDM.
6. Connectez-vous au serveur SSDM en tant qu'utilisateur `novell`.
7. Accédez au répertoire `/opt/novell/sentinel/bin`.
8. Exécutez le script `load_kibana_data.sh` à l'aide de la commande suivante :

   ```
   ./load_kibana_data.sh http://<adresse_ip>:<port>> <alerts/events/misc>
   ```

   Par exemple :

   ```
   ./load_kibana_data.sh http://127.0.0.1:9200 alerts
   ./load_kibana_data.sh http://127.0.0.1:9200 events
   ```
9. Connectez-vous à l'interface Web SSDM et accédez à la visualisation des événements pour afficher les visualisations et les tableaux de bord mis à jour.

Ajout du pilote JDBC DB2

Après avoir mis à niveau Sentinel, ajoutez le pilote JDBC adéquat et configurez-le pour la collecte et la synchronisation de données en effectuant les étapes suivantes :

1. Copiez la version du pilote IBM DB2 JDBC (`db2jcc-*.jar`) qui convient à votre version de la base de données DB2 dans le dossier `/opt/novell/sentinel/lib`.
2. Assurez-vous que vous avez bien défini la propriété et les autorisations nécessaires pour le fichier du pilote.
3. Configurez ce pilote pour la collecte des données. Pour plus d'informations, reportez-vous à la documentation du connecteur de base de données.

Configuration des propriétés de fédération de données dans l'applicatif Sentinel

Suivez la procédure ci-dessous après la mise à niveau de l'applicatif Sentinel, de sorte que la fédération de données n'affiche pas d'erreur dans l'environnement dans lequel deux cartes réseau ou plus sont configurées :

1. Sur le serveur d'un demandeur autorisé, ajoutez la propriété suivante au fichier `/etc/opt/novell/sentinel/config/configuration.properties` :

   ```
   sentinel.distsearch.console.ip=<l'une des adresses IP du demandeur autorisé>
   ```

2. Sur le serveur de sources de données, ajoutez la propriété suivante au fichier `/etc/opt/novell/sentinel/config/configuration.properties` :

   ```
   sentinel.distsearch.target.ip=<l'une des adresses IP de la source de données>
   ```

3. Redémarrez Sentinel :

   ```
   rcsentinel restart
   ```

4. Connectez-vous au serveur du demandeur autorisé et cliquez sur Intégration. Si la source de données que vous souhaitez ajouter est déjà présente, supprimez-la et rajoutez-la en spécifiant l'une des adresses IP que vous avez ajoutées à l'étape 2.

   De même, ajoutez les demandeurs autorisés en spécifiant les adresses IP que vous avez ajoutées à l'étape 1.

Enregistrement de l'applicatif Sentinel pour les mises à jour

Si vous avez mis à niveau le système d'exploitation, vous devez réenregistrer l'applicatif Sentinel pour recevoir les dernières mises à jour du système d'exploitation et de Sentinel. Pour ce faire, vous pouvez utiliser votre clé d'enregistrement existante. Pour enregistrer l'applicatif, reportez-vous à la section « Enregistrement pour obtenir les mises à jour » page 108.

Mise à jour des bases de données externes pour la synchronisation des données

À partir de Sentinel 8.x, la taille du champ d'événement `Message (msg)` est passée de 4 000 à 8 000 caractères pour accueillir davantage d'informations.

Si vous avez créé une stratégie de synchronisation des données dans les versions précédentes de Sentinel qui synchronise un champ d'événement Message (msg) avec une base de données externe, vous devez augmenter en conséquence la taille de la colonne assignée appropriée dans la base de données externe.

REMARQUE : L'étape précédente s'applique uniquement si vous mettez à niveau une version précédente de Sentinel vers une version 8.x.

Réauthentification de Sentinel en mode d'authentification multi-critères (AMC)

Lorsque vous mettez à niveau le serveur Sentinel en mode AMC, les instances NetFlow Collector Manager existantes ne se réauthentifient pas automatiquement sur le serveur Sentinel. Vous devez effectuer les étapes suivantes pour réauthentifier manuellement les instances NetFlow Collector Manager sur le serveur Sentinel.

Pour recommencer l'authentification de Sentinel en mode AMC :

1. Connectez-vous à l'ordinateur sur lequel NetFlow Collector Manager est installé.
2. Accédez à `/opt/novell/sentinel/setup`.
3. Exécutez le script `configure.sh`.

   Vous êtes invité à vous connecter au serveur Sentinel.
4. Indiquez votre nom d'utilisateur et votre mot de passe LDAP.
5. Fournissez l'ID et le secret du client Sentinel.

   Pour récupérer l'ID client Sentinel et le secret client Sentinel, accédez à l'URL suivante :

   `https://Sentinel_FQDN:port/SentinelAuthServices/oauth/clients`

   Où :

   - `Sentinel_FQDN` est le nom de domaine complet du serveur Sentinel.

     Par exemple, `abc.netiq.com`

     où `abc` est le nom d'hôte du serveur Sentinel, `netiq.com` est le nom du domaine.
   - `Port` est le port qu'utilise Sentinel (généralement 8443).

   L'URL indiquée se base sur votre session Sentinel actuelle pour récupérer l'ID client Sentinel et le secret client Sentinel.

31 Mise à niveau des plug-ins Sentinel

Lors des mises à niveau de Sentinel, les plug-ins ne sont mis à niveau que si l'un d'eux n'est pas compatible avec la dernière version de Sentinel.

Qu'ils soient nouveaux ou mis à jour, les plug-ins de Sentinel, y compris les Solution Packs, sont fréquemment téléchargés sur le site Web des plug-ins Sentinel. Pour obtenir les derniers correctifs de bogue, les mises à jour de la documentation et les améliorations de plug-in, téléchargez et installez la dernière version du plug-in. Pour obtenir des informations sur l'installation d'un plug-in, reportez-vous à la documentation relative à ce plug-in.

VI Migration de données à partir du stockage traditionnel

La migration des données depuis Sentinel avec stockage traditionnel vous permet de valoriser vos données Sentinel existantes et le temps que vous y avez investi. Pour migrer les données depuis Sentinel avec stockage traditionnel, la version de Sentinel des deux serveurs, source et cible, doit être la même. Par exemple, pour migrer des données d'un serveur Sentinel 8.1 (source) vers un serveur Sentinel 8.2 (cible), vous devez d'abord mettre à niveau Sentinel 8.1 vers Sentinel 8.2, puis lancer la migration des données.

Cette section fournit des informations sur la migration des données existantes vers le composant de stockage des données de votre choix.

32 Migration de données vers un stockage évolutif

Vous pouvez avoir un ou plusieurs serveurs Sentinel avec stockage traditionnel. Le processus de migration de données à suivre dépend de la façon dont vous voulez paramétrer et maintenir votre déploiement Sentinel.

Tableau 32-1 *Processus de migration des données de votre déploiement Sentinel*

Déploiement Sentinel	Processus de migration
Vous n'avez qu'un serveur Sentinel et vous prévoyez de le mettre à niveau vers un stockage évolutif.	Migrez les données d'événements et les données brutes du stockage traditionnel vers le stockage évolutif après la mise à niveau de votre serveur Sentinel et l'activation du stockage évolutif. Pour plus d'informations, reportez-vous à la section Chapitre 34, « Migration des données », page 187.
Vous avez un seul serveur Sentinel avec stockage traditionnel et vous voulez installer un autre serveur Sentinel pour le stockage évolutif afin d'avoir toutes les fonctions de Sentinel à disposition.	Utilisez l'utilitaire de sauvegarde et de restauration pour migrer les données du serveur Sentinel avec stockage traditionnel vers le serveur au stockage évolutif. Pour plus d'informations sur l'utilitaire de sauvegarde et de restauration, reportez-vous à la section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Déploiement Sentinel	Processus de migration
Dans votre installation multiniveau à plusieurs serveurs Sentinel, vous prévoyez d'ajouter un nouveau serveur Sentinel ou d'utiliser un des serveurs existants pour du stockage évolutif : vous devez migrer les données de configuration en plus des données d'événements et des données brutes.	Dans un environnement multiniveau, vous pouvez identifier le serveur Sentinel traditionnel qui stocke la plupart de vos données, puis migrer les données avec l'utilitaire de sauvegarde et de restauration. Pour sauvegarder des données en provenance de vos autres serveurs Sentinel, vous devez suivre une autre approche de migration des données de configuration, des données d'événements et des données brutes de ces serveurs, décrite ultérieurement dans cette section. Vous devez aussi recréer manuellement une partie des configurations. Vous ne pouvez pas utiliser l'utilitaire de sauvegarde et de restauration pour migrer vos données depuis plusieurs serveurs puisqu'il écrase les données existantes lors de la restauration. Par exemple, si vous avez déjà restauré des données du Serveur A et que vous restaurez ensuite des données du Serveur B, l'utilitaire va écraser les données restaurées depuis le Serveur A. Par conséquent, pour comprendre le processus de migration des données, suivez les instructions fournies dans les sections ci-dessous dans l'ordre indiqué : ◆ Données migrables ◆ Migration des données de configuration ◆ Migration des données ◆ Migration des alertes et des données NetFlow ◆ Mise à jour des clients Sentinel ◆ Importation de la configuration ESM

Données migrables

Vous pouvez migrer les données d'événements, les données brutes et une partie des données de configuration. Le reste de la configuration, impossible à migrer, doit être recréé manuellement.

Tableau 32-2 Configurations migrables et configurations à recréer

Configurations migrables	Configurations à recréer
◆ Règles de corrélation ◆ Opérations ◆ Assignations ◆ Filtres ◆ Sources de diffusion de news de menaces ◆ Configuration ESM ◆ Alertes sauf pour les données de la base de connaissances ◆ NetFlow	◆ Locataires, rôles, utilisateurs et configuration LDAP ◆ Règles de routage des événements et des alertes ◆ Stratégies de conservation des données et des alertes ◆ Tableaux de bord ◆ Vues en temps réel ◆ Informations d'identité ◆ Configuration des sources de diffusion de news ◆ Configuration des plug-ins d'intégrateur et d'opérations ◆ Configuration de sécurité

Migration des données de configuration

Avant de migrer des données d'événements, vous devez migrer les données de configuration vers le serveur Sentinel cible. Vous pouvez sauvegarder une partie de la configuration avec Solution Designer et les options d'exportation et d'importation ESM (Event Source Management). Le reste de la configuration, impossible à sauvegarder ou exporter, doit être recréé manuellement.

- « Backing Up Data on the Source Server (Sauvegarde des données sur le serveur source) » page 181
- « Restauration des données sur le serveur cible » page 182

Backing Up Data on the Source Server (Sauvegarde des données sur le serveur source)

Vous devez sauvegarder les données nécessaires à l'aide des différentes options de Sentinel.

- « Using Solution Packs (Utilisation des packs de solutions) » page 181
- « Utilisation de l'option de configuration des exportations dans l'interface ESM » page 182

Using Solution Packs (Utilisation des packs de solutions)

Sauvegardez la configuration suivante sur le serveur source à l'aide de Solution Designer :

Tableau 32-3 Données de configuration

	Data	Remarques
❒	Règles de corrélation	Créez des contrôles distincts pour chaque moteur de corrélation Correlation Engine afin de migrer séparément les règles de chaque moteur.
❒	Opérations	Vous pouvez uniquement sauvegarder les opérations JavaScript et non les options héritées comme les listes dynamiques et la création d'incident.

	Data	Remarques
❒	Enrichissement des événements	Sentinel sauvegarde aussi les cartes annexées aux champs d'événements. Il est donc inutile de recréer les cartes annexées après la restauration de données d'enrichissement des événements.
❒	Filtres	Sauvegarde tous les filtres personnalisés
❒	Sources de diffusion de news	Solution Pack sauvegarde uniquement les plug-ins des sources de diffusion de news, sans la configuration des plug-ins.

Pour plus d'informations sur la sauvegarde des données dans Solution Designer, reportez-vous à la section « Creating Solution Packs » (Création des Solution Packs) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Utilisation de l'option de configuration des exportations dans l'interface ESM

Sauvegardez la configuration de votre collecte de données à l'aide de l'option d'exportation de la configuration ESM. Pour plus d'informations, reportez-vous à la section « Exporting Configurations » (Exportation des configurations) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Restauration des données sur le serveur cible

- « Installation des données de configuration depuis un Solution Pack » page 182
- « Recréation manuelle de la configuration » page 182

Installation des données de configuration depuis un Solution Pack

Avec Solution Designer, importez les données de configuration sauvegardées sur le serveur source. Pour plus d'informations, reportez-vous à la section « Installing Content from Solution Packs » (Installation de contenu avec des Solution Packs) du manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

Renommez les éventuels doublons d'objets notamment de Filtres, d'Opérations et de Règles de corrélation. Par défaut, tous les filtres sont publics après importation sur le serveur cible. Ré-assignez manuellement l'autorisation pour chaque filtre.

Recréation manuelle de la configuration

À l'exception des données de configuration importées depuis Solution Pack, vous devez recréer manuellement toutes les autres configurations. Pour plus d'informations sur les configurations à recréer manuellement, reportez-vous à Tableau 32-2, « Configurations migrables et configurations à recréer », page 181.

Migration des données d'événements et des données brutes

Pour migrer des données d'événement et les données brutes, reportez-vous à la section Migration des données.

Migration des alertes et des données NetFlow

Vous pouvez utiliser l'utilitaire de sauvegarde et de restauration pour migrer les alertes et les données NetFlow du serveur source vers le serveur cible. Pour les alertes, l'utilitaire restaure les événements déclencheurs de l'alerte. Toutefois, il ne restaure pas la règle de corrélation associée ni les informations de la base de connaissances.

Utilisez les commandes suivantes pour sauvegarder et restaurer les alertes et les données NetFlow :

```
For backing up:
./backup_util.sh -i

For restore:
./backup_util.sh -m restore -f <backup_file_path>
```

Pour les alertes et les données NetFlow, vous disposez de l'option de remplacer les données existantes ou d'ajouter à celles-ci d'autres données. Choisissez l'option voulue.

Même si la commande ci-dessus sauvegarde et restaure les données Security Intelligence, vous ne pouvez pas les utiliser car Security Intelligence n'est pas disponible dans SSDM.

Pour plus d'informations sur l'utilitaire de sauvegarde et de restauration, reportez-vous à la section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Mise à jour des clients Sentinel

Vous devez mettre à jour toute configuration de vos gestionnaires de collecteurs Collector Manager, de vos moteurs de corrélation Correlation Engine et de vos gestionnaires NetFlow Collector Manager afin qu'ils commencent à communiquer avec le serveur cible. Pour plus d'informations, reportez-vous à la section « Updating Sentinel Clients » (Mise à jour des clients Sentinel) du manuel *Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

REMARQUE : Il est vrai que vous avez déjà migré des données d'événements depuis le serveur source, mais vous devez malgré tout réexécuter le script de migration des données pour transférer toute donnée d'événement qui serait arrivée pendant ou après le processus de migration des données. Pour plus d'informations, reportez-vous à la section Chapitre 34, « Migration des données », page 187.

