NetIQ® Sentinel™

Guide d'installation et de configuration

Février 2015

Mentions légales

Table des matières

À propos de ce guide et de la bibliothèque

Ce *Guide d'installation et de configuration* vous présente NetIQ 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.

À propos de NetIQ Corporation

Fournisseur international de logiciels d'entreprise, nos efforts sont constamment axés sur trois défis inhérents à votre environnement (le changement, la complexité et les risques) et la façon dont vous pouvez les contrôler.

Notre point de vue

Adaptation au changement et gestion de la complexité et des risques : rien de neuf

Parmi les défis auxquels vous êtes confronté, il s'agit peut-être des principaux aléas qui vous empêchent de disposer du contrôle nécessaire pour mesurer, surveiller et gérer en toute sécurité vos environnements informatiques physiques, virtuels et en nuage (cloud computing).

Services métiers critiques plus efficaces et plus rapidement opérationnels

Nous sommes convaincus qu'en proposant aux organisations informatiques un contrôle optimal, nous leur permettons de fournir des services dans les délais et de manière plus rentable. Les pressions liées au changement et à la complexité ne feront que s'accroître à mesure que les organisations évoluent et que les technologies nécessaires à leur gestion deviennent elles aussi plus complexes.

Notre philosophie

Vendre des solutions intelligentes et pas simplement des logiciels

Pour vous fournir un contrôle efficace, nous veillons avant tout à comprendre les scénarios réels qui caractérisent les organisations informatiques telles que la vôtre, et ce jour après jour. De cette manière, nous pouvons développer des solutions informatiques à la fois pratiques et intelligentes qui génèrent assurément des résultats éprouvés et mesurables. En même temps, c'est tellement plus gratifiant que la simple vente de logiciels.

Vous aider à réussir, telle est notre passion

Votre réussite constitue le fondement même de notre manière d'agir. Depuis la conception des produits jusqu'à leur déploiement, nous savons que vous avez besoin de solutions informatiques opérationnelles qui s'intègrent en toute transparence à vos investissements existants. En même temps, après le déploiement, vous avez besoin d'une formation et d'un support continus. En effet, il vous faut un partenaire avec qui la collaboration est aisée... pour changer. En fin de compte, votre réussite est aussi la nôtre.

Nos solutions

- Gouvernance des accès et des identités
- Gestion des accès
- Gestion de la sécurité
- Gestion des systèmes et des applications

- Gestion des charges de travail
- Gestion des services

Contacter le support

Pour toute question concernant les produits, tarifs et fonctionnalités, contactez votre partenaire local. Si vous ne pouvez pas contacter votre partenaire, contactez notre équipe de support ventes.

Monde :	www.netiq.com/about_netiq/officelocations.asp
États-Unis et Canada :	1-888-323-6768
Courrier électronique :	info@netiq.com
Site Web :	www.netiq.com

Contacter le support technique

Pour tout problème spécifique au produit, contactez notre équipe du support technique.

Monde :	www.netiq.com/support/contactinfo.asp
Amérique du Nord et du Sud :	1-713-418-5555
Europe, Moyen-Orient et Afrique:	+353 (0) 91-782 677
Courrier électronique :	support@netiq.com
Site Web :	www.netiq.com/support

Contacter le support en charge de la documentation

Notre objectif est de vous proposer une documentation qui réponde à vos besoins. Si vous avez des suggestions d'améliorations, cliquez sur le bouton **Add Comment** (Ajouter un commentaire) au bas de chaque page dans les versions HTML de la documentation publiée à l'adresse www.netiq.com/documentation. Vous pouvez également envoyer un message électronique à l'adresse Documentation-Feedback@netiq.com. Nous accordons une grande importance à vos commentaires et sommes impatients de connaître vos impressions.

Contacter la communauté d'utilisateurs en ligne

La communauté en ligne de NetIQ, Qmunity, est un réseau collaboratif vous mettant en relation avec vos homologues et des spécialistes de NetIQ. En proposant des informations immédiates, des liens utiles vers des ressources et un accès aux experts NetIQ, Qmunity vous aide à maîtriser les connaissances nécessaires pour tirer pleinement parti du potentiel de vos investissements informatiques. Pour plus d'informations, consultez le site http://community.netiq.com.

Présentation de Sentinel

Cette section explique de manière détaillée en quoi consiste Sentinel et comment cette application fournit une solution de gestion des événements à votre organisation.

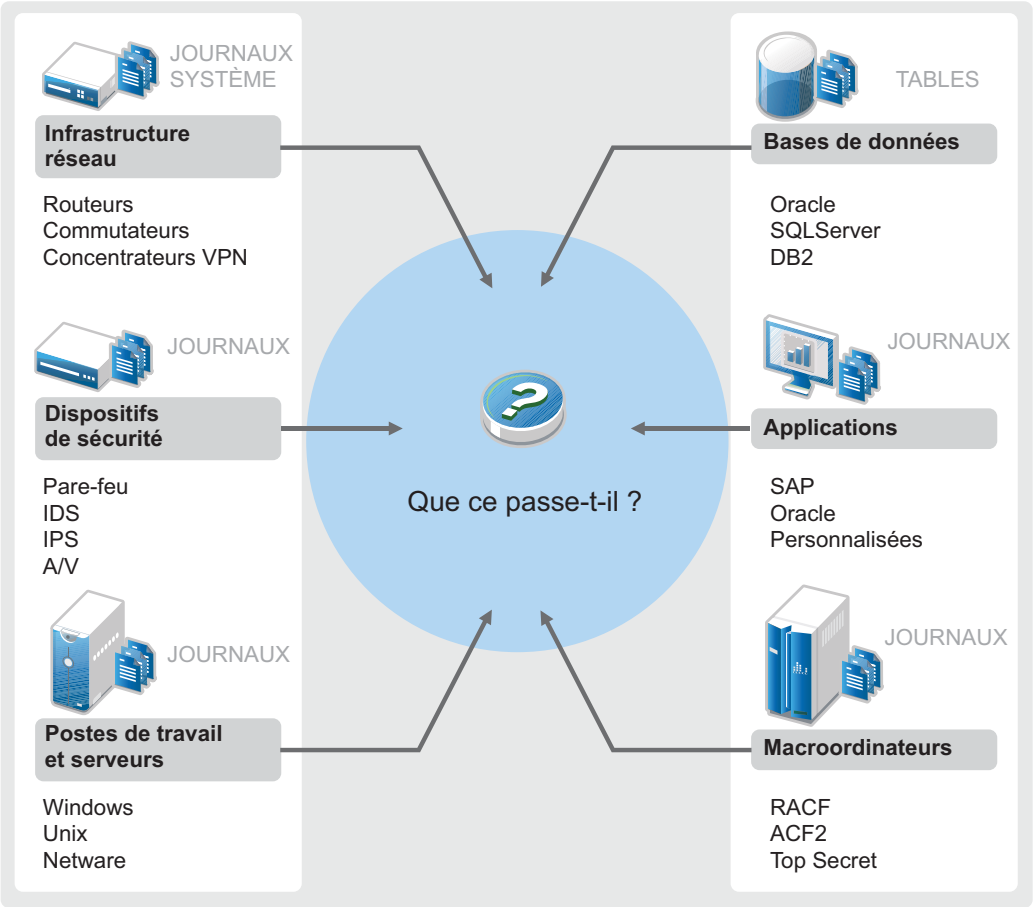
1 Qu'est-ce que Sentinel ?

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

1.1 Défis liés à la sécurisation d'un environnement informatique

Compte tenu de la complexité de votre environnement informatique, sa sécurisation constitue un véritable défi. Il compte en effet de nombreux macroordinateurs, applications, bases de données, postes de travail et serveurs divers qui comportent tous des journaux d'événements. À cela, il faut ajouter les périphériques de sécurité et d'infrastructure réseau, qui contiennent tous des journaux dans lesquels sont consignés les événements qui se produisent dans votre environnement informatique.

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



Les défis surviennent pour les raisons suivantes :

- Votre environnement informatique compte de nombreux périphériques.
- Les journaux sont dans différents formats.
- Les journaux sont stockés dans des silos.
- La quantité d'informations générées dans les journaux.
- L'impossibilité de déterminer les auteurs des différentes tâches sans analyse manuelle de l'ensemble des journaux.

Pour que ces informations soient exploitables, vous devez pouvoir 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 sont pas conformes aux normes.

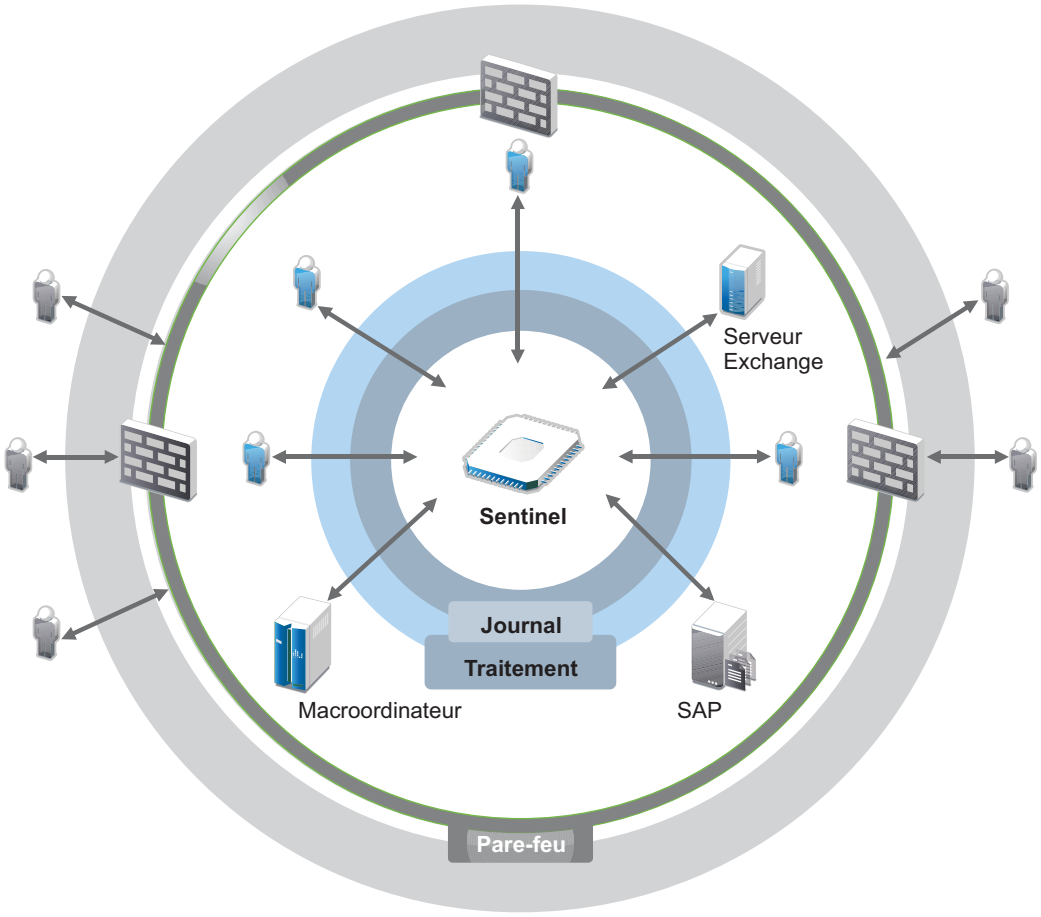
- Prendre des mesures afin de garantir la conformité aux stratégies d'entreprise.
- Générer des rapports pour prouver la conformité.