Importation de la configuration ESM

Importez la configuration de collecte des données utilisée sur le serveur source avec l'option de configuration d'importation de l'interface utilisateur ESM. Pour plus d'informations, reportez-vous à la section « Importing Configurations » (Importation des configurations) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

33 Migration de données vers Elasticsearch

Sentinel stocke les données dans un stockage traditionnel basé sur des fichiers et indexe les données localement sur le serveur Sentinel par défaut. Lorsque vous activez la visualisation des événements, Sentinel stocke et indexe les données dans Elasticsearch en plus du stockage traditionnel basé sur les fichiers. Les tableaux de bord affichent uniquement les événements traités une fois que vous avez activé la visualisation des événements. Pour afficher les événements figurant dans le stockage basé sur les fichiers, vous devez migrer les données à partir du stockage basé sur les fichiers vers Elasticsearch. Pour migrer des données vers Elasticsearch, reportez-vous à la section Chapitre 34, « Migration des données », page 187.

34 Migration des données

Vous pouvez utiliser le script `data_uploader.sh` pour migrer des données vers l'un des composants de stockage de données suivants :

- **Kafka :** Vous pouvez migrer à la fois des données d'événements et des données brutes vers Kafka. Exécutez le script pour les données d'événements, puis les données brutes. Le script migre les données dans les rubriques Kafka.

  Vous pouvez préciser des personnalisations comme la compression des données lors de la migration, la transmission des données par lot, etc. Pour ce faire, vous devez créer un fichier de propriétés et y ajouter les propriétés requises au format clé-valeur. Par exemple :

  ```
  compression.type=lz4
  ```

  ```
  batch.size=20000
  ```

  Pour plus d'informations sur les propriétés Kafka, reportez-vous à la Documentation de Kafka. Configurez les propriétés et leurs valeurs avec prudence car le script ne les valide pas.

  REMARQUE : Assurez-vous que le serveur Sentinel est en mesure de résoudre tous les noms d'hôtes de courtier Kafka sur des adresses IP correctes pour l'ensemble de la grappe Kafka. Si DNS n'est pas configuré pour permettre cela, ajoutez les noms d'hôte du courtier Kafka au fichier `/etc/hosts` du serveur Sentinel.

- **Elasticsearch :** Vous pouvez migrer uniquement des données d'événement vers Elasticsearch. Avant de migrer les données, assurez-vous que vous avez activé la visualisation des événements. Pour plus d'informations, reportez-vous à la section « Activation de la visualisation des événements » page 127.

Il les transfère pour la plage de dates (du, au) que vous précisez. Lorsque vous exécutez le script, il affiche les paramètres obligatoires et facultatifs que vous devez spécifier pour lancer la migration des données et également des informations sur les propriétés pertinentes à utiliser pour le composant de stockage des données de votre choix.

Le script doit être exécuté en tant qu'utilisateur novell. Il faut donc vous assurer que les répertoires de données et tout fichier précisé disposent des autorisations appropriées pour l'utilisateur novell. Par défaut, le script migre les données depuis le stockage primaire. Pour les migrer depuis un stockage secondaire, entrez le chemin approprié vers ce stockage lors de l'exécution du script.

Pour migrer des données :

1. Connectez-vous au serveur Sentinel en tant qu'utilisateur novell.
2. Exécutez le script suivant :

   ```
   /opt/novell/sentinel/bin/data_uploader.sh
   ```

3. Suivez les instructions à l'écran et réexécutez le script avec les paramètres requis.

Les données migrées auront la période de conservation définie sur le serveur cible.

Après la migration des données, le script en enregistre l'état notamment les partitions téléchargées, les partitions dont la migration a échoué et le nombre d'événements. Pour les partitions dont la date correspond au jour précédent ou à la date courante, l'état du transfert de données affichera IN_PROGRESS (en cours) pour prendre en compte les événements susceptibles d'arriver tardivement.

Réexécutez le script si la migration des données a échoué ou si l'état de la migration des données des partitions continue d'afficher IN_PROGRESS. Lorsque vous réexécutez le script, celui-ci commence par vérifier le fichier d'état pour repérer les partitions déjà migrées, puis il reprend la migration des autres. Le script conserve les journaux dans le répertoire `/var/opt/novell/sentinel/log/data_uploader.log` à des fins de dépannage.

VII Déploiement de Sentinel pour une haute disponibilité

Cette section fournit des informations sur la procédure d'installation de Sentinel en mode actif-passif en haute disponibilité afin de permettre à Sentinel de basculer vers un noeud de grappe redondant en cas de panne matérielle ou logicielle. Pour plus d'informations sur la mise en œuvre de la haute disponibilité et de la reprise après sinistre dans votre environnement Sentinel, contactez le support technique de .

REMARQUE : la configuration en mode HA est prise en charge uniquement sur le serveur Sentinel. Cependant, les instances Collector Manager et Correlation Engine peuvent toujours communiquer avec le serveur Sentinel HA.

---

35 Concepts

La haute disponibilité fait référence à une méthodologie de conception visant à assurer la disponibilité d'un système tant qu'il est praticable. L'objectif est de réduire au maximum les causes d'interruption de services tels que les échecs système et les besoins de maintenance, mais également de détecter le plus rapidement possible les événements susceptibles d'interrompre les services et de restaurer le plus vite possible le système à la suite d'une interruption. Dans la pratique, les méthodes automatisées de détection et de récupération en cas d'interruptions de services deviennent vite nécessaires puisqu'il convient d'atteindre des niveaux de disponibilité plus élevés.

Pour plus d'informations sur la haute disponibilité, consultez le manuel SUSE High Availability Guide (Guide de SUSE High Availability).

Systèmes externes

Sentinel est une application complexe qui compte plusieurs niveaux interdépendants et fournit un large éventail de services. Elle intègre en outre plusieurs systèmes tiers externes pour la collecte et le partage de données ainsi que pour le traitement des incidents. La plupart des solutions haute disponibilité permettent à ceux qui les implémentent de déclarer des dépendances entre les services nécessitant une haute disponibilité, mais cela ne s'applique qu'aux services s'exécutant sur la grappe proprement dite. Des systèmes externes à Sentinel, tels que les sources d'événements, doivent être configurés séparément pour assurer la disponibilité requise par l'organisation et doivent également être configurés pour gérer correctement les périodes d'indisponibilité de Sentinel, comme en cas de basculement. Si les droits d'accès sont très restreints, par exemple, en cas de recours à des sessions authentifiées pour l'envoi et/ou la réception de données entre Sentinel et un système tiers, ce dernier doit être configuré pour accepter les sessions au départ et à destination de n'importe quel noeud de grappe (Sentinel doit être configuré avec une adresse IP virtuelle pour ce faire).

Stockage partagé

Toutes les grappes haute disponibilité nécessitent une certaine forme de stockage partagé pour pouvoir déplacer rapidement les données d'application d'un noeud de grappe à l'autre, en cas de défaillance du noeud d'origine. La haute disponibilité exigée pour le système de stockage proprement dit est généralement obtenue à l'aide de la technologie SAN (Storage Area Network) connectée aux noeuds de grappe à l'aide d'un réseau Fibre Channel. Cela dit, d'autres systèmes utilisent NAS (Network Attached Storage), iSCSI ou d'autres technologies qui autorisent le montage distant d'un système de stockage partagé. Le stockage partagé est surtout nécessaire pour qu'en cas de défaillance d'un noeud de cluster, le cluster puisse déplacer sans problème le système de stockage vers un nouveau noeud.

Sentinel peut utiliser deux approches de base pour le stockage partagé. La première place l'ensemble des composants présents (fichiers binaires de l'application, configuration et données d'événement) sur le système de stockage partagé. En cas de basculement, le système de stockage

est démonté du noeud primaire et déplacé vers le noeud de sauvegarde qui charge l'ensemble de l'application et de la configuration à partir de l'emplacement de stockage partagé. Dans la seconde approche, les données d'événement sont enregistrées sur le système de stockage partagé, mais les fichiers binaires et la configuration de l'application sont stockées sur chaque noeud de grappe. En cas de basculement, seules les données d'événement sont déplacées vers le noeud de sauvegarde.

Chaque approche a son lot d'avantages et d'inconvénients, mais la seconde approche permet à l'installation Sentinel d'utiliser des chemins d'installation compatibles FHS standard, de vérifier la création des paquetages RPM ainsi que d'installer des correctifs et de modifier la configuration à chaud de manière à réduire les temps d'interruption de service.

À l'aide d'un exemple, cette solution vous guide dans la procédure d'installation d'une grappe qui utilise le système de stockage partagé iSCSI et place les fichiers binaires/la configuration de l'application sur chaque noeud de grappe.

Surveillance des services

L'un des composants clés de tout environnement à haute disponibilité est de pouvoir disposer d'une méthode fiable et cohérente pour surveiller les ressources à haute disponibilité, ainsi que les ressources dont elles dépendent. Pour mener à bien cette surveillance, l'environnement à haute disponibilité SLE utilise un composant appelé Agent de ressource ayant pour mission de signaler l'état de chaque ressource et de démarrer ou d'arrêter cette dernière (à chaque demande).

Pour éviter les interruptions de service inutiles, l'état indiqué par les agents de ressource pour les ressources surveillées doit être fiable. Les faux-positifs (une ressource est censée avoir échoué, mais s'est rétablie de façon autonome) peuvent entraîner la migration des services (et les interruptions qui en découlent) alors que ce n'est pas nécessaire, tandis que les faux-négatifs (l'agent de ressource signale qu'une ressource fonctionne correctement alors que ce n'est pas le cas) peuvent empêcher le bon fonctionnement du service. D'un autre côté, la surveillance externe d'un service peut être compliquée. Par exemple, il se peut que le port d'un service Web réponde à une simple commande ping, mais qu'il ne fournisse pas la réponse appropriée lorsqu'une véritable demande est envoyée. Dans de nombreux cas, pour obtenir une mesure réellement précise, la fonctionnalité de test automatique doit être intégrée au service proprement dit.

Cette solution fournit à Sentinel un agent de ressource OCF de base pour lui permettre d'effectuer une surveillance des principaux échecs au niveau du système Sentinel, du matériel et du système d'exploitation. Actuellement, les fonctionnalités de surveillance externes de Sentinel sont basées sur des sondes de port IP, mais il existe un risque de faux-positifs et de faux-négatifs. Nous avons l'intention d'améliorer Sentinel et l'agent de ressource au fil du temps afin d'améliorer la fiabilité de ce composant.

Fencing (Isolement)

Au sein d'une grappe haute disponibilité, les services critiques sont surveillés en permanence et redémarrés automatiquement sur les autres noeuds en cas d'échec. Cette automatisation peut toutefois induire des erreurs en cas de problème de communication avec le noeud primaire : bien que le service exécuté sur ce noeud semble arrêté, il continue en réalité à s'exécuter et à inscrire des données dans l'espace de stockage partagé. Dans ce cas, le démarrage d'un nouvel ensemble de services sur un noeud de sauvegarde peut facilement entraîner l'altération des données.

Pour éviter cette situation, les clusters utilisent diverses techniques collectivement appelées Fencing (isolement), notamment SBD (Split Brain Detection) et STONITH (Shoot The Other Node In The Head). L'objectif premier est d'éviter l'altération des données sur le système de stockage partagé.

36 Configuration système requise

Lors de l'allocation de ressources de grappe pour la prise en charge d'une installation à haute disponibilité (HA), respectez les exigences suivantes :

- ❒ (Conditionnel) Pour les installations d'applicatif HA, assurez-vous que l'applicatif Sentinel HA avec licence valide est disponible. L'applicatif Sentinel HA est un applicatif ISO qui comprend les paquetages suivants :
  - Système d'exploitation : SLES 12 SP3
  - Paquet SLES HAE (SLES High Availability Extension)
  - Logiciel Sentinel (y compris RPM HA)
- ❒ (Conditionnel) Pour les installations HA traditionnelles, vérifiez que les éléments suivants sont disponibles :
  - Système d'exploitation : SLES 11 SP4 ou SLES 12 SP1 ou ultérieur
  - Image ISO SLES HAE avec des licences valides
  - Programme d'installation de Sentinel (fichier TAR)
- ❒ (Conditionnel) Si vous utilisez le système d'exploitation SLES avec le kernel version 3.0.101 ou une version ultérieure, vous devez charger manuellement le pilote de surveillance sur l'ordinateur. Pour identifier le pilote approprié à votre matériel, contactez le fabricant du matériel. Pour charger le pilote de surveillance, procédez comme suit :
  1. À l'invite de commande, exécutez la commande suivante pour charger le pilote de surveillance dans la session en cours :

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. Dans le fichier `/etc/init.d/boot.local`, ajoutez la ligne suivante pour vous assurer que l'ordinateur charge automatiquement le pilote de surveillance à chaque démarrage :

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```
- ❒ Assurez-vous que chaque noeud de grappe qui héberge les services Sentinel respecte la configuration requise spécifiée au Chapitre 5, « Configuration du système », page 39.
- ❒ Veillez à disposer d'un espace de stockage suffisant pour accueillir l'application et les données Sentinel.
- ❒ Veillez à utiliser une adresse IP virtuelle pour les services pouvant être migrés d'un noeud à l'autre en cas de basculement.
- ❒ Assurez-vous que votre périphérique de stockage partagé répond aux exigences, en termes de taille et de performances, spécifiées au Chapitre 5, « Configuration du système », page 39. Utilisez une machine virtuelle SLES standard configurée avec des cibles iSCSI comme espace de stockage partagé.

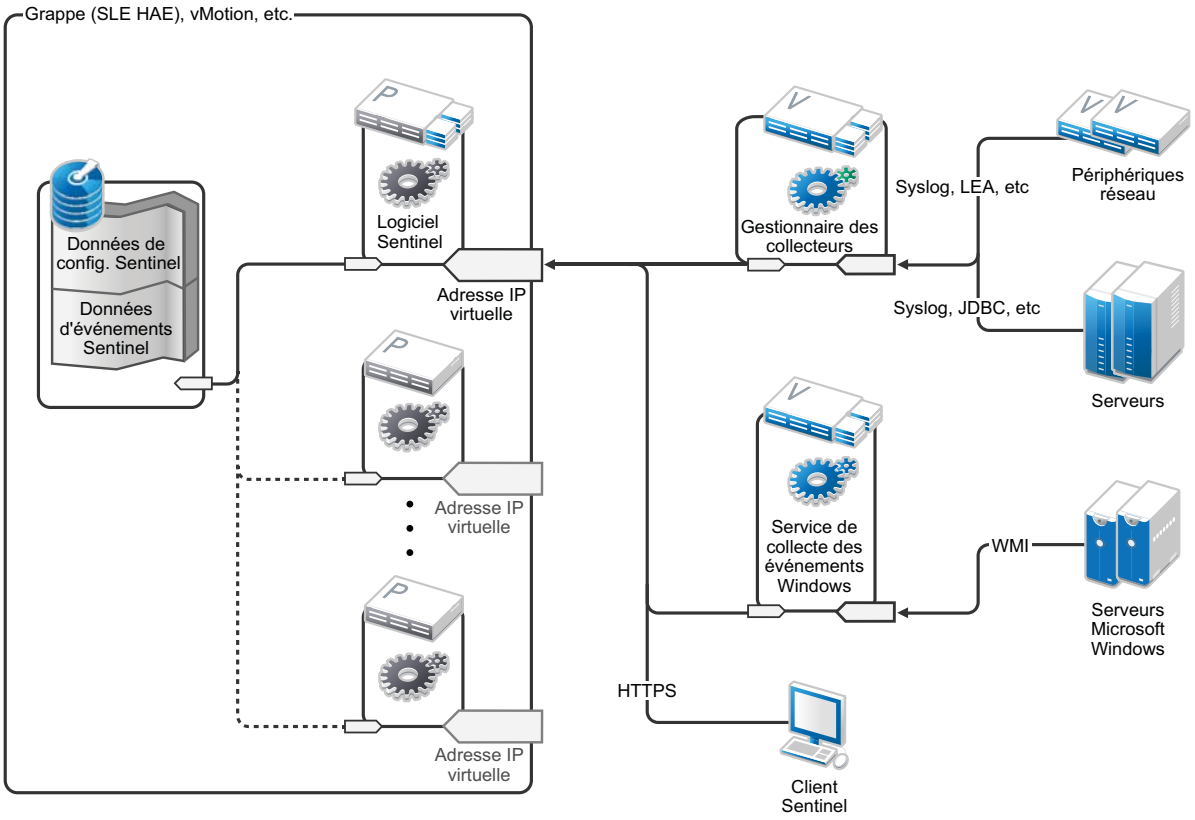
  Pour iSCSI, vous devez utiliser la plus grande unité de transfert des messages (Message Transfer Unit - MTU) prise en charge par votre matériel. Les plus grandes MTU contribuent à un stockage performant. Sentinel risque de rencontrer des problèmes si la latence et la bande passante vers le stockage sont inférieures à celles recommandées.

- ❒ Veillez à disposer, au minimum, de deux noeuds de grappe disposant des ressources nécessaires pour exécuter Sentinel dans l'environnement du client. Il est recommandé d'avoir deux machines virtuelles SLES.
- ❒ Veillez à créer une méthode pour que les noeuds de grappe puissent communiquer avec l'espace de stockage partagé (Fibre Channel pour un SAN, par exemple). Utilisez une adresse IP dédiée pour vous connecter à la cible iSCSI.
- ❒ Veillez à disposer d'une adresse IP virtuelle pouvant être migrée d'un noeud de grappe vers un autre pour faire office d'adresse IP externe pour Sentinel.
- ❒ Veillez à disposer d'au moins une adresse IP par noeud de grappe pour les communications internes à la grappe. Vous pouvez utiliser une adresse IP de monodiffusion. Cependant, l'utilisation d'une adresse de multidiffusion est recommandée pour les environnements de production.

37 Installation et configuration

Ce chapitre fournit les procédures d'installation et de configuration de Sentinel dans un environnement à haute disponibilité (HA).

Le schéma suivant illustre une architecture HA active-passive :



- « Configuration initiale » page 196
- « Configuration de l'espace de stockage partagé » page 197
- « Installation de Sentinel » page 202
- « Installation de clusters » page 205
- « Configuration du cluster » page 205
- « Configuration des ressources » page 209
- « Configuration du stockage secondaire » page 210

Configuration initiale

Configurez le matériel de l'ordinateur, du réseau et de l'espace de stockage, ainsi que les systèmes d'exploitation, les comptes utilisateur et les autres ressources système de base conformément aux instructions du document relatif à la configuration requise pour Sentinel et le client local. Testez les systèmes afin de vérifier leur bon fonctionnement et leur stabilité.

Utilisez la liste de contrôle suivante pour procéder à l'installation et la configuration initiales.

	Éléments de la liste de contrôle
?	Les caractéristiques de l'espace disque, de l'UC et de la mémoire virtuelle de chaque noeud de la grappe doit respecter la configuration système requise définie au Chapitre 5, « Configuration du système », page 39 sur la base du taux d'événements attendu.
?	Les caractéristiques de l'espace disque et des E/S des noeuds de stockage doivent respecter la configuration système requise définie au Chapitre 5, « Configuration du système », page 39 sur la base du taux d'événements attendu et des stratégies de conservation des données pour les espaces de stockage primaire et/ou secondaire.
?	Si vous souhaitez configurer les pare-feux des systèmes d'exploitation de manière à restreindre l'accès à Sentinel et au cluster, reportez-vous au Chapitre 8, « Ports utilisés », page 65 pour plus d'informations sur les ports qui doivent être disponibles selon votre configuration locale et les sources qui envoient des données d'événement.
?	Assurez-vous que l'heure est synchronisée sur tous les noeuds de la grappe. Pour ce faire, vous pouvez utiliser le protocole NTP ou une technologie similaire.
?	◆ La grappe requiert une résolution de nom d'hôte fiable. Entrez tous les noms d'hôte internes de la grappe dans le fichier `/etc/hosts` pour garantir la continuité de la grappe en cas de défaillance DNS. ◆ Veillez à ne pas assigner de nom d'hôte à une adresse IP en boucle. ◆ Lorsque vous configurez le nom d'hôte et le nom de domaine dans le cadre de l'installation du système d'exploitation, désélectionnez l'option **Assign Hostname to Loopback IP** (Assigner le nom d'hôte à l'adresse IP en boucle).

Vous pouvez utiliser la configuration suivante :

- (Conditionnel) Pour les installations à haute disponibilité traditionnelles :
  - Deux machines virtuelles de noeud de grappe avec SLES 11 SP4 ou SLES 12 SP1 ou version ultérieure.
  - (Conditionnel) Vous pouvez installer X Windows si vous souhaitez configurer l'interface graphique. Configurez les scripts de démarrage pour qu'ils démarrent sans Windows X (niveau d'exécution 3), de sorte que vous puissiez les démarrer uniquement en cas de besoin.
- (Conditionnel) Pour les installations d'applicatifs HA : deux machines virtuelles de noeud de grappe basées sur l'applicatif HA ISO. Pour plus d'informations sur l'installation de l'applicatif HA ISO, reportez-vous à la « Installation de Sentinel » page 104.
- Les noeuds ont deux cartes réseau : une pour les accès externes et une autre pour les communications iSCSI.
- Configurez les cartes réseau externes avec des adresses IP qui permettent un accès distant par le biais de SSH ou d'un protocole similaire. Dans le cadre de notre exemple, nous utiliserons les adresses 172.16.0.1 (node01) et 172.16.0.2 (node02).

- Chaque noeud doit disposer d'un espace disque suffisant pour le système d'exploitation, les fichiers binaires et les données de configuration Sentinel, le logiciel de grappe, l'espace temporaire, etc. Consultez la configuration système requise pour SLES et SLES HAE, ainsi que la configuration requise pour l'application Sentinel.
- Une machine virtuelle avec SLES 11 SP4 ou SLES 12 SP1 ou une version ultérieure, configurée avec des cibles iSCSI pour le stockage partagé
  - (Conditionnel) Vous pouvez installer X Windows si vous souhaitez configurer l'interface graphique. Configurez les scripts de démarrage pour qu'ils démarrent sans Windows X (niveau d'exécution 3), de sorte que vous puissiez les démarrer uniquement en cas de besoin.
  - Le système a deux cartes réseau : l'une pour les accès externes et l'autre pour les communications iSCSI.
  - Configurez la carte réseau externe avec une adresse IP qui permet un accès distant à l'aide de SSH ou d'un protocole similaire. Par exemple, 172.16.0.3 (storage03).
  - Le système doit disposer de suffisamment d'espace pour le système d'exploitation, l'espace temporaire et l'emplacement de stockage partagé afin de pouvoir contenir les données Sentinel. Il doit également avoir un peu d'espace pour une partition SBD. Consultez la configuration système requise pour SLES ainsi que les exigences à respecter pour le stockage des données d'événement Sentinel.

REMARQUE : dans une grappe de production, vous pouvez utiliser des adresses IP internes non routables sur des cartes réseau distinctes (éventuellement deux pour assurer la redondance) pour les communications internes entre les grappes.

Configuration de l'espace de stockage partagé

Configurez votre espace de stockage partagé et assurez-vous de pouvoir le monter sur chaque noeud de grappe. Si vous utilisez le protocole Fibre Channel et un réseau SAN, il se peut que vous deviez fournir des connexions physiques, ainsi qu'une configuration supplémentaire. Sentinel utilise cet espace de stockage partagé pour stocker les bases de données et les données d'événement. Assurez-vous que cet espace de stockage partagé est correctement dimensionné en fonction du taux d'événements attendu et des stratégies de conservation des données.

Prenons l'exemple d'un programme d'installation d'espace de stockage partagé :

Une implémentation classique peut consister en un SAN rapide attaché à l'aide de FibreChannel à tous les noeuds de grappe, avec un vaste ensemble RAID pour stocker les données d'événements locales. Un stockage en réseau (NAS) distinct ou un noeud iSCSI peuvent être utilisés pour le stockage secondaire plus lent. Pour autant que le noeud de grappe puisse monter le stockage primaire comme un périphérique de bloc normal, la solution peut l'utiliser. Le stockage secondaire peut également être monté en tant que périphérique de bloc ou consister en un volume NFS ou CIFS.

REMARQUE : Configurez votre stockage partagé et testez son montage sur chaque nœud de grappe. Toutefois, la configuration de grappe gérera le montage réel de l'espace de stockage.

Effectuez la procédure suivante pour créer des cibles iSCSI hébergées par une machine virtuelle SLES :

1. Connectez-vous à la machine virtuelle `storage03` créée lors de la Configuration initiale et démarrez une session de console.
2. Exécutez la commande suivante pour créer un fichier vide de la taille souhaitée pour l'espace de stockage primaire de Sentinel :

   `dd if=/dev/zero of=/localdata count=<taille fichier> bs=<taille bit>`

   Par exemple, exécutez la commande suivante pour créer un fichier de 20 Go rempli de zéros copiés à partir du pseudo-périphérique `/dev/zero` :

   ```
   dd if=/dev/zero of=/localdata count=20480000 bs=1024
   ```
3. Répétez les étapes 1 et 2 afin de créer, de la même manière, un fichier pour le stockage secondaire.

   Par exemple, exécutez la commande suivante pour le stockage secondaire :

   ```
   dd if=/dev/zero of=/networkdata count=20480000 bs=1024
   ```

REMARQUE : dans cet exemple, vous avez créé deux fichiers présentant les mêmes caractéristiques en termes de taille et de performances afin de représenter les deux disques. Pour un déploiement en production, vous pouvez créer l'espace de stockage primaire sur un SAN rapide et l'espace de stockage secondaire sur un volume iSCSI, NFS ou CIFS plus lent.

Effectuez les étapes décrites dans les sections suivantes pour configurer les périphériques d'initiateur et les cibles iSCSI :

- « Configuration des cibles iSCSI » page 198
- « Configuration des initiateurs iSCSI » page 200

Configuration des cibles iSCSI

Effectuez la procédure suivante pour configurer les fichiers `localdata` et `networkdata` en tant que cibles iSCSI.

Pour plus d'informations sur la configuration des cibles iSCSI, reportez-vous à la section Creating iSCSI Targets with YaST (Création des cibles iSCSI avec YaST) dans la documentation de SUSE.

1. Exécutez YaST à partir de la ligne de commande (ou utilisez l'interface graphique si vous préférez) : `/sbin/yast`
2. Sélectionnez **Périphériques réseau** > **Paramètres réseau**.
3. Vérifiez que l'onglet **Présentation** est sélectionné.
4. Sélectionnez la carte réseau secondaire dans la liste affichée, puis avancez avec la touche Tab jusqu'à l'option Modifier et appuyez sur `Entrée`.
5. Sous l'onglet **Adresse**, assignez l'adresse IP statique 10.0.0.3. Cette adresse sera utilisée pour les communications iSCSI internes.
6. Cliquez sur **Suivant**, puis sur **OK**.
7. (Conditionnel) Dans l'écran principal :
   - Si vous utilisez SLES 11 SP4, sélectionnez **Network Services** (Services réseau) > **iSCSI Target** (Cible iSCSI).
   - Si vous utilisez SLES 12 SP1 ou une version ultérieure, sélectionnez **Network Services** (Services réseau) > **iSCSI LIO Target** (Cible iSCSI LIO).

REMARQUE : si vous ne trouvez pas cette option, accédez à **Software** (Logiciels) > **Software Management** (Gestion des logiciels) > **iSCSI LIO Server** (Serveur iSCSI LIO) et installez le paquet iSCSI LIO.

8 (Conditionnel) Si vous y êtes invité, installez le logiciel requis :

- Pour SLES 11 SP4 : `iscsitarget RPM`
- Pour SLES 12 SP1 ou version ultérieure : `iscsiliotarget RPM`

9 (Conditionnel) Avec une version SLES 12 SP1 ou ultérieure, effectuez les opérations suivantes sur tous les noeuds de la grappe :

9a Exécutez la commande suivante pour ouvrir le fichier qui contient le nom de l'initiateur iSCSI :

```
cat /etc/iscsi/initiatorname.iscsi
```

9b Notez le nom de l'initiateur qui sera utilisé pour la configuration des initiateurs iSCSI :

Par exemple :

```
InitiatorName=iqn.1996-04.de.suse:01:441d6988994
```

Ces noms d'initiateur seront utilisés lors de la configuration de l'installation du client cible iSCSI.

10 Cliquez sur **Service**, sélectionnez l'option **When Booting** (Au démarrage) pour que le service se lance au démarrage du système d'exploitation.

11 Sélectionnez l'onglet **Global**, désélectionnez **No Authentication** (Pas d'authentification) pour permettre l'authentification, puis spécifiez les informations d'identification nécessaires pour les authentifications entrante et sortante.

L'option **No Authentication** (Pas d'authentification) est activée par défaut. Toutefois, vous devez activer l'authentification pour vous assurer que la configuration est sécurisée.

12 Cliquez sur **Cibles**, puis sur **Ajouter** pour ajouter une nouvelle cible.

La cible iSCSI génère automatiquement un ID, puis présente une liste reprenant les numéros d'unité logique (LUN) disponibles.