Après avoir compris les défis liés à la sécurisation de votre environnement informatique, vous devez déterminer comment, d'une part, assurer la sécurité des utilisateurs, et d'autre part, protéger votre entreprise contre les utilisateurs sans les traiter comme s'ils étaient mal intentionnés ou les accabler à tel point qu'ils ne puissent plus être productifs. Sentinel offre la solution.

1.2 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*



Vous savez ainsi à tout moment ce qui se passe dans votre environnement et pouvez identifier qui a réalisé des opérations sur certaines ressources. Cela vous permet de déterminer le comportement des utilisateurs et de surveiller efficacement les contrôles. Que ces personnes soient ou non des utilisateurs internes, vous pouvez corréler l'ensemble de leurs opérations, de manière à identifier les activités non autorisées avant qu'elles n'aient des conséquences néfastes.

Sentinel est une solution économique pour les raisons suivantes :

- fournit une solution unique permettant de surveiller les divers contrôles informatiques et de se conformer à plusieurs réglementations ;.
- comble le vide existant entre ce qui devrait théoriquement se passer dans votre environnement réseau et ce qui se passe réellement ;
- prouve aux auditeurs et aux régulateurs que votre organisation documente, surveille et établit des rapports sur les contrôles de sécurité ;
- offre une solution de surveillance de la conformité et des programmes de création de rapports prêts à l'emploi ;
- permet d'obtenir la visibilité et le contrôle nécessaires pour évaluer en continu l'efficacité des programmes de conformité et de sécurité de votre entreprise.

Sentinel automatise les processus de création de rapports, d'analyse et de collecte des 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, et fournit les contrôles informatiques qui vous permettent d'entreprendre une action immédiate en cas de violation de sécurité ou d'événement non conforme. En récapitulant des informations sur votre environnement, Sentinel vous permet également de communiquer aux principales parties prenantes votre stratégie globale en matière de sécurité.

2 Fonctionnement de Sentinel

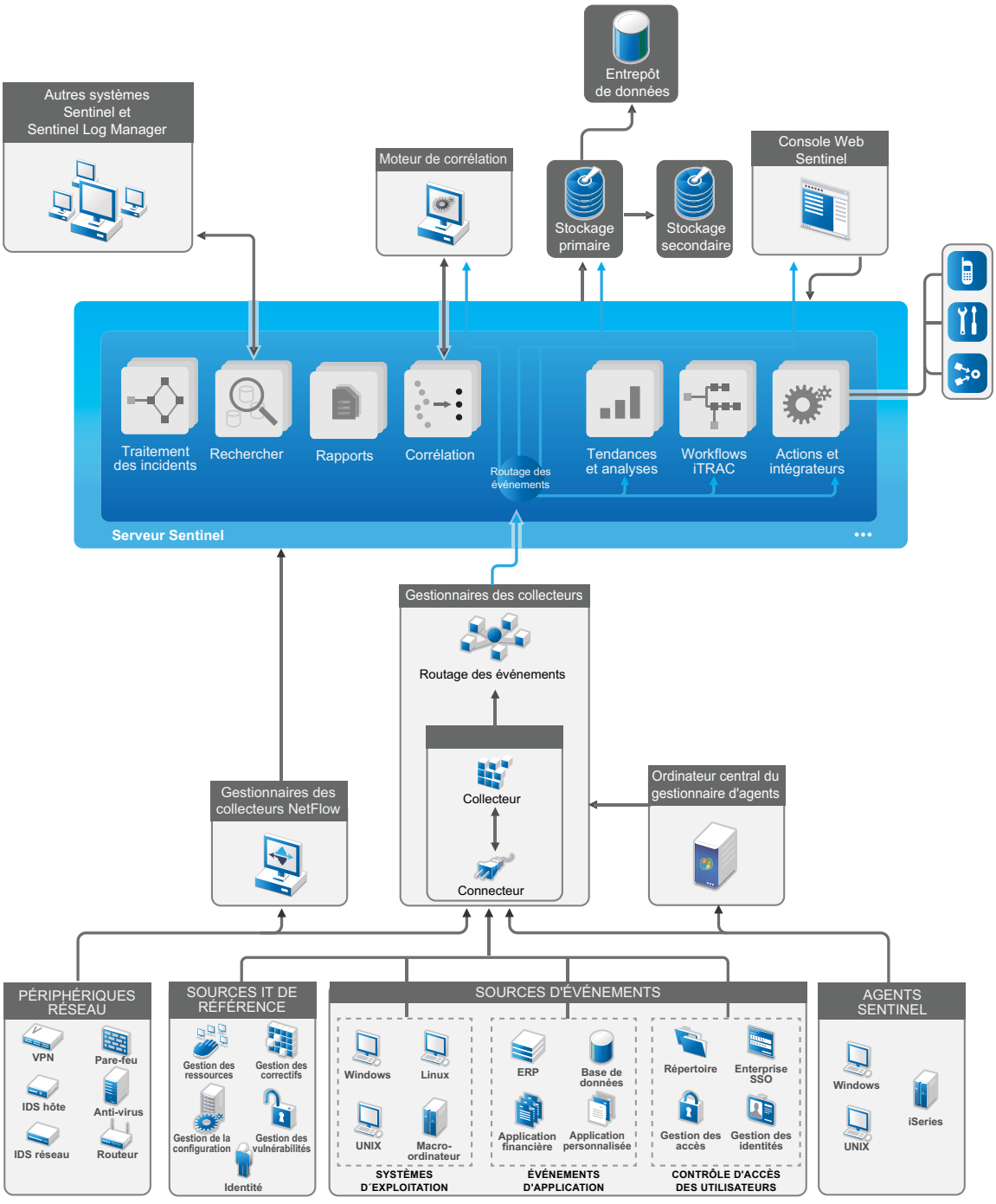
Sentinel gère en permanence les informations de sécurité et les événements dans tout votre environnement informatique afin de vous offrir une solution de surveillance complète.

Sentinel effectue les opérations suivantes :

- collecte les journaux, événements et informations de sécurité de l'ensemble des sources d'événements de votre environnement informatique ;
- uniformise le format des journaux, événements et informations de sécurité collectés ;
- stocke les événements dans une zone de stockage de fichiers avec des stratégies de conservation des données personnalisables ;
- collecte les données de flux réseau et vous aide à effectuer une surveillance approfondie des activités réseau ;
- permet de lier de manière hiérarchique plusieurs systèmes Sentinel dont Sentinel Log Manager ;
- permet de rechercher des événements non seulement sur votre serveur Sentinel local, mais aussi sur d'autres serveurs Sentinel situés aux quatre coins du globe ;
- effectue une analyse statistique qui vous permet de définir une ligne de base, puis de la comparer à la situation réelle afin de déterminer s'il existe des problèmes non identifiés ;
- met en corrélation un ensemble d'événements similaires ou comparables sur une période donnée, afin de déterminer 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 ci-dessous illustre le fonctionnement de Sentinel :

Figure 2-1 *Architecture de Sentinel*



Les sections suivantes décrivent en détail les composants Sentinel :

- Section 2.1, « Sources d'événements », page 21
- Section 2.2, « Événement Sentinel », page 21
- Section 2.3, « Gestionnaire des collecteurs. », page 23
- Section 2.4, « Agent Manager », page 24

2.1 Sources d'événements

Sentinel collecte les événements et informations de sécurité à partir de nombreuses sources diverses de votre environnement informatique. Ces sources, appelées sources d'événements, peuvent correspondre à de nombreux éléments de votre réseau.

Périmètre de sécurité : périphériques de sécurité y compris le matériel et les logiciels utilisés pour créer un périmètre de sécurité pour votre environnement, tels que des pare-feux, des IDS et des VPN.

Systèmes d'exploitation : événements des 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.

Événements d'applications : événements générés par les applications installées sur le réseau.

Contrôle d'accès des utilisateurs : événements générés par les applications ou périphériques qui permettent à des utilisateurs d'accéder aux ressources de l'entreprise.

Pour plus d'informations sur la collecte d'événements depuis des sources d'événements, consultez la section « Configuring Agentless Data Collection » (Configuration de la collecte de données sans agent).

2.2 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. L'ajout d'informations de catégorie (taxonomie) à des événements facilite leur comparaison, notamment lorsqu'ils sont issus de systèmes dont le mode de signalisation est différent. Par exemple, l'authentification échoue. Les événements sont traités par l'affichage en temps réel, le moteur de corrélation, les tableaux de bord et le serveur dorsal.

Un événement comprend plus de 200 champs. Les champs d'événement sont de types différents et ont des fonctions différentes. Certains sont prédéfinis, tels que ceux relatifs à la gravité, à la sévérité, à l'IP de destination et au port de destination. Il existe deux ensembles de champs configurables : d'une part, les champs réservés, destinés à l'usage interne de Sentinel pour permettre le développement futur du produit et, d'autre part, les champs client, destinés aux extensions client.