13 Cliquez sur **Ajouter** pour ajouter un nouveau numéro d'unité logique.

14 Laissez 0 comme numéro d'unité logique, puis dans la boîte de dialogue **Chemin d'accès** (sous Type=fileio), accédez au fichier `/localdata` que vous avez créé. Si vous disposez d'un disque dédié au stockage, spécifiez un périphérique de bloc, tel que `/dev/sdc`.

15 Répétez les étapes 13 et 14 et ajoutez le numéro d'unité logique 1, puis sélectionnez à présent `/networkdata`.

16 (Conditionnel) Si vous utilisez SLES 11 SP4, effectuez les opérations suivantes :

16a Conservez les valeurs par défaut des autres options, cliquez sur **OK**, puis sur **Suivant**.

16b (Conditionnel) Si vous avez activé l'authentification à l'étape 11, fournissez les informations d'identification pour l'authentification.

Sélectionnez un client, sélectionnez **Edit Auth** (Modifier l'authentification) > **Incoming Authentication** (Authentification entrante) et spécifiez le nom d'utilisateur et le mot de passe.

17 (Conditionnel) Si vous utilisez une version SLES 12 SP1 ou ultérieure, effectuez les opérations suivantes :

17a Conservez les valeurs par défaut des autres options, puis cliquez sur **Suivant**.

17b Cliquez sur **Ajouter**. Lorsque vous êtes invité à entrer le nom du client, indiquez le nom de l'initiateur que vous avez copié à l'étape 9. Répétez cette étape pour ajouter tous les noms de client, en spécifiant le nom de l'initiateur.

La liste des noms de client s'affichera dans la liste correspondante.

17c (Conditionnel) Si vous avez activé l'authentification à l'étape 11, fournissez les informations d'identification pour l'authentification.

Sélectionnez un client, sélectionnez **Edit Auth** (Modifier l'authentification) > **Incoming Authentication** (Authentification entrante) et spécifiez le nom d'utilisateur et le mot de passe. Répétez cette procédure pour tous les clients.

18 Cliquez de nouveau sur **Suivant** pour sélectionner les options d'authentification par défaut, puis sur **Terminer** pour quitter la configuration. Si vous êtes invité à redémarrer iSCSI, acceptez.

19 Quittez YaST.

REMARQUE : Cette procédure expose deux cibles iSCSI sur le serveur à l'adresse IP 10.0.0.3. Vérifiez, sur chaque noeud de la grappe, qu'il est possible de monter le périphérique de stockage partagé local de données.

Configuration des initiateurs iSCSI

Effectuez la procédure suivante pour formater les périphériques de l'initiateur iSCSI.

Pour plus d'informations sur la configuration des initiateurs iSCSI, reportez-vous à la section Configuring the iSCSI Initiator (Configuration de l'initiateur iSCSI) dans la documentation de SUSE.

1 Connectez-vous à l'un des noeuds de grappe (node01) et démarrez YaST.

2 Sélectionnez **Périphériques réseau** > **Paramètres réseau**.

3 Vérifiez que l'onglet **Présentation** est sélectionné.

4 Sélectionnez dans la liste la carte réseau secondaire, puis avancez avec la touche Tab jusqu'à l'option Modifier et appuyez sur Entrée.

5 Cliquez sur **Adresse**, assignez l'adresse IP statique 10.0.0.1. Cette adresse servira pour les communications iSCSI internes.

6 Sélectionnez **Suivant**, puis cliquez sur **OK**.

7 Cliquez sur **Network Services** (Services réseau) > **iSCSI Initiator** (Initiateur iSCSI).

8 Si vous y êtes invité, installez le logiciel requis (RPM `iscsiclient`).

9 Cliquez sur **Service**, sélectionnez **When Booting** (Au démarrage) pour que le service iSCSI se lance au démarrage du système.

10 Cliquez sur **Discovered Targets** (Cibles découvertes), puis sélectionnez **Discovery** (Découverte).

11 Indiquez l'adresse IP de la cible iSCSI (10.0.0.3).

(Conditionnel) Si vous avez activé l'authentification à l'étape 11 de la « Configuration des cibles iSCSI » page 198, désélectionnez **No Authentication** (Pas d'authentification). Dans le champ **Outgoing Authentication** (Authentification sortante), entrez le nom d'utilisateur et le mot de passe définis lors de la configuration de la cible iSCSI.

Cliquez sur **Suivant**.

12 Sélectionnez la cible iSCSI découverte avec l'adresse IP 10.0.0.3, puis sélectionnez **Se connecter**.

13 Effectuez la procédure suivante.

13a Basculez vers Automatic (Automatique) dans le menu déroulant **Startup** (Démarrage).

13b (Conditionnel) Si vous avez activé l'authentification, désélectionnez **No Authentication** (Pas d'authentification).

Le nom d'utilisateur et le mot de passe spécifiés à l'étape 11 doivent s'afficher dans la section **Outgoing Authentication** (Authentification sortante). Si ces informations d'identification ne s'affichent pas, entrez-les dans cette section.

13c Cliquez sur **Suivant**.

14 Basculez vers l'onglet **Connected Targets** (Cibles connectées) pour vérifier que vous êtes connecté à la cible.

15 Quittez la configuration. Cette procédure doit avoir monté les cibles iSCSI en tant que périphériques de bloc sur le noeud de grappe.

16 Dans le menu principal de YaST, sélectionnez **System** (Système) > **Partitioner** (Partitionneur).

17 Dans la vue Système, de nouveaux disques durs des types suivants (tels que `/dev/sdb` et `/dev/sdc`) doivent s'afficher dans la liste :

- Dans SLES 11 SP4 : IET-VIRTUAL-DISK
- Dans SLES 12 SP1 ou une version ultérieure : LIO-ORG-FILEIO

Appuyez sur la touche Tab pour accéder au premier disque de la liste (qui doit correspondre à l'emplacement de stockage primaire), sélectionnez-le, puis appuyez sur Entrée.

18 Sélectionnez **Ajouter** pour ajouter une nouvelle partition au disque vide. Formatez le disque en tant que partition principale, mais ne le montez pas. Vérifiez que l'option **Do not mount partition** (Ne pas monter la partition) est sélectionnée.

19 Sélectionnez **Next** (Suivant), puis **Finish** (Terminer) après avoir passé en revue les modifications à apporter.

Le disque formaté (par exemple `/dev/sdb1`) doit à présent être prêt. Il est appelé `/dev/<SHARED1>` dans les étapes suivantes de cette procédure.

20 Retournez dans le **partitionneur** et répétez la procédure de partitionnement/formatage (étapes 16 à 19) pour `/dev/sdc` ou tout autre périphérique de bloc correspondant au stockage secondaire. Vous devez obtenir une partition `/dev/sdc1` ou un disque au format similaire (appelé `/dev/<NETWORK1>` comme ci-dessous).

21 Quittez YaST.

22 (Conditionnel) Si vous effectuez une installation HA traditionnelle, créez un point de montage et testez la partition locale comme suit (le nom exact du périphérique peut dépendre de la mise en œuvre spécifique) :

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

Vous devez pouvoir créer des fichiers sur la nouvelle partition et les consulter, quel que soit l'emplacement de montage de la partition.

23 (Conditionnel) Pour procéder à un démontage si vous effectuez une installation HA traditionnelle :

```
# umount /var/opt/novell
```

24 (Conditionnel) Pour les installations d'applicatif HA, répétez les étapes 1 à 15 pour vous assurer que chaque noeud de la grappe peut monter l'espace de stockage partagé local. Pour chaque noeud de grappe, remplacez l'adresse IP du noeud à l'étape 5 par une autre adresse IP.

25 (Conditionnel) Pour les installations HA traditionnelles, répétez les étapes 1 à 15, 22 et 23 pour vous assurer que chaque noeud de la grappe peut monter l'espace de stockage partagé local. Pour chaque noeud de grappe, remplacez l'adresse IP du noeud à l'étape 6 par une autre adresse IP.

Installation de Sentinel

Sentinel peut être installé de deux façons : vous pouvez installer tous les composants de Sentinel dans l'emplacement de stockage partagé (en utilisant l'option `--location` pour rediriger l'installation de Sentinel vers l'emplacement de montage de l'espace de stockage partagé) ou y installer uniquement les données variables de l'application.

Installez Sentinel sur chaque nœud de grappe qui peut l'héberger. Après avoir procédé à la première installation de Sentinel, vous devez effectuer une installation complète comprenant les fichiers binaires de l'application, la configuration et toutes les zones de stockage des données. Pour les installations suivantes sur les autres noeuds de la grappe, seule l'application devra être installée. Les données de Sentinel seront disponibles une fois l'espace de stockage partagé monté.

Installation sur le premier noeud

- « Installation HA traditionnelle » page 202
- « Installation de l'applicatif Sentinel HA » page 203

Installation HA traditionnelle

1. Connectez-vous à l'un des noeuds de grappe (node01) et ouvrez une fenêtre de console.
2. Téléchargez le programme d'installation de Sentinel (fichier tar.gz) et enregistrez-le dans le répertoire `/tmp` sur le noeud de grappe.
3. Pour démarrer l'installation, procédez de la façon suivante :

   3a Exécutez les commandes suivantes :

   ```
   mount /dev/<SHARED1> /var/opt/novell
   cd /tmp
   tar -xvzf sentinel_server*.tar.gz
   cd sentinel_server*
   ./install-sentinel --record-unattended=/tmp/install.props
   ```

   3b Spécifiez `2` pour sélectionner la configuration personnalisée lorsque vous êtes invité à sélectionner la méthode de configuration.
4. Exécutez l'installation et configurez le produit comme il se doit.
5. Démarrez Sentinel et testez les fonctions de base. Vous pouvez utiliser l'adresse IP du noeud de grappe externe standard pour accéder au produit.
6. Arrêtez Sentinel et démontez le stockage partagé à l'aide des commandes suivantes :

   ```
   rcsentinel stop
   umount /var/opt/novell
   ```

   Cette étape supprime les scripts de démarrage automatique pour permettre au cluster de gérer le produit.

   ```
   cd /
   insserv -r sentinel
   ```

Installation de l'applicatif Sentinel HA

L'applicatif Sentinel HA comprend le logiciel Sentinel déjà installé et configuré. Pour configurer le logiciel Sentinel pour HA, procédez comme suit :

1. Connectez-vous à l'un des noeuds de grappe (node01) et ouvrez une fenêtre de console.
2. Accédez au répertoire suivant :

   ```
   cd /opt/novell/sentinel/setup
   ```

3. Enregistrez la configuration :
   - **3a** Exécutez la commande suivante :

     ```
     ./configure.sh --record-unattended=/tmp/install.props --no-start
     ```

     Cette étape enregistre la configuration dans le fichier `install.props`, ce qui s'avère nécessaire pour configurer les ressources de la grappe à l'aide du script `install-resources.sh`.
   - **3b** Spécifiez `2` pour sélectionner la configuration personnalisée lorsque vous êtes invité à sélectionner la méthode de configuration.
   - **3c** Dans l'invite de mot de passe, spécifiez `2` pour entrer un nouveau mot de passe.

     Si vous indiquez `1`, le fichier `install.props` ne stocke pas le mot de passe.
4. Arrêtez Sentinel à l'aide de la commande suivante :

   ```
   rcsentinel stop
   ```

   Cette étape supprime les scripts de démarrage automatique pour permettre au cluster de gérer le produit.

   ```
   insserv -r sentinel
   ```

5. Utilisez les commandes suivantes pour déplacer le dossier de données Sentinel vers le stockage partagé. Cette opération de déplacement permet aux noeuds d'utiliser le dossier de données Sentinel via le stockage partagé.

   ```
   mkdir -p /tmp/new
   ```

   ```
   mount /dev/<SHARED1> /tmp/new
   ```

   ```
   mv /var/opt/novell/* /tmp/new
   ```

   ```
   umount /tmp/new/
   ```

6. Vérifiez le déplacement à l'aide des commandes suivantes :

   ```
   mount /dev/<SHARED1>  /var/opt/novell/
   ```

   ```
   umount /var/opt/novell/
   ```

Installation sur les noeuds suivants

- « Installation HA traditionnelle » page 204
- « Installation de l'applicatif Sentinel HA » page 204

Répétez l'installation sur les autres noeuds :

Le programme d'installation initial de Sentinel crée pour le produit un compte utilisateur qui emploie l'ID utilisateur suivant disponible au moment de l'installation. Les installations suivantes en mode sans surveillance tentent d'employer le même ID utilisateur pour la création du compte, mais des conflits sont possibles (si les noeuds de grappe ne sont pas identiques au moment de l'installation). Il est vivement recommandé d'effectuer l'une des opérations suivantes :

- Synchronisez la base de données des comptes utilisateur sur l'ensemble des noeuds de grappe (manuellement via LDAP ou méthode similaire) avant de commencer les autres installations. De cette façon, le programme d'installation détectera la présence du compte utilisateur existant et l'emploiera.
- Surveillez les résultats des installations sans surveillance suivantes. Un avertissement est émis si le compte utilisateur n'a pas pu être créé avec le même ID utilisateur.

Installation HA traditionnelle

1. Connectez-vous à chaque noeud de grappe supplémentaire (node02) et ouvrez une fenêtre de console.
2. Exécutez les commandes suivantes :

```
cd /tmp
scp root@node01:/tmp/sentinel_server*.tar.gz .
scp root@node01:/tmp/install.props .
tar -xvzf sentinel_server*.tar.gz
cd sentinel_server*
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props
insserv -r sentinel
```

Installation de l'applicatif Sentinel HA

1. Connectez-vous à chaque noeud de grappe supplémentaire (node02) et ouvrez une fenêtre de console.
2. Exécutez la commande suivante :

```
insserv -r sentinel
```

3. Arrêtez les services Sentinel.

```
rcsentinel stop
```

4. Supprimez le répertoire Sentinel.

```
rm -rf /var/opt/novell/*
```

À la fin de ce processus, Sentinel doit être installé sur tous les noeuds, mais il est très probable qu'il ne fonctionne correctement que sur le premier tant que les diverses clés n'ont pas été synchronisées. Cette synchronisation a lieu lors de la configuration des ressources de grappe.

Installation de clusters

Vous ne devez installer le logiciel de grappe que pour les installations HA traditionnelles. L'applicatif Sentinel HA comprend le logiciel de grappe et ne nécessite aucune installation manuelle.

Suivez la procédure ci-dessous pour configurer SLES HAE avec une couche d'agents de ressource spécifique de Sentinel :

1. Installez le logiciel de grappe sur chaque noeud.
2. Enregistrez chaque noeud de grappe au niveau du gestionnaire de grappes.
3. Vérifiez que chaque noeud de grappe s'affiche dans la console de gestion des grappes.

   REMARQUE : L'agent de ressource OCF pour Sentinel est un script Shell simple qui effectue différents contrôles pour vérifier si Sentinel est fonctionnel. Si vous n'utilisez pas l'agent de ressource OCF pour surveiller Sentinel, vous devez développer une solution de surveillance similaire pour l'environnement de grappe local. Pour développer votre propre agent, passez en revue l'agent de ressource existant stocké dans le fichier `Sentinelha.rpm` du paquetage de téléchargement de Sentinel.

   ---
4. Installez le logiciel SLE HAE principal conformément à la documentation SLE HAE.Pour plus d'informations sur l'installation de produits complémentaires SLES, reportez-vous au Guide de déploiement.
5. Répétez l'étape 4 sur tous les noeuds de la grappe. Le produit complémentaire installe le logiciel de communication et de gestion des grappes principal ainsi que les nombreux agents de ressource utilisés pour surveiller les ressources de grappe.
6. Installez un RPM supplémentaire pour fournir les autres agents de ressource de grappe spécifiques à Sentinel. Le RPM HA se trouve dans le fichier `novell-Sentinelha-<version_Sentinel>*.rpm` stocké dans le répertoire de téléchargement par défaut de Sentinel et que vous avez décompressé pour installer le produit.
7. Sur chaque noeud de grappe, copiez le fichier `novell-Sentinelha-<version_Sentinel>*.rpm` dans le répertoire `/tmp`, puis exécutez les commandes suivantes :

```
cd /tmp
```

```
rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

Configuration du cluster

Le logiciel de la grappe doit être configuré pour enregistrer chaque noeud en tant que membre de la grappe. Dans le cadre de cette configuration, vous pouvez également configurer des ressources d'isolement et STONITH (Shoot The Other Node In The Head) pour garantir la cohérence de la grappe.

IMPORTANT : Les procédures dans cette section utilisent les commandes `rcopenais` et `openais`, qui fonctionnent uniquement avec SLES 11 SP4. Pour une version SLES 12 SP2 ou ultérieure, utilisez la commande `systemctl pacemaker.service`.

Par exemple, pour la commande `/etc/rc.d/openais start` , utilisez la commande `systemctl start pacemaker.service`.

Utilisez la procédure suivante pour la configuration de la grappe :

Pour cette solution, vous devez utiliser des adresses IP privées pour les communications de grappe internes et appliquer la monodiffusion pour ne pas devoir demander d'adresse de multidiffusion à l'administrateur réseau. Vous devez également utiliser une cible iSCSI configurée sur la machine virtuelle SLES qui héberge déjà l'espace de stockage partagé pour servir de périphérique SBD (Split Brain Detection) à des fins d'isolement.

Configuration du périphérique SBD

1. Connectez-vous à `storage03` et démarrez une session de console. Exécutez la commande suivante pour créer un fichier vide de la taille de votre choix :

   `dd if=/dev/zero of=/sbd count=<taille fichier> bs=<taille bit>`

   Par exemple, exécutez la commande suivante pour créer un fichier de 1 Mo rempli de zéros copiés à partir du pseudo-périphérique `/dev/zero` :

   ```
   dd if=/dev/zero of=/sbd count=1024 bs=1024
   ```

2. Exécutez YaST à partir de la ligne de commande ou utilisez l'interface graphique : `/sbin/yast`
3. Sélectionnez **Network Services** (Services réseau) > **iSCSI Target** (Cible iSCSI).
4. Cliquez sur **Cibles**, puis sélectionnez la cible existante.
5. Sélectionnez **Modifier**. L'interface utilisateur propose une liste des numéros d'unité logique disponibles.
6. Cliquez sur **Ajouter** pour ajouter un numéro d'unité logique.
7. Laissez 2 comme numéro d'unité logique. Accédez à la boîte de dialogue **Chemin d'accès**, puis sélectionnez le fichier `/sbd` que vous avez créé.
8. Conservez les valeurs par défaut des autres options, puis cliquez sur **OK**, sur **Suivant** et une fois encore sur **Suivant** pour sélectionner les options d'authentification par défaut.
9. Cliquez sur **Terminer** pour quitter la configuration. Redémarrez les services si nécessaire. Quittez YaST.

REMARQUE : la procédure suivante nécessite que chaque noeud de grappe puisse résoudre le nom d'hôte de l'ensemble des noeuds de grappe (faute de quoi le fichier csync2 de synchronisation des services échouera). Si le DNS n'est pas configuré ou est indisponible, ajoutez des entrées pour chaque hôte au fichier `/etc/hosts` qui répertorie chaque adresse IP et son nom d'hôte (telles qu'elles sont signalées par la commande hostname). Veillez également à ne pas assigner de nom d'hôte à une adresse IP en boucle.

Procédez comme suit pour exposer une cible iSCSI pour le périphérique SBD sur le serveur à l'adresse IP 10.0.0.3 (storage03).

Configuration du noeud

Connectez-vous à un noeud de grappe (node01) et ouvrez une console :

1. Exécutez YaST.
2. Cliquez sur **Network Services** (Services réseau) > **iSCSI Initiator** (Initiateur iSCSI).
3. Sélectionnez **Connected Targets** (Cibles connectées), puis choisissez la cible iSCSI configurée ci-dessus.
4. Sélectionnez l'option **Se déconnecter**, puis déconnectez-vous de la cible.
5. Basculez vers l'onglet **Discovered Targets** (Cibles découvertes), sélectionnez **Target** (Cible), puis reconnectez-vous pour rafraîchir la liste des périphériques. Ne modifiez pas l'option de démarrage **automatic** (Automatique), et désélectionnez **No Authentication** (Pas d'authentification).

6. Sélectionnez **OK** pour quitter l'outil de l'initiateur iSCSI.
7. Ouvrez **System** (Système) > **Partitioner** (Partitionneur) et identifiez le périphérique SBD comme suit : 1MB IET-VIRTUAL-DISK. Il sera répertorié en tant que **/dev/sdd** ou une forme similaire (prenez-en note).
8. Quittez YaST.
9. Exécutez la commande `ls -l /dev/disk/by-id/` et notez l'ID de périphérique lié au nom de périphérique situé ci-dessus.
10. (Conditionnel) Exécutez l'une des commandes suivantes :
    - Si vous utilisez SLES 11 SP4 :

      `sleha-init`
    - Avec une version SLES 12 SP1 ou ultérieure :

      `ha-cluster-init`
11. À l'invite de saisie de l'adresse réseau vers laquelle effectuer la liaison, spécifiez l'adresse IP de la carte réseau externe (172.16.0.1).
12. Acceptez le port et l'adresse de multidiffusion par défaut. Nous modifierons ces paramètres par la suite.
13. Entrez `y` pour activer SBD, puis spécifiez `/dev/disk/by-id/<ID_périphérique>`, sachant que `<ID_périphérique>` est l'ID situé ci-dessus (vous pouvez utiliser la touche Tab pour que le chemin soit fourni automatiquement).
14. (Conditionnel) Entrez `N` lorsque l'invite suivante s'affiche :

    ```
    Do you wish to configure an administration IP? [y/N]
    ```

    Pour configurer une adresse IP d'administration, indiquez l'adresse IP virtuelle pendant la « Configuration des ressources » page 209
15. Suivez les étapes de l'assistant et veillez à ce qu'aucune erreur ne soit signalée.
16. Démarrez YaST.
17. Sélectionnez **High Availability** (Haute disponibilité) > **Cluster** (ou simplement Cluster sur certains systèmes).
18. Dans la zone à gauche, veillez à ce que l'option **Communication Channels** (Canaux de communication) soit sélectionnée.
19. Accédez à la première ligne de la configuration à l'aide de la touche Tab, puis modifiez la sélection **udp** en **udpu** (cette opération désactive la multidiffusion au profit de la monodiffusion).
20. Sélectionnez **Add a Member Address** (Ajouter une adresse de membre), spécifiez ce noeud (172.16.0.1), puis répétez l'opération pour ajouter les autres noeuds de grappe : 172.16.0.2.
21. Cliquez sur **Terminer** pour achever la configuration.
22. Quittez YaST.
23. Exécutez la commande `/etc/rc.d/openais restart` pour redémarrer les services de grappe avec le nouveau protocole de synchronisation.

Connectez-vous à chaque noeud de grappe supplémentaire (node02) et ouvrez une console :

1. Exécutez YaST.
2. Cliquez sur **Network Services** (Services réseau) > **iSCSI Initiator** (Initiateur iSCSI).
3. Sélectionnez **Connected Targets** (Cibles connectées), puis choisissez la cible iSCSI configurée ci-dessus.
4. Sélectionnez l'option **Se déconnecter**, puis déconnectez-vous de la cible.

5 Basculez vers l'onglet **Discovered Targets** (Cibles découvertes), sélectionnez **Target** (Cible), puis reconnectez-vous pour rafraîchir la liste des périphériques. Ne modifiez pas l'option de démarrage **automatic** (Automatique), et désélectionnez **No Authentication** (Pas d'authentification).

6 Sélectionnez **OK** pour quitter l'outil de l'initiateur iSCSI.

7 (Conditionnel) Exécutez l'une des commandes suivantes :

- Si vous utilisez SLES 11 SP4 :

  ```
  sleha-join
  ```

- Avec une version SLES 12 SP1 ou ultérieure :

  ```
  ha-cluster-join
  ```

8 Entrez l'adresse IP du premier noeud de grappe.

(Conditionnel) Si la grappe ne démarre pas correctement, procédez comme suit :

1 Exécutez la commande `crm status` pour vérifier si les nœuds sont reliés. Si les nœuds ne sont pas connectés, redémarrez tous les nœuds de la grappe.

2 Copiez manuellement le fichier `/etc/corosync/corosync.conf` de `node01` vers `node02` ou exécutez `csync2 -x -v` sur `node01`. Vous pouvez également paramétrer manuellement la grappe sur `node02` à l'aide de YaST.

3 (Conditionnel) Si la commande `csync2 -x -v` que vous avez exécutée à l'étape 1 ne parvient pas à synchroniser l'ensemble des fichiers, procédez comme suit :

3a Effacez la base de données csync2 dans le répertoire`/var/lib/csync2` de tous les nœuds.

3b Sur tous les nœuds, mettez à jour la base de données csync2 afin de la faire correspondre au système de fichiers, mais sans marquer aucun élément en vue de leur synchronisation avec d'autres serveurs :

```
csync2 -cIr /
```

3c Sur le nœud actif, procédez comme suit :

3c1 Trouvez toutes les différences entre les nœuds actifs et passifs, et marquez ces différences pour la synchronisation :

```
csync2 -TUXI
```

3c2 Réinitialisez la base de données pour forcer le nœud actif à ignorer les conflits :

```
csync2 -fr /
```

3c3 Démarrez la synchronisation sur tous les autres nœuds :

```
csync2 -xr /
```

3d Sur tous les nœuds, vérifiez que tous les fichiers sont synchronisés :

```
csync2 -T
```

Cette commande répertorie uniquement les fichiers qui ne sont pas synchronisés.

4 Exécutez la commande suivante sur `node02` :

Pour SLES 11 SP4 :

```
/etc/rc.d/openais start
```

Pour une version SLES 12 SP1 ou ultérieure :

```
systemctl start pacemaker.service
```

(Conditionnel) Si le service `xinetd` n'ajoute pas correctement le nouveau service `csync2`, le script ne fonctionne pas correctement. Le service `xinetd` est nécessaire pour que l'autre noeud puisse synchroniser les fichiers de configuration de la grappe sur ce noeud. En cas d'erreurs du type `csync2 run failed` (échec de l'exécution de csync2), ce problème risque de vous concerner.

Pour résoudre ce problème, exécutez la commande `kill -HUP `cat /var/run/xinetd.init.pid`, puis réexécutez le script `sleha-join`.

5 Exécutez `crm_mon` sur chaque noeud de grappe afin de vérifier que la grappe s'exécute correctement. Vous pouvez également utiliser la console Web « hawk » pour vérifier la grappe. Le nom de connexion par défaut est `hacluster` et le mot de passe est `linux`.

(Conditionnel) En fonction de votre environnement, procédez comme suit pour modifier des paramètres supplémentaires :

1 Pour vous assurer qu'une défaillance sur un noeud d'une grappe à deux noeuds n'entraîne pas l'arrêt inopiné de l'ensemble de la grappe, définissez l'option de grappe globale `no-quorum-policy` sur `ignore` :

```
crm configure property no-quorum-policy=ignore
```

REMARQUE : si votre grappe comporte plusieurs noeuds, ne définissez pas cette option.

2 Pour être sûr que le gestionnaire des ressources autorise l'exécution des ressources et leur déplacement, définissez l'option de grappe globale `default-resource-stickiness` sur 1 :

```
crm configure property default-resource-stickiness=1
```

Configuration des ressources

Les agents de ressource sont fournis par défaut avec SLE HAE. Si vous ne souhaitez pas utiliser SLE HAE, vous devez surveiller ces ressources supplémentaires à l'aide d'une autre technologie :

- une ressource de système de fichiers correspondant au système de stockage partagé utilisé par le logiciel.
- une ressource d'adresse IP correspondant à l'adresse IP virtuelle donnant accès aux services.
- le logiciel de base de données PostgreSQL qui stocke les métadonnées de configuration et d'événement.

Utilisez la procédure suivante pour la configuration des ressources :

Le script `crm` vous aide pour la configuration de la grappe. Le script extrait les variables de configuration pertinentes du fichier d'installation sans surveillance généré dans le cadre de l'installation de Sentinel. Si vous n'avez pas généré de fichier de configuration ou que vous souhaitez modifier la configuration actuelle des ressources, vous pouvez procéder comme suit pour modifier le script en conséquence.

1 Connectez-vous au noeud sur lequel vous avez initialement installé Sentinel.

REMARQUE : il doit s'agir du noeud sur lequel vous avez effectué l'installation complète de Sentinel.

2 Modifiez le script pour qu'il apparaisse comme suit, où `<SHARED1>` est le volume partagé que vous avez créé précédemment :