Il est possible d'attribuer une nouvelle fonction aux champs en les renommant. La source d'un champ peut être externe, auquel cas le champ est défini explicitement par le périphérique ou le collecteur ou référentiel correspondant. 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 pour être le code de génération du bâtiment contenant les ressources mentionnées comme IP de destination d'un événement, ou bien encore, un champ peut être défini par le service d'assignation à l'aide d'une assignation définie par le client utilisant l'IP de destination de l'événement.

- Section 2.2.1, « Service d'assignation », page 22
- Section 2.2.2, « Acheminement des assignations », page 22
- Section 2.2.3, « Détection d'exploitation (service d'assignation) », page 22

2.2.1 Service d'assignation

Le service d'assignation permet à un mécanisme sophistiqué de propager les données pertinentes pour l'entreprise sur le système. Ces données peuvent enrichir les événements d'informations de référence qui fourniront le contexte nécessaire aux analystes : les décisions prises sont plus pertinentes, les rapports plus utiles et les règles de corrélation mûrement réfléchies.

Vous pouvez enrichir les données d'événement à l'aide d'assignations afin d'ajouter des informations détaillées sur l'hôte et sur l'identité aux événements entrants qui proviennent des périphériques source. Ces informations supplémentaires peuvent être utilisées pour les opérations avancées de corrélation et de création de rapports. Le système prend en charge plusieurs assignations intégrées, ainsi que des assignations 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 à l'aide d'API dans le code du collecteur, puis sont exportées automatiquement vers le service d'assignation.
- Les assignations personnalisées sont stockées sous forme de 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 gestionnaire des collecteurs et appliquées localement. Ce processus distribué garantit que l'assignation ne surcharge pas le serveur principal.

2.2.2 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. Cette capacité d'acheminement s'avère particulièrement précieuse dans un système en temps réel critique tel que Sentinel, où doit exister un mouvement des données régulier, prédictif, flexible et indépendant des charges temporaires du système.

2.2.3 Détection d'exploitation (service d'assignation)

Sentinel permet de recouper des signatures de données d'événement avec les données d'analyse de vulnérabilité. Les utilisateurs sont notifiés automatiquement et immédiatement lorsqu'une attaque tente d'exploiter un système vulnérable. Ceci est réalisé au moyen des éléments suivants :

- Données de flux Advisor

- Détection d'intrusion
- Analyse de la vulnérabilité
- pare-feux

Advisor fournit une référence croisée entre les signatures de données d'événement et les données de scanner de vulnérabilité. 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. Pour plus d'informations sur Advisor, reportez-vous à la section « Detecting Vulnerabilities and Exploits » (Détection des vulnérabilités et des Exploits) du manuel *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

2.3 Gestionnaire des collecteurs.

Le gestionnaire des collecteurs gère la collecte des données, surveille les messages d'état du système et filtre les événements selon les besoins. Ses principales fonctions sont les suivantes :

- conversion des événements ;
- ajout de pertinence aux événements par l'intermédiaire du service d'assignation ;
- routage des événements ;
- détermination des données en temps réel, de vulnérabilité, de ressources ou des données ne nécessitant pas de transmission en temps réel ;
- envoi de messages d'état de santé au serveur Sentinel.

2.3.1 Collecteurs

Les collecteurs uniformisent et collectent les informations des connecteurs. Les collecteurs sont écrits en JavaScript et définissent la logique des opérations suivantes :

- réception des données brutes envoyées par les connecteurs ;
- analyse et normalisation des données ;
- application d'une logique reproductible aux données ;
- conversion des données spécifiques des périphériques en données propres à Sentinel ;
- formatage des événements ;
- transmission des données uniformisées, analysées et formatées au gestionnaire des collecteurs ;
- filtrage des événements selon le périphérique.

Pour plus d'informations sur les collecteurs, consultez le site Web des plug-ins Sentinel.

2.3.2 Connecteurs

Les connecteurs permettent de connecter les sources d'événements au système Sentinel. Les connecteurs utilisent des protocoles standard du secteur pour obtenir les événements tels que Syslog, JDBC pour lire les données des tables de base de données, WMI pour lire les journaux des événements Windows (Windows Event), etc. Les connecteurs permettent d'effectuer les opérations suivantes :

- acheminer des données d'événement brutes depuis les sources d'événement jusqu'au collecteur ;

- filtrer les connexions de manière spécifique ;
- gérer les erreurs de connexion.

2.4 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 non disponibles à partir du 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 et de disposer d'un point de collecte pour les événements acheminés vers Sentinel. Pour plus d'informations sur Agent Manager, reportez-vous à la documentation correspondante.

2.5 Gestionnaire des collecteurs NetFlow

Le gestionnaire des collecteurs NetFlow collecte des données de flux réseau (NetFlow, IPFIX, etc.) à partir de périphériques réseau tels que des routeurs, des commutateurs et des pare-feu. Ces données décrivent des informations de base sur toutes les connexions réseau établies entre les hôtes, y compris les paquets et les octets transmis, ce qui vous aide à visualiser le comportement des différents hôtes ou de l'ensemble du réseau.

La fonctionnalité Gestionnaire des collecteurs NetFlow effectue les opérations suivantes :

- Collecte des données de flux réseau dans les octets, flux et paquets des périphériques réseau pris en charge.
- Agrégation et envoi des données collectées au serveur Sentinel en vue de la visualisation et de l'analyse des activités réseau au sein de votre environnement.

Pour plus d'informations sur la visualisation et l'analyse des données de flux réseau, reportez-vous à la section « Visualizing and Analyzing Network Flow Data » (Visualisation et analyse des données de flux réseau) du *NetIQ Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

2.6 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 deux flux de données distincts, mais liés, en provenance des gestionnaires de collecteurs : les données d'événement analysées et les données brutes. Les données brutes sont immédiatement stockées dans des partitions protégées pour fournir une chaîne de preuves sécurisée. Les données d'événement analysées sont routées en fonction des règles que vous définissez. Vous pouvez les filtrer, les envoyer dans l'espace de stockage, les analyser en temps réel et les router vers des systèmes externes. Toutes les données d'événement envoyées dans l'espace de stockage sont ensuite mises en correspondance avec les stratégies de conservation définies par l'utilisateur qui déterminent la partition dans laquelle ces données sont placées, ainsi que la stratégie de nettoyage qui s'applique avant leur suppression.

Le stockage des données Sentinel repose sur une structure à 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 les sauvegarder dans un stockage hors ligne tel que Amazon Glacier. Au besoin, vous pouvez réimporter temporairement les partitions à des fins d'analyse légale à long terme.

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 Storage (Configuration du stockage de données) » du manuel *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

2.7 Corrélation

Un seul événement peut paraître insignifiant, mais associé à d'autres événements, il peut vous avertir d'un éventuel problème. Sentinel vous aide à mettre en corrélation ces événements à l'aide de règles que vous créez et déployez dans le moteur de corrélation, et à effectuer l'opération adéquate pour atténuer les problèmes.

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, reportez-vous à la section « Correlating Event Data » (Corrélation de données d'événement) du manuel *NetIQ Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

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

2.8 Security Intelligence

La fonction de corrélation de Sentinel permet de rechercher des modèles connus d'activité, que ce soit pour la sécurité, la conformité ou d'autres raisons. La fonction Security Intelligence recherche toute activité extraordinaire qui pourrait être malveillante, mais ne met en corrélation 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'étudier les écarts (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 *NetIQ Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

2.9 Réparation d'incident

Sentinel fournit un système de gestion automatisée des réponses en cas d'incidents qui vous permet de documenter et de formaliser le processus de suivi, de réaffectation et de réponse aux incidents et violations de stratégies, et qui garantit une intégration bilatérale 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 *NetIQ Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

2.10 Flux de travail 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 suivre les problèmes système ou de sécurité, depuis leur identification (via des règles de corrélation ou par identification manuelle) jusqu'à leur résolution.

Les workflows peuvent être créés manuellement ou automatiquement. Des fonctions avancées, telles que la création de branche, les demandes d'intervention basées sur l'heure et les variables locales, sont prises en charge. 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 *NetIQ Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

2.11 Opérations et intégrateurs

Les opérations exécutent manuellement ou automatiquement certains types d'actions, tels que l'envoi d'un message électronique dans Sentinel. Elles peuvent être déclenchées par des règles de routage, par l'exécution manuelle d'une opération d'événement ou d'incident et par 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 *NetIQ 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

2.12 Recherches

Sentinel propose une option permettant d'effectuer une recherche sur des événements. La recherche peut porter sur les données de l'emplacement de stockage primaire ou secondaire. 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 « Performing a Search » (Réalisation d'une recherche) dans le manuel *NetIQ Sentinel User Guide* (Guide d'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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

2.13 Rapports

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

Vous pouvez exécuter et planifier des rapports, mais aussi les envoyer par message électronique au format PDF. Vous pouvez également exécuter les rapports comme s'il s'agissait d'une simple recherche pour ensuite interagir avec 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 *NetIQ Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

2.14 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. Grâce à l'affichage des informations sur les utilisateurs à l'origine d'une opération ou affectés par une opération, les temps de réponse aux incidents sont améliorés et l'analyse basée sur les comportements est activée. Pour plus d'informations, reportez-vous à la section « Leveraging Identity Information » (Utilisation des informations sur l'identité) du manuel *NetIQ Sentinel User Guide* (Guide de l'utilisateur de NetIQ Sentinel).

2.15 Analyse d'événements

Sentinel fournit un ensemble puissant d'outils qui vous permettent de rechercher et d'analyser facilement les données d'événement critiques. Le système est réglé et optimisé pour offrir la meilleure efficacité dans un type donné d'analyse, ainsi que des méthodes permettant d'effectuer en toute transparence la transition d'un type d'analyse à un autre.

Les investigations dans les événements dans Sentinel commencent souvent par la visualisation presque en temps réel dans Active Views. Il existe des outils plus élaborés, mais les flux d'événements filtrés et les graphiques récapitulatifs affichés dans Active Views permettent de réaliser des analyses simples et globales des tendances et des données d'événement, ainsi que d'identifier des événements spécifiques. Avec le temps, vous créez des filtres personnalisés pour des classes de données spécifiques telles que la sortie depuis la corrélation. Vous pouvez utiliser Active Views comme un tableau de bord qui présente la stratégie globale d'utilisation et de sécurité.