```
mount /dev/<SHARED1> /var/opt/novell
```

```
cd /usr/lib/ocf/resource.d/novell

./install-resources.sh
```

3. (Conditionnel) Vous pourriez avoir des difficultés avec les nouvelles ressources de la grappe. Dans ce cas, exécutez la commande suivante sur node02 :

   Pour SLES 11 SP4 :

   ```
   /etc/rc.d/openais start
   ```

   Pour SLES 12 SP1 :

   ```
   systemctl start pacemaker.service
   ```

4. Le script `install-resources.sh` vous demande d'entrer quelques valeurs, notamment l'adresse IP virtuelle à utiliser pour l'accès à Sentinel ainsi que le nom du périphérique de stockage partagé. Il crée ensuite automatiquement les ressources de grappe requises. N'oubliez pas que le script exige que le volume partagé soit déjà monté, mais aussi que le fichier d'installation sans surveillance créé pendant l'installation de Sentinel soit présent à l'emplacement `/tmp/install.props`. Vous ne devez exécuter ce script que sur le premier noeud installé ; tous les fichiers de configuration pertinents seront automatiquement synchronisés avec les autres noeuds.

5. Si votre environnement diffère de la solution recommandée par , vous pouvez modifier le fichier `resources.cli` (dans le même répertoire) et modifier les définitions de primitives à partir de ce fichier. Par exemple, la solution recommandée utilise une ressource de système de fichiers simple, mais vous préférerez peut-être utiliser une ressource cLVM davantage axée sur la grappe.

6. Après avoir exécuté le script Shell, vous pouvez exécuter une commande d'état `crm`. Le résultat devrait se présenter comme suit :

   ```
   crm status
   ```

   ```
   Last updated: Thu Jul 26 16:34:34 2012
   Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
   Stack: openais
   Current DC: node01 - partition with quorum
   Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
   2 Nodes configured, 2 expected votes
   5 Resources configured.
   ```

   ```
   Online: [ node01, node02 ]
   stonith-sbd    (stonith:external/sbd):    Started node01
    Resource Group: sentinelgrp
        sentinelip    (ocf::heartbeat:IPaddr2):    Started node01
        sentinelfs    (ocf::heartbeat:Filesystem):    Started node01
        sentineldb    (ocf::novell:pgsql):    Started node01
        sentinelserver    (ocf::novell:sentinel):    Started node01
   ```

7. À ce stade, les ressources Sentinel pertinentes doivent être configurées dans la grappe. Vous pouvez examiner la façon dont elles sont configurées et groupées dans l'outil de gestion des grappes, par exemple, en exécutant l'état crm.

Configuration du stockage secondaire

Procédez comme suit pour configurer l'espace de stockage secondaire, de sorte que Sentinel puisse faire migrer des partitions d'événements vers un espace de stockage meilleur marché :

REMARQUE : cette opération est facultative et l'espace de stockage secondaire ne doit pas être configuré avec un mode Haute disponibilité comme pour le reste du système. Vous pouvez utiliser n'importe quel répertoire, qu'il soit monté à partir d'un SAN ou non, d'un volume CIFS ou NFS.

1. Dans la barre de menus supérieure de l'interface principale de Sentinel, cliquez sur **Stockage**.
2. Sélectionnez **Configuration**.
3. Sélectionnez l'une des cases d'option sous le stockage secondaire non configuré.

Utilisez une simple cible iSCSI comme emplacement de stockage réseau partagé avec une configuration relativement comparable à celle du système de stockage primaire. Les technologies de stockage utilisées peuvent être différentes dans votre environnement de production.

Utilisez la procédure suivante pour configurer le stockage secondaire que Sentinel doit utiliser :

REMARQUE : Pour une cible iSCSI, la cible est montée en tant que répertoire à utiliser comme stockage secondaire. Vous devez configurer le montage en tant que ressource de système de fichiers de la même façon que le système de fichiers de stockage primaire. Cette configuration n'a pas été effectuée automatiquement dans le cadre du script d'installation de la ressource, car d'autres variantes sont possibles.

1. Passez en revue les étapes ci-dessus pour déterminer quelle partition a été créée pour accueillir le stockage secondaire (`/dev/<NETWORK1>` ou une appellation de type `/dev/sdc1`). Créez au besoin un répertoire vide sur lequel la partition peut être montée (par exemple, `/var/opt/netdata`).
2. Configurez le système de fichiers réseau en tant que ressource de grappe. Pour ce faire, utilisez l'interface principale de Sentinel ou exécutez la commande suivante :

   ```
   crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
   ```

   `/dev/<NETWORK1>` représente la partition créée dans la section Configuration du stockage partagé ci-dessus et <PATH> est le répertoire local sur lequel elle peut être montée.
3. Ajoutez la nouvelle ressource au groupe des ressources gérées :

   ```
   crm resource stop sentinelgrp
   crm configure delete sentinelgrp
   crm configure group sentinelgrp sentinelip sentinelfs sentinelnetfs sentineldb sentinelserver
   crm resource start sentinelgrp
   ```
4. Vous pouvez vous connecter au noeud qui héberge actuellement les ressources (utilisez l'`état crm` ou `Hawk`). Vérifiiez que le stockage réseau est correctement monté (utilisez la commande `mount`).
5. Connectez-vous à l'interface principale de Sentinel.
6. Sélectionnez **Stockage**, **Configuration**, puis **SAN (monté localement)**) sous Stockage secondaire non configuré.
7. Entrez le chemin de l'emplacement dans lequel le stockage secondaire est monté, par exemple `/var/opt/netdata`.

Utilisez des versions simplifiées des ressources requises telles que l'agent de ressource simple du système de fichiers. Au besoin, vous pouvez utiliser des ressources de grappe plus sophistiquées telles que cLVM (une version de volume logique du système de fichiers).

38 Configuration de Sentinel HA en tant que SSDM

Ce chapitre fournit des informations sur la configuration d'une installation de Sentinel HA en tant que SSDM. Ces instructions s'appliquent aussi bien aux installations traditionnelles qu'aux installations d'applicatifs.

Pour configurer une installation de Sentinel HA en tant que SSDM, procédez comme suit :

1. Installez et configurez le stockage évolutif pour Sentinel. Pour plus d'informations, reportez-vous à la Chapitre 13, « Installation et configuration du stockage évolutif », page 89.
2. Activez le stockage évolutif sur le noeud actif. Pour plus d'informations, reportez-vous à la section « Enabling Scalable Storage Post-Installation » (Activation du stockage évolutif après l'installation) du *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
3. Exécutez la commande suivante sur le noeud actif :

   ```
   csync2 -x -v
   ```

   Cette commande synchronise la configuration SSDM sur tous les noeuds passifs.
4. (Conditionnel) Si la commande `csync2 -x -v` que vous avez exécutée à l'étape 3 ne parvient pas à synchroniser l'ensemble des fichiers, procédez comme suit :

   4a Effacez la base de données csync2 (située dans le répertoire `/var/lib/csync2`) de tous les noeuds.

   4b Exécutez la commande suivante sur tous les serveurs pour mettre à jour la base de données csync2 afin de la faire correspondre au système de fichiers, mais sans marquer aucun élément en vue de leur synchronisation avec d'autres serveurs :

   ```
   csync2 -cIr /
   ```

   4c Exécutez la commande suivante pour rechercher toutes les différences entre un serveur expert et les serveurs distants et les marquer en vue de leur synchronisation :

   ```
   csync2 -TUXI
   ```

   4d Exécutez la commande suivante pour réinitialiser la base de données afin de forcer le serveur actuel à remporter tous les conflits :

   ```
   csync2 -fr /
   ```

   4e Exécutez la commande suivante pour lancer une synchronisation sur tous les autres serveurs :

   ```
   csync2 -xr /
   ```

   4f Exécutez la commande suivante pour vérifier que tous les fichiers sont synchronisés :

   ```
   csync2 -T
   ```

   Cette commande ne répertorie aucun fichier si la synchronisation réussit.

39 Mise à niveau de Sentinel dans une configuration à haute disponibilité

Lorsque vous mettez à niveau Sentinel dans un environnement à haute disponibilité (HA), commencez par mettre à niveau les noeuds passifs de la grappe, puis passez au noeud actif.

Conditions préalables

- Téléchargez la dernière version du programme d'installation sur le site Web de téléchargement .
- Si vous utilisez le système d'exploitation SLES avec le kernel version 3.0.101 ou une version ultérieure, vous devez charger manuellement le pilote de surveillance sur l'ordinateur. Pour identifier le pilote approprié à votre matériel, contactez le fabricant du matériel. Pour charger le pilote de surveillance, procédez comme suit :
  1. À l'invite de commande, exécutez la commande suivante pour charger le pilote de surveillance dans la session en cours :

     `/sbin/modprobe -v --ignore-install <nom pilote surveillance>`
  2. Ajoutez la ligne suivante au fichier `/etc/init.d/boot.local` pour vous assurer que l'ordinateur charge automatiquement le pilote de surveillance à chaque démarrage :

     `/sbin/modprobe -v --ignore-install <nom pilote surveillance>`

Mise à niveau d'une installation Sentinel HA traditionnelle

Cette section fournit des informations sur la mise à niveau d'une installation traditionnelle de Sentinel, ainsi que sur la mise à niveau de son système d'exploitation.

IMPORTANT : Les procédures dans cette section utilisent les commandes `rcopenais` et `openais`, qui fonctionnent uniquement avec SLES 11 SP4. Pour une version SLES 12 SP2 ou ultérieure, utilisez la commande `systemctl pacemaker.service`.

Par exemple, pour la commande `/etc/rc.d/openais start` , utilisez la commande `systemctl start pacemaker.service`.

Mise à niveau de Sentinel HA

1 Activez le mode de maintenance sur la grappe :

```
crm configure property maintenance-mode=true
```

Le mode de maintenance permet d'éviter toute perturbation des ressources de la grappe en cours d'exécution lors de la mise à jour de Sentinel. Vous pouvez exécuter cette commande depuis n'importe quel noeud de la grappe.

2 Vérifiez si le mode de maintenance est actif :

```
crm status
```

Les ressources de la grappe doivent apparaître dans l'état non géré.

3 Mettez à niveau le noeud passif de la grappe :

3a Arrêtez la pile de grappes :

```
rcopenais stop
```

L'arrêt de la pile de grappes garantit que les ressources de la grappe restent accessibles et évite tout arrêt des noeuds.

3b Connectez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez mettre à niveau Sentinel.

3c Extrayez les fichiers d'installation du fichier TAR :

```
tar xfz <nom_fichier_installation>
```

3d Exécutez la commande suivante dans le répertoire dans lequel vous avez extrait les fichiers d'installation :

```
./install-sentinel --cluster-node
```

3e Lorsque la mise à niveau est terminée, redémarrez la pile de grappes :

```
rcopenais start
```

Répétez l'Étape 3 pour tous les noeuds passifs de la grappe.

3f Supprimez les scripts de démarrage automatique pour permettre à la grappe de gérer le produit.

```
cd /
insserv -r sentinel
```

4 Mettez à niveau le noeud actif de la grappe :

4a Sauvegardez votre configuration, puis créez une exportation ESM.

Pour plus d'informations sur la sauvegarde des données, reportez-vous à la section « Backing Up and Restoring Data (Sauvegarde et restauration des données) » du manuel *Sentinel Administration Guide (Guide d'administration de NetIQ Sentinel 7.1)*.

4b Arrêtez la pile de grappes :

```
rcopenais stop
```

L'arrêt de la pile de grappes garantit que les ressources de la grappe restent accessibles et évite tout arrêt des noeuds.

4c Connectez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez mettre à niveau Sentinel.

4d Exécutez la commande suivante pour extraire les fichiers d'installation du fichier TAR :

```
tar xfz <nom_fichier_installation>
```

4e Exécutez la commande suivante dans le répertoire dans lequel vous avez extrait les fichiers d'installation :

```
./install-sentinel
```

4f Lorsque la mise à niveau est terminée, démarrez la pile de grappes :

```
rcopenais start
```

4g Supprimez les scripts de démarrage automatique pour permettre à la grappe de gérer le produit.

```
cd /
insserv -r sentinel
```

4h Exécutez la commande suivante pour synchroniser les éventuelles modifications dans les fichiers de configuration :

```
csync2 -x -v
```

5 Désactivez le mode de maintenance sur la grappe :

```
crm configure property maintenance-mode=false
```

Vous pouvez exécuter cette commande depuis n'importe quel noeud de la grappe.

6 Vérifiez si le mode de maintenance est inactif :

```
crm status
```

Les ressources de grappe doivent apparaître dans l'état Démarré.

7 (Facultatif) Vérifiez si la mise à niveau de Sentinel s'est déroulée correctement :

```
rcsentinel version
```

Mise à niveau du système d'exploitation

Cette section fournit des informations sur la procédure visant à effectuer une mise niveau majeure du système d'exploitation, par exemple passer de SLES 11 à SLES 12 dans une grappe Sentinel HA. Lorsque vous mettez à niveau le système d'exploitation, vous devez effectuer quelques tâches de configuration pour vérifier que Sentinel HA fonctionne correctement après la mise à niveau du système d'exploitation.

Effectuez les étapes décrites dans les sections suivantes :

- « Mise à niveau du système d'exploitation » page 217
- « Configuration des cibles iSCSI » page 218
- « Configuration des initiateurs iSCSI » page 219
- « Configuration de la grappe HA » page 220

Mise à niveau du système d'exploitation

Pour mettre à niveau le système d'exploitation, procédez comme suit :

1 Connectez-vous en tant qu'utilisateur `root` à n'importe quel noeud de la grappe Sentinel HA.

2 Exécutez la commande suivante pour activer le mode de maintenance sur la grappe :

```
crm configure property maintenance-mode=true
```

Le mode de maintenance permet d'éviter toute perturbation des ressources de la grappe en cours d'exécution lors de la mise à niveau du système d'exploitation.

3 Exécutez la commande suivante pour vérifier si le mode de maintenance est actif :

```
crm status
```

Les ressources de la grappe doivent apparaître dans l'état non géré.

4 Vérifiez que vous avez mis à niveau Sentinel vers la version 8.2 ou version ultérieure sur tous les noeuds de la grappe.

5 Vérifiez que tous les noeuds de la grappe sont enregistrés auprès de SLES et SLES HA.

6 Procédez comme suit pour mettre à niveau le système d'exploitation sur le noeud passif de la grappe :

6a Exécutez la commande suivante pour arrêter la pile de grappes :

```
rcopenais stop
```

L'arrêt de la pile de grappes garantit que les ressources de la grappe restent inaccessibles et évite l'isolement des noeuds.

6b Procédez à la mise à niveau du système d'exploitation. Pour plus d'informations, reportez-vous à la section Mise à niveau du système d'exploitation.

7 Répétez l'étape 6 sur tous les nœuds passifs pour mettre à niveau le système d'exploitation.

8 Répétez l'étape 6 sur le nœud actif pour mettre à niveau le système d'exploitation sur ce nœud.

9 Répétez l'étape 6b pour mettre à niveau le système d'exploitation sur un espace de stockage partagé.

10 Vérifiez que le système d'exploitation est mis à niveau vers SLES12 SP3 sur tous les noeuds de la grappe.

Configuration des cibles iSCSI

Pour configurer des cibles iSCSI, procédez comme suit :

1 Vérifiez si le paquet iSCSI LIO est installé dans l'espace de stockage partagé. S'il ne l'est pas encore, accédez au Gestionnaire de logiciels YaST2 et installez le paquet iSCSI LIO (RPM `iscciliotarget`).

2 Effectuez les opérations suivantes sur tous les noeuds de la grappe :

2a Exécutez la commande suivante pour ouvrir le fichier qui contient le nom de l'initiateur iSCSI :