La recherche interactive permet alors d'effectuer une analyse plus 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 particulier. En cliquant sur les données d'événement ou en utilisant le panneau de filtrage à gauche, vous pouvez rapidement accéder aux événements spécifiques.

Lors de l'analyse de centaines d'événements, les fonctionnalités de création de rapport 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 élaborées dans l'interface de recherche dans un modèle de création de rapport. Ce dernier crée instantanément un rapport qui affiche les mêmes données, mais dans un format plus adapté aux grands nombres d'événements.

Sentinel comprend de nombreux modèles à cette fin. Certains modèles sont définis de manière à afficher des types particuliers d'informations telles que les données d'authentification ou la création d'un utilisateur. D'autres modèles sont génériques et vous permettent de personnaliser les groupes et colonnes du rapport de manière interactive.

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

II Planification de votre installation Sentinel

Cette section vous explique les points de planification à prendre en considération avant d'installer Sentinel. Si vous souhaitez effectuer une configuration qui n'est pas abordée dans les sections suivantes ou pour toute question, contactez le support technique de NetIQ.

3 Liste de contrôle pour la mise en œuvre

Utilisez la liste de contrôle suivante pour la planification, l'installation et la configuration de Sentinel :

❒	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 le système 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 33.
❒	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 37.
❒	Consultez le nombre d'événements par seconde (EPS) du moteur de corrélation et du gestionnaire des collecteurs, ainsi que les enregistrements par seconde (RPS) du gestionnaire des collecteurs NetFlow. Déterminez le nombre de gestionnaires de collecteurs, de moteurs de corrélation et de gestionnaires des collecteurs NetFlow que vous devez installer pour améliorer les performances et l'équilibrage de la charge.	Section 6.1, « Avantages des déploiements distribués », page 39.
❒	Consultez les 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 63.
❒	Veillez à configurer l'heure sur le serveur Sentinel.	Chapitre 17, « Configuration de l'heure », page 99.
❒	Lorsque vous installez Sentinel, les plug-ins disponibles au moment de la sortie de Sentinel sont installés par défaut. Configurez les plug-ins prêts à l'emploi à utiliser pour la collecte des données et la création de rapports.	Chapitre 19, « Configuration des plug-ins prêts à l'emploi », page 107.

❒	Tâches	Voir
❒	Sentinel s'accompagne de 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 de Sentinel.
❒	Installez les collecteurs et connecteurs supplémentaires nécessaires dans votre environnement.	Chapitre 15, « Installation de collecteurs et de connecteurs supplémentaires », page 93.
❒	Installez les gestionnaires des collecteurs et les moteurs de corrélation supplémentaires nécessaires dans votre environnement.	Section 12.4, « Installation de gestionnaires des collecteurs et de moteurs de corrélation », page 73.

4 Présentation des informations de licence

La plate-forme Sentinel comprend un large éventail de fonctionnalités, car les besoins sont différents d'un client à l'autre. NetIQ propose des modèles d'octrois de licence variés pour répondre à tous les besoins.

Avant la version 7.3 de Sentinel, la plate-forme Sentinel de base se composait de deux produits distincts : Sentinel et Sentinel Log Manager. À partir de Sentinel 7.3, NetIQ propose les deux produits en tant que plate-forme unique pour améliorer son offre de nouvelles fonctionnalités, de nouveaux correctifs, de documentation et de support, tout en permettant aux clients de sélectionner la solution dont les fonctionnalités sont les mieux adaptées à leurs besoins.

La plate-forme Sentinel regroupe deux solutions principales :

- **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 est dédié aux cas d'utilisation SIEM tels que la détection des menaces, des alertes et la correction des problèmes en temps réel.
- **Sentinel for Log Management :** une solution adaptée aux cas d'utilisation de la gestion des journaux comme la possibilité de collecter, stocker, effectuer des recherches et créer des rapports sur les données.

  Sentinel for Log Management 7.3 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 7.3, consultez la FAQ disponible à l'adresse https://www.netiq.com/products/sentinel/frequently-asked-questions/slm122-to-slm73-upgrade-faqs.html.

NetIQ fournit des licences distinctes pour chacune de ces solutions. Selon la clé de licence que vous ajoutez, la solution correspondante est activée. D'autres éléments relatifs à l'octroi de licences Sentinel, tels que le nombre d'EPS, le nombre de périphériques autorisés et les plug-ins nécessitent des licences supplémentaires. Pour plus de détails, reportez-vous à votre accord de licence utilisateur final.

Le tableau suivant présente les services et fonctions spécifiques à chacune des solutions :

Tableau 4-1 *Services et fonctions Sentinel*

Services et fonctions	Sentinel Enterprise	Sentinel for Log Management
Fonctionnalité principale	Oui	Oui
◆ Collecte d'événements de base ◆ Collecte de données non liées aux événements (ressources, vulnérabilités, identités) ◆ Analyse et normalisation ◆ Classification taxinomique des données d'événement ◆ Assignation contextuelle en ligne ◆ Collecte et stockage NetFlow ◆ Visualisation NetFlow en temps réel ◆ Visualisation NetFlow basée sur les événements ◆ Recherche d'événements (localement) ◆ Création de rapports sur les événements ◆ Filtrage des événements ◆ Visualisation des événements en temps réel ◆ Stockage d'événements ◆ Stratégies de conservation des données ◆ Non-rejet de la banque d'événements ◆ Activation FIPS ◆ Opérations déclenchées manuellement ◆ Création et gestion manuelles des incidents ◆ Opérations et workflows liés aux incidents ◆ Workflows iTRAC		
Opérations	Oui	Oui
◆ Opérations déclenchées par la corrélation (uniquement si la corrélation est activée) ◆ Opérations déclenchées par les règles de routage (uniquement si les règles sont activées) ◆ Opérations déclenchées manuellement		
Règles de routage	Oui	Oui
◆ Routage d'événement (externe) ◆ Opérations déclenchées par les règles de routage (uniquement si les opérations sont activées)		
Lien Sentinel	Oui	Oui

Services et fonctions	Sentinel Enterprise	Sentinel for Log Management
Corrélation ◆ Corrélation de modèles en temps réel ◆ Opérations déclenchées par les règles de corrélation (uniquement si les opérations sont activées) ◆ Triage des alertes ◆ Tableaux de bord des alertes	Oui	Non
Synchronisation des données	Oui	Oui
Restauration des données d'événements à partir des archives	Oui	Oui
Fédération des données (recherche distribuée)	Oui	Oui
Security Intelligence ◆ Règles d'anomalie ◆ Analyse statistique en temps réel	Oui	Non
Analyse statistique en temps réel	Oui	Non
Expiration de la licence	Jamais	Jamais
Limite du nombre d'EPS	Illimité	Illimité

4.1 Licences Sentinel

Cette section fournit des informations sur les différentes licences Sentinel.

4.1.1 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 nombre 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 34.

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 adapte la date d'expiration en conséquence.

Une fois la licence d'évaluation arrivée à expiration, le système s'exécute avec une clé de licence de base qui offre un ensemble restreint de fonctionnalités et un nombre d'événements limité à 25 EPS. La licence de base est également connue sous le nom de licence gratuite.

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.

4.1.2 Licence gratuite

La licence gratuite vous permet d'utiliser un ensemble restreint de fonctionnalités et un nombre d'événements limité à 25 EPS. Elle n'a pas de date d'expiration.

La licence gratuite vous permet de collecter et de stocker des événements. Lorsque le nombre 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 : NetIQ ne fournit pas de support technique ni de mises à jour de produits pour la version gratuite de Sentinel.

4.1.3 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 certain taux de collecte des données, certaines fonctions et sources d'événements. Certaines clauses 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 *NetIQ 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, il est recommandé de consulter les services NetIQ Consulting ou un partenaire NetIQ Sentinel avant de finaliser l'architecture Sentinel.

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 concernant NetIQ Sentinel.

5.1 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 concernant le connecteur et le collecteur sur la page Web des plug-ins de Sentinel.

5.2 Environnement virtuel

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

Pour accéder aux recommandations concernant la machine physique, consultez le Chapitre 5, « Configuration du système », page 37.

6 Considérations sur le déploiement

Sentinel dispose d'une architecture évolutive qui peut gérer la charge que vous devez y placer. Vous pouvez placer sur Sentinel plusieurs types de charge. Ce chapitre présente les points essentiels à prendre en compte lors de l'évolution d'un déploiement Sentinel. Un spécialiste NetIQ Services ou NetIQ Partner Services peut vous aider à concevoir en détail le système complet de votre environnement personnalisé.

6.1 Avantages des déploiements distribués

Par défaut, le serveur Sentinel comprend les composants suivants :

- **Gestionnaire des collecteurs :** il fournit un point flexible de collecte de données pour Sentinel. Le programme d'installation de Sentinel installe un gestionnaire des collecteurs par défaut pendant l'installation.
- **Moteur de corrélation :** 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.
- **Gestionnaire des collecteurs NetFlow :** Le gestionnaire des collecteurs NetFlow collecte des données de flux réseau (NetFlow, IPFIX, etc.) à partir de périphériques réseau tels que des routeurs, des commutateurs et des pare-feu. Ces données décrivent des informations de base sur toutes les connexions réseau établies entre les hôtes, y compris les paquets et les octets transmis, ce qui vous aide à visualiser le comportement des différents hôtes ou de l'ensemble du réseau.

IMPORTANT : Pour les environnements de production, NetIQ Corporation recommande de 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.

6.1.1 Avantages de l'installation de gestionnaires des collecteurs supplémentaires

Par défaut, le serveur Sentinel comprend un gestionnaire des collecteurs. Cependant, pour les environnements de production, les gestionnaires de collecteurs distribués assurent un isolement bien supérieur lors de la réception de gros volumes de données. Dans ce cas, même si le gestionnaire des collecteurs distribué est surchargé, le serveur Sentinel continue de répondre aux demandes de l'utilisateur.