```
cat /etc/iscsi/initiatorname.iscsi
```

2b Notez le nom de l'initiateur qui sera utilisé pour la configuration des initiateurs iSCSI :

Par exemple :

```
InitiatorName=iqn.1996-04.de.suse:01:441d6988994
```

Ces noms d'initiateur seront utilisés lors de la configuration de l'installation du client cible iSCSI.

3 Cliquez sur **Service**, sélectionnez l'option **When Booting** (Au démarrage) pour que le service se lance au démarrage du système d'exploitation.

4 Sélectionnez l'onglet **Global**, désélectionnez **No Authentication** (Pas d'authentification) pour activer l'authentification, puis spécifiez le nom d'utilisateur et le mot de passe pour les authentifications entrante et sortante.

L'option **No Authentication** (Pas d'authentification) est activée par défaut. Toutefois, vous devez activer l'authentification pour vous assurer que la configuration est sécurisée.

5 Cliquez sur **Cibles**, puis sur **Ajouter** pour ajouter une nouvelle cible.

6 Cliquez sur **Ajouter** pour ajouter un nouveau numéro d'unité logique.

7 Laissez 0 comme numéro d'unité logique, dans la boîte de dialogue **Chemin d'accès** (sous Type=fileio), puis sélectionnez le fichier `/localdata` que vous avez créé. Si vous disposez d'un disque dédié au stockage, spécifiez un périphérique de bloc, tel que `/dev/sdc`.

8 Répétez les étapes 6 et 7, puis ajoutez le numéro d'unité logique 1, et sélectionnez à présent `/networkdata`.

9 Répétez les étapes 6 et 7, puis ajoutez le numéro d'unité logique 2, et sélectionnez à présent `/sbd`.

10 Conservez les valeurs par défaut des autres options. Cliquez sur **Suivant**.

11 Cliquez sur **Ajouter**. Lorsque vous êtes invité à entrer le nom du client, indiquez le nom de l'initiateur que vous avez copié à l'étape 2. Répétez cette étape pour ajouter tous les noms de client, en spécifiant le nom de l'initiateur.

La liste des noms de client s'affichera dans la liste correspondante.

12 (Conditionnel) Si vous avez activé l'authentification à l'étape 4, fournissez les informations d'identification pour l'authentification spécifiées à cette étape.

Sélectionnez un client, sélectionnez **Edit Auth** (Modifier l'authentification) > **Incoming Authentication** (Authentification entrante) et spécifiez le nom d'utilisateur et le mot de passe. Répétez cette procédure pour tous les clients.

13 Cliquez sur **Next** (Suivant) pour sélectionner les options d'authentification par défaut, puis sur **Finish** (Terminer) pour quitter la configuration. Redémarrez iSCSI si vous y êtes invité.

14 Quittez YaST.

Configuration des initiateurs iSCSI

Pour configurer des initiateurs iSCSI, procédez comme suit :

1 Connectez-vous à l'un des noeuds de grappe (node01) et démarrez YaST.

2 Cliquez sur **Network Services** (Services réseau) > **iSCSI Initiator** (Initiateur iSCSI).

3 Si vous y êtes invité, installez le logiciel requis (RPM `iscsiclient`).

4 Cliquez sur **Service**, sélectionnez **When Booting** (Au démarrage) pour que le service iSCSI se lance au démarrage.

5 Cliquez sur **Discovered Targets** (Cibles découvertes).

REMARQUE : Si des cibles iSCSI préexistantes sont affichées, supprimez-les.

Sélectionnez **Discovery** (Découverte) pour ajouter une nouvelle cible iSCSI.

6 Indiquez l'adresse IP de la cible iSCSI (10.0.0.3).

(Conditionnel) Si vous avez activé l'authentification à l'étape 4 de la « Configuration des cibles iSCSI » page 218, désélectionnez **No Authentication** (Pas d'authentification). Dans la section **Outgoing Authentication** (Authentification sortante), entrez les informations d'identification pour l'authentification définies lors de la configuration de la cible iSCSI.

Cliquez sur **Suivant**.

7 Sélectionnez la cible iSCSI découverte avec l'adresse IP 10.0.0.3, puis sélectionnez **Log In** (Se connecter).

8 Effectuez la procédure suivante.

8a Basculez vers Automatic (Automatique) dans le menu déroulant **Startup** (Démarrage).

8b (Conditionnel) Si vous avez activé l'authentification, désélectionnez **No Authentication** (Pas d'authentification).

Le nom d'utilisateur et le mot de passe spécifiés doivent s'afficher dans la section **Outgoing Authentication** (Authentification sortante). Si ces informations d'identification ne s'affichent pas, entrez-les dans cette section.

8c Cliquez sur **Suivant**.

9 Basculez vers l'onglet **Connected Targets** (Cibles connectées) pour vérifier que vous êtes connecté à la cible.

10 Quittez la configuration. Cette procédure doit avoir monté les cibles iSCSI en tant que périphériques de bloc sur le noeud de grappe.

11 Dans le menu principal de YaST, sélectionnez **System** (Système) > **Partitioner** (Partitionneur).

12 La vue Système doit afficher de nouveaux disques durs de type LIO-ORG-FILEIO (tels que `/dev/sdb` et `/dev/sdc`) dans la liste, ainsi que des disques déjà formatés (tels que `/dev/sdb1` ou `/dev/ < SHARED1`).

13 Répétez les étapes 1 à 12 sur tous les noeuds.

Configuration de la grappe HA

Pour configurer la grappe HA, procédez comme suit :

1 Démarrez YaST2 et accédez à **High Availability** (Haute disponibilité) > **Cluster** (Grappe).

2 Si vous y êtes invité, installez le paquet HA et résolvez les dépendances.

Après l'installation du paquet HA, Cluster—Communication Channels (Grappe—Canaux de communication) s'affiche.

3 Veillez à ce que l'option `Unicast` (Monodiffusion) soit sélectionnée comme option de transport.

4 Sélectionnez **Add a Member Address** (Ajouter une adresse de membre) et indiquez l'adresse IP du noeud, puis répétez cette opération pour ajouter toutes les autres adresses IP du noeud de la grappe.

5 Vérifiez que l'option **Auto Generate Node ID** (Générer automatiquement un ID de noeud) est sélectionnée.

6 Vérifiez que le service HAWK est activé sur tous les noeuds. À défaut, exécutez la commande suivante pour l'activer :

```
service hawk start
```

7 Exécutez la commande suivante :

```
ls -l /dev/disk/by-id/
```

L'ID de partition SBD s'affiche. Par exemple, `scsi-1LIO-ORG_FILEIO:33caaa5a-a0bc-4d90-b21b-2ef33030cc53`.

Copiez l'ID.

8 Ouvrez le fichier SBD (`/etc/sysconfig/sbd`) et remplacez l'ID de `SBD_DEVICE` par celui copié à l'étape 7.

9 Exécutez les commandes suivantes pour redémarrer le service pacemaker :

```
rcpacemaker restart
```

10 Exécutez les commandes suivantes pour supprimer les scripts de démarrage automatique (autostart) afin que la grappe puisse gérer le produit.

```
cd /
```

```
insserv -r sentinel
```

11 Répétez les étapes 1 à 10 sur tous les noeuds de la grappe.

12 Exécutez la commande suivante pour synchroniser les éventuelles modifications dans les fichiers de configuration :

```
csync2 -x -v
```

13 Exécutez la commande suivante pour désactiver le mode de maintenance sur la grappe :

```
crm configure property maintenance-mode=false
```

Vous pouvez exécuter cette commande depuis n'importe quel noeud de la grappe.

14 Exécutez la commande suivante pour vérifier si le mode de maintenance est inactif :

```
crm status
```

Les ressources de grappe doivent apparaître dans l'état Démarré.

Mise à niveau d'une installation d'applicatif Sentinel HA

Vous pouvez mettre à niveau une installation d'applicatif Sentinel HA à l'aide du correctif Zypper.

IMPORTANT : Les procédures dans cette section utilisent les commandes `rcopenais` et `openais`, qui fonctionnent uniquement avec SLES 11 SP4. Pour une version SLES 12 SP2 ou ultérieure, utilisez la commande `systemctl pacemaker.service`.

Par exemple, pour la commande `/etc/rc.d/openais start` , utilisez la commande `systemctl start pacemaker.service`.

- « Mise à niveau de l'applicatif Sentinel HA à l'aide de Zypper » page 221

Mise à niveau de l'applicatif Sentinel HA à l'aide de Zypper

Avant de procéder à la mise à niveau, vous devez enregistrer tous les noeuds d'applicatif via le gestionnaire de l'applicatif Sentinel. Pour plus d'informations, reportez-vous à la section « Enregistrement pour obtenir les mises à jour » page 108. Si vous n'enregistrez pas l'applicatif, Sentinel affiche un avertissement en jaune.

1 Activez le mode de maintenance sur la grappe.

```
crm configure property maintenance-mode=true
```

Le mode de maintenance permet d'éviter toute perturbation des ressources de la grappe en cours d'exécution lors de la mise à jour du logiciel Sentinel. Vous pouvez exécuter cette commande depuis n'importe quel noeud de la grappe.

2 Vérifiez que le mode de maintenance est actif.

```
crm status
```

Les ressources de la grappe doivent apparaître dans l'état non géré.

3 Mettez à niveau le noeud passif de la grappe :

3a Arrêtez la pile de grappes.

```
rcopenais stop
```

L'arrêt de la pile de grappes garantit que les ressources de la grappe restent inaccessibles et évite l'isolement des noeuds.

3b Téléchargez les mises à jour de l'application Sentinel HA.

```
zypper -v patch
```

3c (Conditionnel) Si le programme d'installation affiche un message indiquant que vous devez résoudre une dépendance pour le paquet OpenSSH, entrez l'option appropriée pour mettre à niveau le paquet OpenSSH vers une version antérieure.

3d (Conditionnel) Si le programme d'installation affiche un message indiquant un changement dans l'architecture ncgOverlay, entrez l'option appropriée pour accepter le changement d'architecture.

3e (Conditionnel) Si le programme d'installation affiche un message indiquant que vous devez résoudre une dépendance pour certains paquets d'applicatifs, entrez l'option appropriée pour désinstaller les paquets dépendants.

3f Une fois la mise à niveau terminée, démarrez la pile de grappes.

```
rcopenais start
```

4 Répétez l'étape 3 pour tous les noeuds passifs de la grappe.

5 Mettez à niveau le noeud actif de la grappe :

5a Sauvegardez votre configuration, puis créez une exportation ESM.

Pour plus d'informations sur la sauvegarde des données, reportez-vous à la section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

5b Arrêtez la pile de grappes.

```
rcopenais stop
```

L'arrêt de la pile de grappes garantit que les ressources de la grappe restent inaccessibles et évite l'isolement des noeuds.

5c Téléchargez les mises à jour de l'application Sentinel HA.

```
zypper -v patch
```

5d (Conditionnel) Si le programme d'installation affiche un message indiquant que vous devez résoudre une dépendance pour le paquet OpenSSH, entrez l'option appropriée pour mettre à niveau le paquet OpenSSH vers une version antérieure.

5e (Conditionnel) Si le programme d'installation affiche un message indiquant un changement dans l'architecture ncgOverlay, entrez l'option appropriée pour accepter le changement d'architecture.

5f (Conditionnel) Si le programme d'installation affiche un message indiquant que vous devez résoudre une dépendance pour certains paquets d'applicatifs, entrez l'option appropriée pour désinstaller les paquets dépendants.

5g Une fois la mise à niveau terminée, démarrez la pile de grappes.

```
rcopenais start
```

5h Exécutez la commande suivante pour synchroniser les éventuelles modifications dans les fichiers de configuration :

```
csync2 -x -v
```

6 Désactivez le mode de maintenance sur la grappe.

```
crm configure property maintenance-mode=false
```

Vous pouvez exécuter cette commande depuis n'importe quel noeud de la grappe.

7 Vérifiez que le mode de maintenance est inactif.

```
crm status
```

Les ressources de grappe doivent apparaître dans l'état Démarré.

8 (Facultatif) Vérifiez si la mise à niveau de Sentinel s'est déroulée correctement :