L'installation de plusieurs gestionnaires des collecteurs dans un réseau distribué présente plusieurs avantages :

- **Des performances système améliorées :** les gestionnaires des collecteurs 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 gestionnaires des collecteurs 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 gestionnaires des collecteurs 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 gestionnaires des collecteurs supplémentaires aux emplacements appropriés sur votre réseau. Ces gestionnaires des collecteurs distants 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 de gestionnaires des collecteurs supplémentaires, reportez-vous à la Section 12.4, « Installation de gestionnaires des collecteurs et de moteurs de corrélation », page 73.

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

6.1.2 Avantages des moteurs de corrélation supplémentaires

Vous pouvez déployer plusieurs moteurs de corrélation, chacun sur son propre serveur, sans devoir répliquer de configurations ni ajouter des bases de données. Pour les environnements comptant un nombre élevé de règles de corrélation ou des taux d'événements extrêmement élevés, vous aurez peut-être avantage à installer plusieurs moteurs de corrélation et à redéployer certaines règles sur les nouveaux moteurs de corrélation. Ces moteurs de corrélation supplémentaires permettent de s'adapter à mesure que le système Sentinel intègre de nouvelles sources de données ou que les taux d'événement augmentent. Pour plus d'informations sur l'installation de moteurs de corrélation supplémentaires, consultez le site Section 12.4, « Installation de gestionnaires des collecteurs et de moteurs de corrélation », page 73.

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

6.1.3 Avantages des gestionnaires des collecteurs NetFlow supplémentaires

Le gestionnaire des collecteurs NetFlow collecte les données de flux réseau en provenance de périphériques réseau. Il est conseillé d'installer des gestionnaires de collecteurs NetFlow supplémentaires au lieu d'utiliser le gestionnaire des collecteurs NetFlow sur le serveur Sentinel, afin de permettre aux ressources système de se consacrer à d'autres fonctions importantes, telles que les recherches et le stockage d'événements.

Vous pouvez installer des gestionnaires de collecteurs NetFlow supplémentaires dans les cas suivants :

- Dans les environnements comprenant de nombreux périphériques réseau et des débits élevés de données de flux réseau, vous pouvez installer plusieurs gestionnaires de collecteurs NetFlow afin de répartir la charge.
- Dans un environnement multi-locataire, vous devez installer un gestionnaire des collecteurs NetFlow pour chaque locataire afin de collecter des données de flux réseau distinctes par locataire.

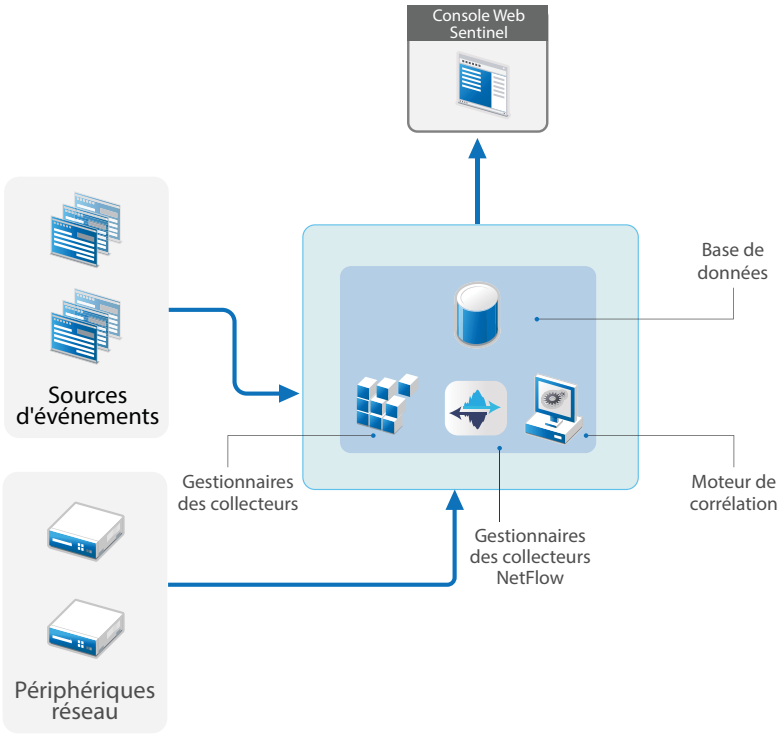
Pour obtenir des informations sur l'installation de gestionnaires des collecteurs NetFlow supplémentaires, reportez-vous au Chapitre 14, « Installation du gestionnaire des collecteurs NetFlow », page 89.

6.2 Déploiement tout-en-un

L'option de déploiement de base est celle d'un système tout-en-un contenant tous les composants Sentinel sur une même machine. Un déploiement tout-en-un convient uniquement si la charge du système est relativement faible et si vous ne devez pas surveiller de machines Windows. Dans de nombreux environnements, des charges variables et imprévisibles, ainsi que des conflits de ressources mineurs entre différents composants peuvent entraîner des problèmes de performances.

IMPORTANT : Pour les environnements de production, NetIQ Corporation recommande de 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 6-1 *Déploiement tout-en-un*

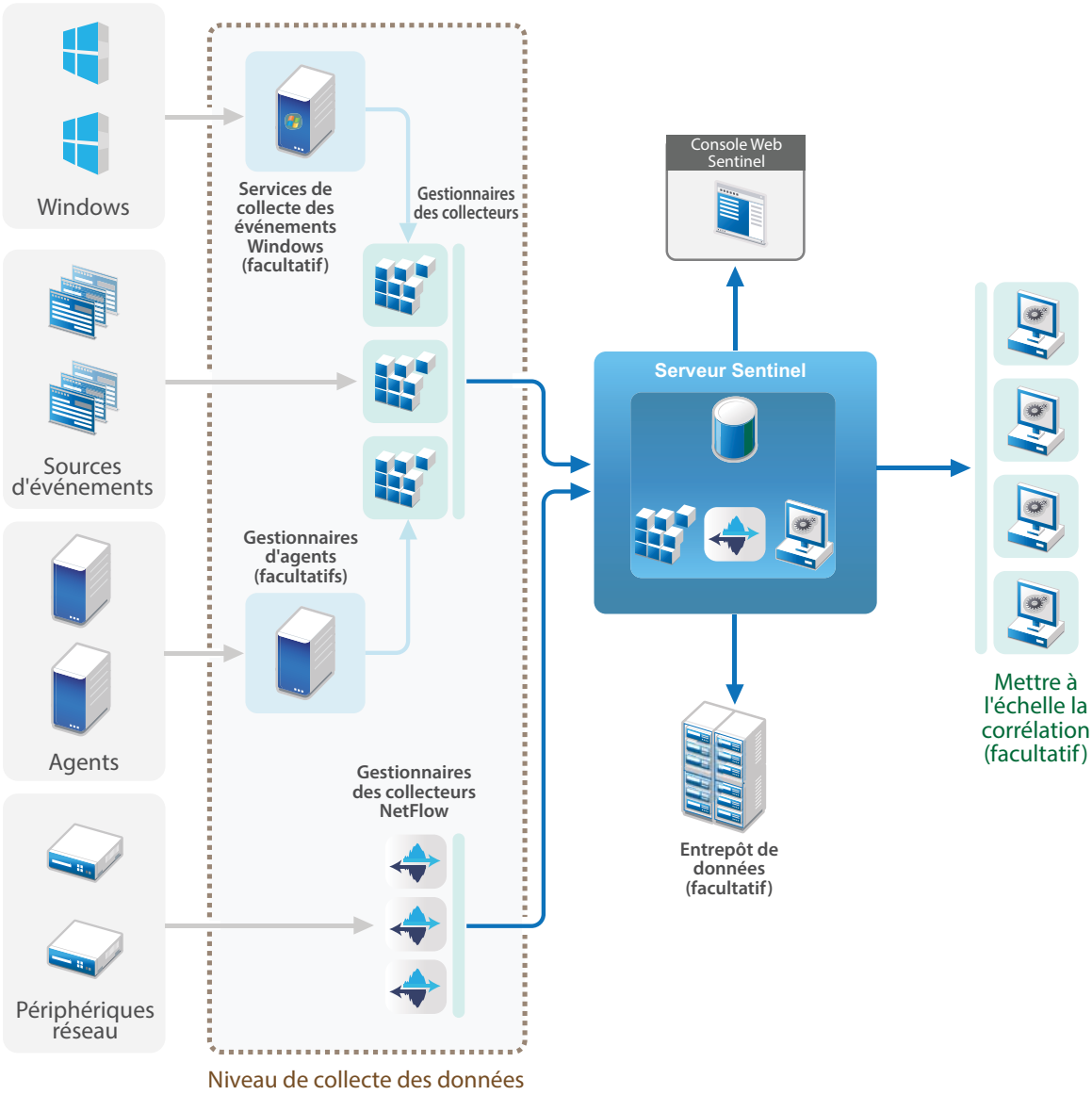


6.3 Déploiement distribué en un niveau

Le déploiement en un niveau permet de surveiller les machines Windows et de gérer des charges plus importantes que le déploiement tout-en-un. La collecte et la mise en corrélation des données peuvent faire l'objet d'une évolutivité horizontale par l'ajout de gestionnaires des collecteurs, de gestionnaires des collecteurs NetFlow et de moteurs de corrélation qui déchargent le serveur central Sentinel de toute la charge de traitement. Outre la gestion de la charge des événements, des règles de corrélation et des données de flux réseau, les gestionnaires des collecteurs NetFlow, les moteurs de corrélation et les gestionnaires des collecteurs distants libèrent 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.

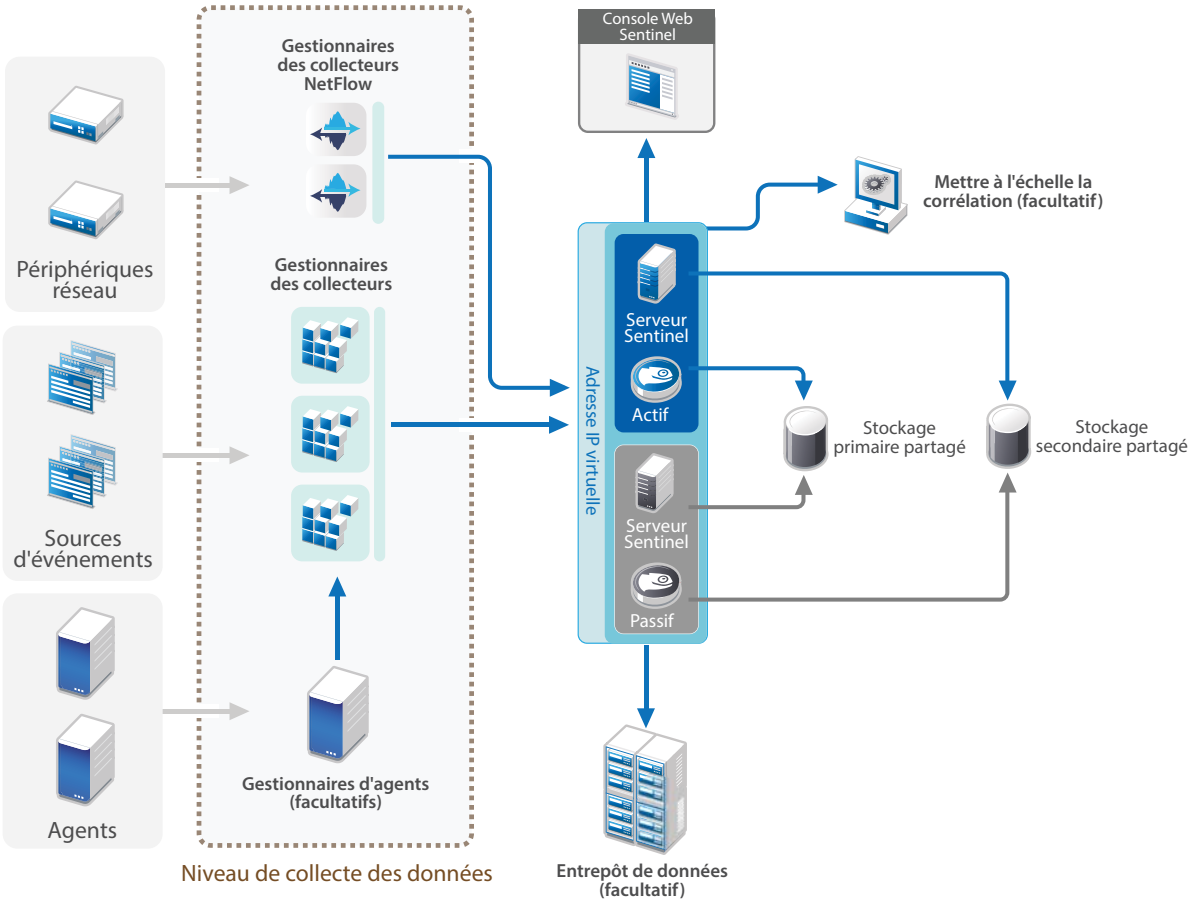
Figure 6-2 Déploiement distribué en un niveau



6.4 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 VI, « Déploiement de Sentinel pour une haute disponibilité », page 143.

Figure 6-3 *Déploiement distribué en un niveau avec haute disponibilité*

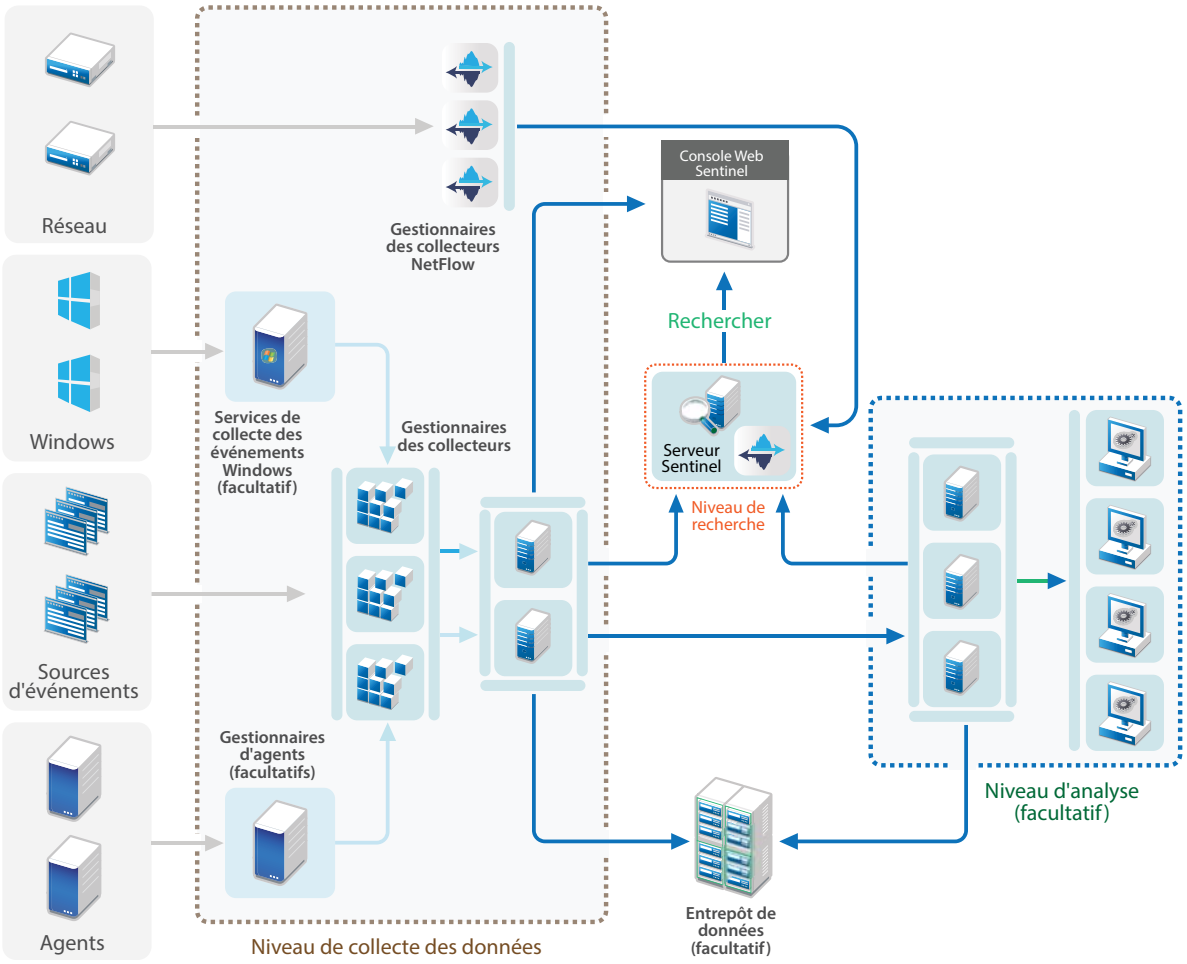


6.5 Déploiement distribué en deux ou trois niveaux

Ce déploiement permet de surpasser les fonctionnalités de gestion des charges d'un seul serveur central Sentinel et de partager la charge de traitement sur plusieurs instances Sentinel en utilisant les fonctionnalités Lien et Recherche distribuée de Sentinel. La collecte des données équilibre la charge sur plusieurs serveurs Sentinel, chacun d'entre eux ayant plusieurs gestionnaires des collecteurs, comme l'indique le niveau de collecte des données. Si vous souhaitez effectuer une corrélation d'événement ou utiliser la fonctionnalité security intelligence, vous pouvez transmettre des données au niveau d'analyse à l'aide de Lien Sentinel. Le niveau de recherche permet d'accéder facilement, grâce à un seul point d'accès et à l'aide de la recherche distribuée Sentinel, à tous les systèmes des autres niveaux. Lorsqu'une demande de recherche est fédérée dans 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.

Les données de flux réseau sont stockées dans le niveau de recherche afin de permettre une navigation aisée à partir des résultats de recherche vers l'analyse du trafic réseau contextuel.

Figure 6-4 Déploiement distribué en deux ou trois niveaux



6.6 Planification des partitions pour le stockage de données

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 exacts, l'ensemble de la structure du répertoire `/var/opt/novell/sentinel` doit se trouver sur une seule partition de disque. Dans le cas contraire, 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 Section 6.6.4, « Structure des répertoires de Sentinel », page 47.

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 Wikipedia sur le partitionnement de disque.

6.6.1 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 dans la Section 6.6.4, « Structure des répertoires de Sentinel », page 47. 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`.

6.6.2 Utilisation de partitions dans une installation 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 Section 13.3.2, « Création de partitions », page 85.

6.6.3 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
Temp	`/tmp`	30 Go	Emplacement des fichiers temporaires de Sentinel et du système d'exploitation ; l'isolation dans une partition distincte protège les données d'application de tout dommage si une fuite remplit l'espace temporaire.
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.

6.6.4 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 de configuration se trouvent dans le répertoire suivant : `/etc/opt/novell/sentinel`.
- Le fichier d'ID de processus (PID) se trouve dans le répertoire `/var/run/sentinel/server.pid`

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

7 Considérations sur le déploiement pour le mode FIPS140-2

Sentinel peut éventuellement être configuré pour utiliser NSS (Network Security Services) de Mozilla, un module cryptographique certifié FIPS 140-2, pouvant servir au codage 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 gestionnaires des collecteurs distants Sentinel, les moteurs de corrélation distants Sentinel, l'interface utilisateur Web de Sentinel, Sentinel Control Center et le service Sentinel Advisor utilise un codage certifié FIPS 140-2.

7.1 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 cryptographique NSS fourni par RHEL 6.3 est certifié FIPS 140-2. Les modules cryptographiques NSS fournis par SLES 11 SP3 n'ont pas encore officiellement reçu la certification FIPS 140-2, mais la procédure de certification du module SUSE est en cours. Une fois certifiés, 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 FIPS 140-2 RHEL 6.2, consultez le site Web relatif aux *modules cryptographiques certifiés FIPS 140-1 et FIPS 140-2*.

7.1.1 Paquetages NSS RHEL

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

- nspr-4.9-1.el6.x86_64
- nss-sysinit-3.13.3-6.el6.x86_64
- nss-util-3.13.3-2.el6.x86_64
- nss-softokn-freebl-3.12.9-11.el6.x86_64
- nss-softokn-3.12.9-11.el6.x86_64
- nss-3.13.3-6.el6.x86_64
- nss-tools-3.13.3-6.el6.x86_64

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

7.1.2 Paquetages NSS SLES

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

- libfreebl3-3.13.1-0.2.1
- mozilla-nspr-4.8.9-1.2.2.1
- mozilla-nss-3.13.1-0.2.1
- mozilla-nss-tools-3.13.1-0.2.1

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

7.2 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

  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 114.