```
rcsentinel version
```

9 (Facultatif) Pour mettre à niveau le système d'exploitation, reportez-vous à « Mise à niveau du système d'exploitation » page 164.

40 Sauvegarde et récupération

La grappe de basculement à haute disponibilité décrit dans ce document fournit un niveau élevé de redondance, de sorte qu'en cas d'échec d'un service sur un noeud de grappe, celui-ci bascule automatiquement vers un autre noeud de la grappe à des fins de récupération. Lorsque ce type d'événement se produit, il convient de rendre au noeud ayant basculé un état opérationnel afin de pouvoir rétablir la redondance dans le système et lui permettre de faire face à un éventuel autre échec. Cette section explique comment restaurer le noeud ayant échoué dans diverses conditions.

Sauvegarde

Bien que le cluster de basculement à haute disponibilité décrit dans ce document fournisse un certain niveau de redondance, il convient toutefois de procéder régulièrement à une sauvegarde traditionnelle de la configuration et des données qui ne peuvent pas facilement être restaurées en cas de perte ou d'altération. La section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel) décrit l'utilisation des outils intégrés de Sentinel pour créer une sauvegarde. Ces outils doivent être utilisés sur le noeud actif dans la grappe car le noeud passif de la grappe n'aura pas accès au périphérique de stockage partagé. D'autres outils de sauvegarde disponibles dans le commerce peuvent être utilisés à la place et peuvent nécessiter une autre configuration en fonction du noeud sur lequel ils peuvent être utilisés.

Récupération

Échec temporaire

Si l'échec est temporaire et que le logiciel et la configuration de l'application et du système d'exploitation ne semblent présenter aucune altération, une simple suppression de l'échec temporaire, par exemple, en redémarrant le noeud, restaure le noeud dans un état opérationnel. L'interface utilisateur de gestion des grappes peut être utilisée pour rétablir l'exécution du service sur le noeud de grappe original, si vous le souhaitez.

Altération du noeud

Si l'échec a entraîné une altération du logiciel ou de la configuration de l'application ou du système d'exploitation présents sur le système de stockage du noeud, le logiciel altéré devra être réinstallé. En répétant les étapes d'ajout d'un noeud à la grappe décrites dans ce document, le noeud est restauré dans un état opérationnel. L'interface utilisateur de gestion des grappes peut être utilisée pour rétablir l'exécution du service sur le noeud de grappe original, si vous le souhaitez.

Configuration des données du cluster

Si l'altération des données survenue sur le périphérique de stockage partagé est telle qu'une récupération est impossible, l'altération affectera l'ensemble du cluster empêchant toute récupération automatique à l'aide du cluster de basculement à haute disponibilité décrit dans ce document. La section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel) décrit l'utilisation des outils intégrés de Sentinel qui permettent de restaurer les données à partir d'une sauvegarde. Ces outils doivent être utilisés sur le noeud actif dans la grappe car le nœud passif de la grappe n'aura pas accès au périphérique de stockage partagé. D'autres outils de sauvegarde et de restauration disponibles dans le commerce peuvent être utilisés à la place et peuvent nécessiter une autre configuration en fonction du nœud sur lequel ils peuvent être utilisés.

VIII Annexes

A Dépannage

Cette section présente certains des problèmes pouvant survenir pendant l'installation, ainsi que les actions à entreprendre pour les résoudre.

Échec de l'installation en raison d'une configuration réseau incorrecte

Au cours du premier démarrage, si le programme d'installation détecte que les paramètres réseau sont incorrects, un message d'erreur s'affiche. Si le réseau est indisponible, l'installation de Sentinel sur l'applicatif échoue.

Pour résoudre ce problème, veuillez configurer correctement les paramètres réseau. Pour vérifier la configuration, utilisez les commandes `ifconfig` et `hostname -f` afin de renvoyer l'adresse IP et le nom d'hôte corrects respectivement.

L'UUID n'est pas créé pour instances Collector Manager avec création d'image ou Correlation Engine

Si vous créez l'image d'un serveur Collector Manager (par exemple, en utilisant l'outil de création d'image ZENWorks) et que vous restaurez les images sur différentes machines, Sentinel n'identifie pas de façon unique les nouvelles instances de Collector Manager. Cela s'explique par la présence d'UUID dupliqués.

Vous devez générer un nouvel UUID en suivant les étapes ci-après sur les systèmes Collector Manager que vous venez d'installer :

1. Supprimez le fichier `host.id` ou `sentinel.id` stocké dans le dossier `/var/opt/novell/sentinel/data`.
2. Redémarrez Collector Manager.

   Collector Manager génère automatiquement l'UUID.

Après la connexion, l'interface principale de Sentinel est vide dans Internet Explorer

Si le niveau de sécurité Internet est réglé sur Haute, une page vierge apparaît après la connexion à Sentinel et la fenêtre contextuelle de téléchargement des fichiers peut être bloquée par le navigateur. Pour éviter ce problème, définissez d'abord le niveau de sécurité sur Moyen-Haut, puis personnalisez-le en procédant comme suit :

1. Accédez à **Outils > Options Internet > Sécurité** et définissez le niveau de sécurité sur **Moyen-Haut**.
2. Vérifiez que dans le menu **Outils, l'option Affichage de compatibilité** n'est pas sélectionnée.
3. Accédez à **Outils > Options Internet > onglet Sécurité > Personnaliser le niveau**, puis faites défiler l'affichage jusqu'à la section **Téléchargements**, sélectionnez **Activer** dans **Demander confirmation pour les téléchargements de fichiers**.

Sentinel ne se lance pas dans Internet Explorer 11 sous Windows Server 2012 R2

Lorsque vous utilisez Windows Server 2012 R2, Sentinel ne se lance pas dans Internet Explorer 11 en raison des configurations de sécurité par défaut d'Internet Explorer 11. Vous devez ajouter manuellement Sentinel à la liste des sites approuvés avant de lancer Sentinel.

Pour ajouter Sentinel à la liste des sites approuvés

1. Ouvrez Internet Explorer 11.
2. Cliquez sur **Paramètres** icône > **Options Internet** > onglet **Sécurité** > **Sites de confiance** > **Sites**
3. Ajoutez un hôte Sentinel à la liste des sites approuvés.

Sentinel ne peut pas exécuter de rapports locaux avec une licence EPS standard

Si votre environnement dispose de la licence EPS 25 par défaut et que vous exécutez un rapport, le rapport échoue avec l'erreur suivante : `License for Distributed Search feature is expired` (la licence pour la fonction de recherche distribuée a expiré).

afin d'exécuter des rapports dans la même machine virtuelle Java que Sentinel, suivez les étapes suivantes :

1. Connectez-vous au serveur Sentinel et ouvrez le fichier `/etc/opt/novell/sentinel/config/obj-component.JasperReportingComponent.properties`.
2. Localisez la propriété `reporting.process.oktorunstandalone`.
3. (Conditionnel) Si la propriété n'est pas dans le fichier, ajoutez-la.
4. Définissez la propriété suivante sur `false`. Par exemple :

   ```
   reporting.process.oktorunstandalone=false
   ```
5. Redémarrez Sentinel.

La synchronisation doit être démarrée manuellement dans Sentinel High Availability après avoir converti le noeud actif en mode FIPS 140-2

Problème : lorsque vous convertissez le noeud actif en mode FIPS 140-2 dans Sentinel HA, la synchronisation visant à convertir tous les noeuds passifs en mode FIPS 140-2 ne s'effectue pas totalement. Vous devez lancer manuellement la synchronisation.

Solution : synchronisez manuellement tous les noeuds passifs vers le mode FIPS 140-2 comme suit :

1. Connectez-vous au noeud actif en tant qu'utilisateur root.
2. Ouvrez le fichier `/etc/csync2/csync2.cfg`.
3. Remplacez la ligne suivante :

   ```
   include /etc/opt/novell/sentinel/3rdparty/nss/*;
   ```

   par

   ```
   include /etc/opt/novell/sentinel/3rdparty/nss;
   ```
4. Enregistrez le fichier `csync2.cfg`.
5. Démarrez la synchronisation manuellement en exécutant la commande suivante :

   ```
   csync2 -x -v
   ```

L'interface principale de Sentinel affiche une page vide après la conversion vers SSDM

Problème : lorsque vous activez SSDM, lorsque vous vous connectez à l'interface principale de Sentinel, le navigateur affiche une page vide.

Solution : fermez votre navigateur, puis reconnectez-vous à l'interface principale de Sentinel. Ce problème ne se produit qu'une seule fois, la première fois que vous vous connectez à l'interface principale de Sentinel après avoir activé SSDM.

Le panneau Champs d'événement est manquant dans la page de planification lors de l'édition de certaines recherches sauvegardées

Problème : lors de l'édition d'une recherche enregistrée mise à niveau de Sentinel 7.2 vers une version ultérieure, le panneau **Champs d'événement**, utilisé pour définir des champs de sortie dans le rapport de recherche CSV, n'apparaît pas dans la page de planification.

Solution : après avoir mis à niveau Sentinel, recréez et replanifiez la recherche pour afficher le panneau **Champs d'événement** dans la page de planification.

Sentinel ne renvoie aucun événement corrélé lorsque vous recherchez des événements pour la règle déployée avec la recherche du nombre de déclenchements par défaut

Problème : Sentinel ne renvoie aucun événement corrélé lorsque vous recherchez tous les événements corrélés qui ont été générés après le déploiement ou l'activation de la règle, en cliquant sur l'icône à côté de **Nombre de déclenchements** du panneau **Statistiques d'activité** de la page Résumé de corrélation concernant la règle.

Solution : remplacez la valeur du champ **De** sur la page Recherche d'événements par une heure moins avancée que celle figurant déjà dans le champ et cliquez à nouveau sur **Rechercher**.

Le tableau de bord Security Intelligence affiche une durée de ligne de base incorrecte lors de la regénération d'une ligne de base

Problème : lors de la regénération de la ligne de base Security Intelligence, les dates de début et de fin de cette ligne sont erronées et affichent le 01/01/1970.

Solution : les bonnes dates sont mises à jour une fois la regénération de la ligne de base terminée.

Le serveur Sentinel s'arrête lors de l'exécution d'une recherche si de nombreux événements figurent dans une seule partition

Problème : le serveur Sentinel s'arrête lorsque vous lancez une recherche si de nombreux événements sont indexés dans une seule partition.

Solution : créez des stratégies de conservation de manière à ce qu'il y ait au moins deux partitions ouvertes par jour. Si vous disposez de plus d'une partition ouverte, cela vous permet de réduire le nombre d'événements indexés dans les partitions.

Vous pouvez également créer des stratégies de conservation qui filtrent les événements en fonction du champ `estzhour`, qui assure le suivi de l'heure. Par conséquent, il vous est possible de mettre en place une stratégie de conservation qui utilise `estzhour:[0 TO 11]` en tant que filtre et une autre stratégie de conservation qui utilise `estzhour:[12 TO 23]` comme filtre.

Pour plus d'informations, reportez-vous à la section « Configuring Data Retention Policies » (Configuration des stratégies de conservation des données) du manuel *Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

Erreur lors de l'utilisation du script report_dev_setup.sh dans la configuration des ports Sentinel pour les exceptions de pare-feu sur les installations d'applicatifs de Sentinel mises à niveau

Problème : Sentinel affiche une erreur lorsque vous utilisez le script `report_dev_setup.sh` afin de configurer les ports Sentinel pour les exceptions de pare-feu.

Solution : configurez les ports Sentinel pour les exceptions de pare-feu en procédant comme suit :

1. Ouvrez le fichier`/etc/sysconfig/SuSEfirewall2`.
2. Remplacez la ligne suivante :

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   par

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Redémarrez Sentinel.

B Désinstallation

Cette annexe fournit des informations sur la désinstallation de Sentinel et les tâches à effectuer après la désinstallation.

Liste de contrôle pour la désinstallation

Utilisez la liste de contrôle suivante pour désinstaller Sentinel :

- ❒ Désinstallez le serveur Sentinel.
- ❒ Désinstallez Collector Manager et Correlation Engine, le cas échéant.
- ❒ Effectuez les tâches de post-désinstallation pour finaliser la désinstallation de Sentinel.

Désinstallation de Sentinel

Un script de désinstallation est disponible ; il vous aidera à supprimer une installation de Sentinel. Avant d'exécuter une nouvelle installation, vous devez effectuer chacune des opérations suivantes pour éviter que des fichiers ou des paramètres système d'une ancienne installation subsistent et nuisent à la nouvelle installation.

AVERTISSEMENT : ces instructions impliquent la modification de fichiers et de paramètres du système d'exploitation. Si ce type d'intervention ne vous est pas familier, contactez l'administrateur système.

Désinstallation du serveur Sentinel

Procédez comme suit pour désinstaller le serveur Sentinel :

1. Connectez-vous au serveur Sentinel en tant qu'utilisateur `root`.

   REMARQUE : un utilisateur non-root ne peut pas désinstaller le serveur Sentinel si l'installation a été effectuée par un utilisateur `root`. Toutefois, l'utilisateur non-root peut désinstaller le serveur Sentinel si l'installation avait été effectuée par un utilisateur non-root.

   ---

2. Accédez au répertoire suivant :

   ```
   <sentinel_installation_path>/opt/novell/sentinel/setup/
   ```

3. Exécutez la commande suivante :

   ```
   ./uninstall-sentinel
   ```

4 Lorsque vous êtes invité à confirmer que vous souhaitez procéder à la désinstallation, appuyez sur o.

   Le script arrête d'abord le service et le supprime ensuite complètement.

Désinstallation de Collector Manager et de Correlation Engine

Procédez comme suit pour désinstaller Collector Manager et Correlation Engine :

1 Connectez-vous en tant qu'utilisateur `root` à l'ordinateur Collector Manager et Correlation Engine.

   REMARQUE : Vous ne pouvez pas désinstaller des instances Collector Manager ou Correlation Engine distantes en tant qu'utilisateur non root si l'installation a été effectuée en tant qu'utilisateur `root`. Un utilisateur non root peut cependant effectuer la désinstallation si l'installation a été réalisée en tant qu'utilisateur non root.

2 Accédez à l'emplacement suivant :

   ```
   /opt/novell/sentinel/setup
   ```

3 Exécutez la commande suivante :

   ```
   ./uninstall-sentinel
   ```

   Le script affiche un avertissement indiquant que Collector Manager ou Correlation Engine, ainsi que toutes les données associées, vont être intégralement supprimés.

4 Saisissez y pour supprimer Collector Manager ou Correlation Engine.

   Le script arrête d'abord le service et le supprime ensuite complètement. Toutefois, les icônes Collector Manager et Correlation Engine affichent toujours un état d'inactivité dans l'interface principale de Sentinel.

5 (Conditionnel) Si vous avez activé la visualisation des événements, vous devez redéployer le plug-in de sécurité Elasticsearch. Pour plus d'informations, reportez-vous à la section « Redéploiement du plug-in de sécurité Elasticsearch » page 86.

6 Effectuez les étapes supplémentaires suivantes pour supprimer manuellement les instances Collector Manager et Correlation Engine de l'interface principale de Sentinel :

   Collector Manager :

   1. Accédez à **Gestion de source d'événements > Vue en direct**.
   2. Cliquez avec le bouton droit de la souris sur l'instance Collector Manager que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

   Correlation Engine :

   1. Accédez à l'**interface principale de Sentinel** en tant qu'administrateur.
   2. Développez l'option **Corrélation**, puis sélectionnez l'instance Correlation Engine à supprimer.
   3. Cliquez sur le bouton **Supprimer** (icône de corbeille).

Désinstallation de NetFlow Collector Manager

Procédez comme suit pour désinstaller NetFlow Collector Manager :

1 Connectez-vous à l'ordinateur sur lequel NetFlow Collector Manager est installé.

REMARQUE : Vous devez vous connecter avec les mêmes droits d'utilisateur que ceux utilisés pour installer NetFlow Collector Manager.

2. Accédez au répertoire suivant :

   ```
   /opt/novell/sentinel/setup
   ```

3. Exécutez la commande suivante :

   ```
   ./uninstall-sentinel
   ```

4. Entrez `y` pour désinstaller Collector Manager.

   Le script arrête d'abord le service, puis le désinstalle complètement.

Tâches ultérieures à la désinstallation

La désinstallation du serveur Sentinel ne supprime pas l'administrateur Sentinel du système d'exploitation. Vous devez supprimer manuellement cet utilisateur.

À l'issue de la désinstallation de Sentinel, certains paramètres système sont conservés. Ils doivent être supprimés avant la nouvelle installation de Sentinel, en particulier si la désinstallation de Sentinel a rencontré des erreurs.

Pour supprimer manuellement les paramètres système Sentinel :

1. Connectez-vous en tant qu'utilisateur `root`.
2. Assurez-vous que tous les processus Sentinel sont arrêtés.
3. Supprimez le contenu du répertoire `/opt/novell/sentinel` ou de tout autre emplacement dans lequel le logiciel Sentinel a été installé.
4. Assurez-vous que personne n'est connecté comme administrateur système Sentinel (novell par défaut), puis supprimez cet utilisateur ainsi que son répertoire privé et son groupe.

   ```
   userdel -r novell
   ```

   ```
   groupdel novell
   ```

5. Redémarrez le système d'exploitation.