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 obtenir des instructions 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 119.

- 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.

- NetIQ 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. Cela ne vous empêche toutefois pas de 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 (qui n'a pas encore été mis à jour) prenne en charge le mode FIPS, faites-en la demande à l'aide de Bugzilla.

7.3 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.	Section 7.4, « Scénarios de déploiement », page 51.
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.	Section 12.2.2, « Installation personnalisée », page 71. Section 12.3, « Installation silencieuse », page 73 Chapitre 20, « Activation du mode FIPS 140-2 dans une installation Sentinel existante », page 109
Configurez les plug-ins Sentinel pour qu'ils s'exécutent en mode FIPS 140-2.	Section 21.5, « Configuration des plug-ins Sentinel pour une exécution en mode FIPS 140-2. », page 114.
Importez les certificats dans le keystore FIPS de Sentinel.	Section 21.6, « Importation de certificats dans une base de données keystore FIPS », page 120

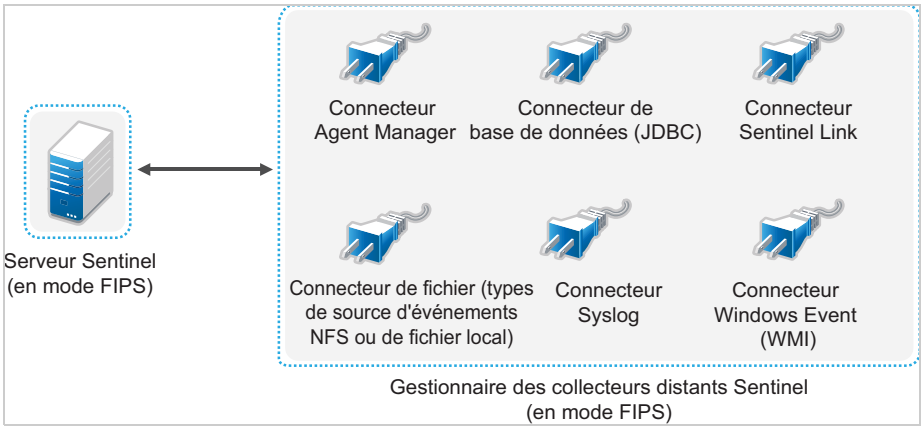
REMARQUE : NetIQ vous recommande vivement d'effectuer une sauvegarde de vos systèmes Sentinel avant de démarrer la conversion en mode FIPS. Si pour une raison quelconque, le serveur doit être restauré en mode non-FIPS, la seule méthode pour ce faire implique d'effectuer une restauration à partir d'une 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 120.

7.4 Scénarios de déploiement

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

7.4.1 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 un gestionnaire des collecteurs distant. Vous pouvez avoir un ou plusieurs gestionnaires des collecteurs distants.



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 109.

---

2 Votre gestionnaire des collecteurs distant Sentinel doit être exécuté en mode FIPS 140-2.

REMARQUE : si le gestionnaire des collecteurs distant (que vous venez d'installer ou de mettre à jour) n'est pas exécuté 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 gestionnaires des collecteurs et des moteurs de corrélation distants » page 109.

---

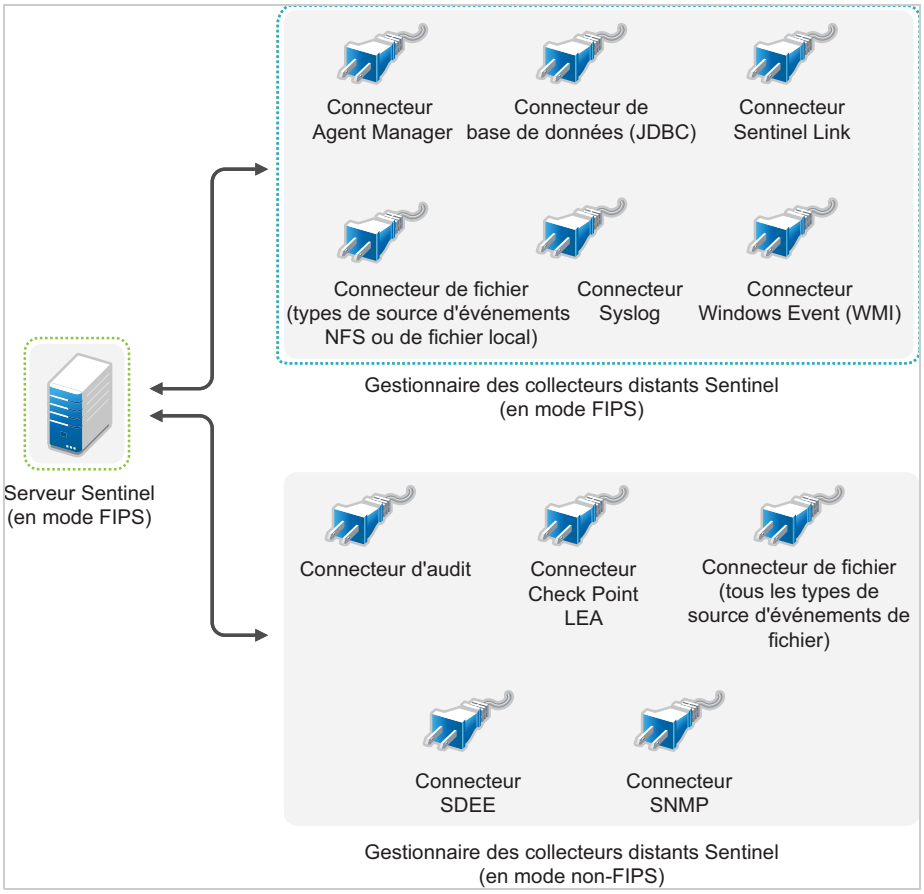
3 Veillez à ce que le serveur FIPS et les gestionnaires des collecteurs distants communiquent entre eux.

4 Faites basculer les moteurs de corrélation distants (le cas échéant) en mode FIPS. Pour plus d'informations, reportez-vous à la section « Activation du mode FIPS 140-2 sur des gestionnaires des collecteurs et des moteurs de corrélation distants » page 109.

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 114.

7.4.2 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. Cet environnement est supposé impliquer la présence d'un serveur Sentinel et une collecte de données via un gestionnaire des collecteurs distant. Vous pouvez avoir un ou plusieurs gestionnaires des collecteurs distants.



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 gestionnaires des collecteurs distants : l'un 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 encore 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 109.

2 Veillez à ce qu'un gestionnaire des collecteurs distant 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 aucun gestionnaire des collecteurs distant, 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 gestionnaires des collecteurs et des moteurs de corrélation distants » page 109.

   2b Mettez à jour le certificat de serveur sur le gestionnaire des collecteurs distant non-FIPS. Pour plus d'informations, reportez-vous à la section « Mise à jour des certificats de serveur dans les gestionnaires des collecteurs et les moteurs de corrélation distants » page 113.

3 Veillez à ce que les deux gestionnaires des collecteurs distants communiquent avec le serveur Sentinel compatible FIPS 140-2.

4 Faites basculer les moteurs de corrélation distants (le cas échéant) en mode FIPS. Pour plus d'informations, reportez-vous à la section « Activation du mode FIPS 140-2 sur des gestionnaires des collecteurs et des moteurs de corrélation distants » page 109.

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 114.

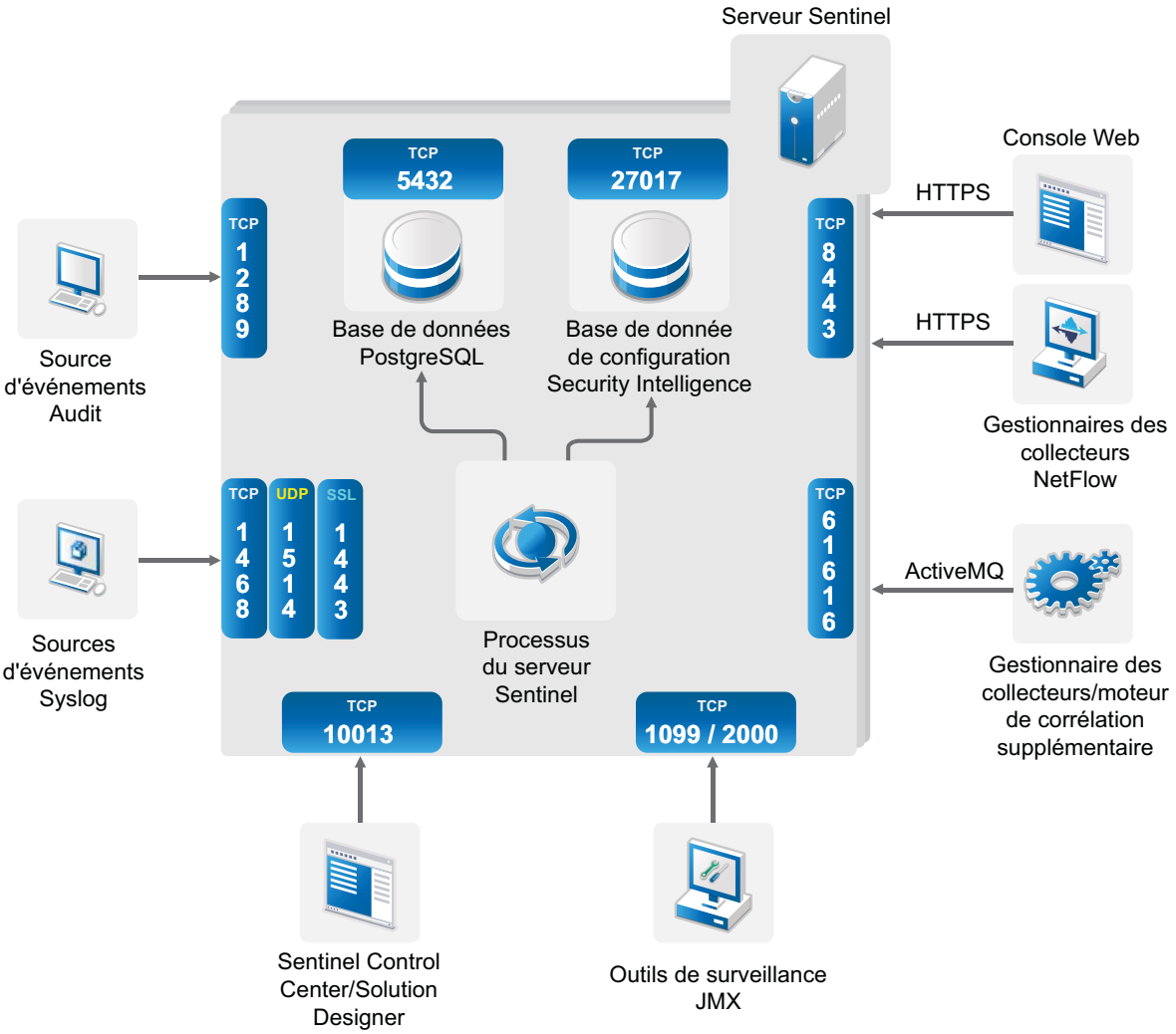
   5a Déployez les connecteurs qui prennent en charge le mode FIPS 140-2 dans le gestionnaire des collecteurs distant s'exécutant en mode FIPS.

   5b Déployez les connecteurs qui ne prennent pas en charge le mode FIPS 140-2 dans le gestionnaire des collecteurs distant non-FIPS.

8 Ports utilisés

Sentinel utilise des ports différents 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. L'illustration suivante indique les ports utilisés dans Sentinel :

Figure 8-1 *Ports utilisés dans Sentinel*



- Section 8.1, « Ports du serveur Sentinel », page 56
- Section 8.2, « Ports du gestionnaire des collecteurs », page 58
- Section 8.3, « Ports du moteur de corrélation », page 59
- Section 8.4, « Ports du gestionnaire des collecteurs NetFlow », page 60

8.1 Ports du serveur Sentinel

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

8.1.1 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 l'interface 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.

8.1.2 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.
TCP 1099 et 2000	Entrant	Facultatif	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 et les connexions entrantes en provenance de gestionnaires des collecteurs NetFlow.
TCP 1443	Entrant	Facultatif	Utilisé pour les messages syslog codés avec SSL.
TCP 61616	Entrant	Facultatif	Utilisé pour les connexions entrantes des gestionnaires des collecteurs et des moteurs de corrélation.
TCP 10013	Entrant	Requis	Utilisé par Sentinel Control Center et Solution Designer.
TCP 1468	Entrant	Facultatif	Utilisé pour les messages syslog.

Ports	Sens	Obligatoire/ facultatif	Description
TCP 10014	Entrant	Facultatif	Utilisé par les gestionnaires des collecteurs distants afin d'établir la connexion au serveur par l'intermédiaire du proxy SSL. Ce port n'est toutefois pas courant. Par défaut, les gestionnaires des collecteurs distants 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 l'URL des mises à jour Advisor (https://secure-www.novell.com/sentinel/download/advisor/).
TCP 8443	Sortant	Facultatif	Si vous utilisez une recherche distribuée, le port initialise une connexion avec les autres systèmes Sentinel pour effectuer la 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.

8.1.3 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	Utilisé par la console de gestion (WebYaST) de l'applicatif Sentinel. Également utilisé par l'applicatif Sentinel pour le service de mise à jour.

Ports	Sens	Obligatoire/ facultatif	Description
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 NetIQ sur Internet ou un service SMT (Subscription Management Tool) sur votre réseau.
TCP 80	Sortant	Facultatif	Initialise une connexion avec le service SMT.

8.2 Ports du gestionnaire des collecteurs

Le gestionnaire des collecteurs utilise les ports suivants pour communiquer avec d'autres composants.

8.2.1 Ports réseau

Pour le bon fonctionnement du gestionnaire des collecteurs 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	Facultatif	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.

8.2.2 Ports de l'applicatif du gestionnaire des collecteurs

Outre les ports ci-dessus, les ports suivants sont également ouverts sur l'applicatif Gestionnaire des collecteurs Sentinel.

Ports	Sens	Obligatoire/ facultatif	Description
TCP 22	Entrant	Requis	Utilisé pour un accès shell sécurisé à l'applicatif Sentinel
TCP 4984	Entrant	Requis	Utilisé par la console de gestion (WebYaST) de l'applicatif Sentinel. 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	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	Sortant	Requis	Initialise une connexion avec l'espace de stockage de la mise à jour logicielle de l'applicatif NetIQ sur Internet ou un service SMT (Subscription Management Tool) sur votre réseau.
TCP 80	Sortant	Facultatif	Initialise une connexion avec le service SMT.

8.3 Ports du moteur de corrélation

Le moteur de corrélation utilise les ports suivants pour communiquer avec d'autres composants.

8.3.1 Ports réseau

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

Ports	Sens	Obligatoire/ facultatif	Description
TCP 1099 et 2000	Entrant	Facultatif	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.

8.3.2 Ports de l'applicatif du moteur de corrélation

Outre les ports ci-dessus, les ports suivants doivent également être ouverts sur le moteur de corrélation Sentinel.

Ports	Sens	Obligatoire/ facultatif	Description
TCP 22	Entrant	Requis	Utilisé pour un accès shell sécurisé à l'applicatif Sentinel

Ports	Sens	Obligatoire/ facultatif	Description
TCP 4984	Entrant	Requis	Utilisé par la console de gestion (WebYaST) de l'applicatif Sentinel. 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 NetIQ sur Internet ou un service SMT (Subscription Management Tool) sur votre réseau.
TCP 80	Sortant	Facultatif	Initialise une connexion avec le service SMT.

8.4 Ports du gestionnaire des collecteurs NetFlow

Le gestionnaire des collecteurs NetFlow utilise les ports suivants pour communiquer avec d'autres composants :

Ports	Sens	Obligatoire/ facultatif	Description
HTTPS 8443	Sortant	Requis	Initialise une connexion avec le serveur Sentinel.
3578	Entrant	Requis	Utilisé pour la réception de données de flux réseau en provenance de périphériques réseau.

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.

9.1 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.
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 références Novell eDirectory ou Microsoft Active Directory.

  Pour plus d'informations sur l'installation interactive, reportez-vous à la Section 12.2, « Installation interactive », page 69.

- **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 sans surveillance. Pour plus d'informations sur l'installation silencieuse, reportez-vous à la Section 12.3, « Installation silencieuse », page 73.

9.2 Installation de l'applicatif

Le programme d'installation de l'applicatif installe Sentinel et le système d'exploitation SLES 11 SP3 64 bits.

L'applicatif Sentinel est disponible dans les formats suivants :

- image de l'applicatif OVF ;
- image Live DVD de l'applicatif matériel directement déployée sur un serveur matériel.

Pour plus d'informations sur l'installation de l'applicatif, reportez-vous au Chapitre 13, « Installation de l'applicatif », page 79.

III 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 de Sentinel installe les composants suivants sur le serveur Sentinel :

- **Processus serveur Sentinel :** il s'agit du principal composant de 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.
- **Serveur Web :** Sentinel utilise Jetty en tant que serveur Web pour une connexion sécurisée à l'interface Web de Sentinel.
- **Base de données PostgreSQL :** Sentinel dispose d'une base de données intégrée qui stocke les informations de configuration Sentinel, les données de ressources et de vulnérabilité, les informations d'identité, l'état des incidents et des processus de travail, etc.
- **Base de données MongoDB :** stocke les données Security Intelligence.
- **Gestionnaire des collecteurs :** il fournit un point flexible de collecte de données pour Sentinel. Le programme d'installation de Sentinel installe un gestionnaire des collecteurs par défaut pendant l'installation.
- **Gestionnaire des collecteurs NetFlow :** Le gestionnaire des collecteurs NetFlow collecte des données de flux réseau (NetFlow, IPFIX, etc.) à partir de périphériques réseau tels que des routeurs, des commutateurs et des pare-feu. Ces données décrivent des informations de base sur toutes les connexions réseau établies entre les hôtes, y compris les paquets et les octets transmis, ce qui vous aide à visualiser le comportement des différents hôtes ou de l'ensemble du réseau.
- **Moteur de corrélation :** 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 *NetIQ 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
  - Flux de travail iTRAC
  - Solution packs

L'architecture de Sentinel étant hautement évolutive, si des taux d'événements élevés sont prévus, vous pouvez répartir les composants entre plusieurs machines afin d'optimiser les performances système. Pour les environnements de production, NetIQ Corporation recommande de configurer un

déploiement distribué, car il isole les composants de collecte de données sur une machine distincte, ce qui s'avère important pour gérer les pointes de trafic et les autres anomalies avec une stabilité maximale du système. Pour plus d'informations, reportez-vous au Section 6.1, « Avantages des déploiements distribués », page 39.

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 37.
- ❒ 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 179.
- ❒ Si vous prévoyez d'installer la version sous licence, vous devez obtenir votre clé de licence auprès du Service clients NetIQ.
- ❒ Vérifiez que les ports répertoriés au Chapitre 8, « Ports utilisés », page 55 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).
- ❒ **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

12 Installation traditionnelle

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

12.1 Présentation des options d'installation

`./install-sentinel --help` affiche les options suivantes :

Options	Valeur	Description
--location	Répertoire	Indique pour l'installation de Sentinel un répertoire différent du répertoire root (/).
-m, --manifest	Nom du fichier	Indique un fichier de manifeste de produit à utiliser à la place du fichier de manifeste par défaut.
--no-configure		Indique de ne pas configurer le produit après l'installation.
-n, --no-start		Indique de ne pas démarrer ou redémarrer Sentinel après l'installation ou la configuration.
-r, --recordunattended	Nom du fichier	Indique un fichier permettant d'enregistrer les paramètres à utiliser lors d'une installation sans surveillance.
-u, --unattended	Nom du fichier	Utilise les paramètres du fichier indiqué lors de l'installation de Sentinel sur des systèmes non surveillés.
-h, --help		Affiche les options à utiliser lors de l'installation de Sentinel.
-l, --log-file	Nom du fichier	Enregistre les messages de journal dans un fichier.
--no-banner		Supprime l'affichage d'un message bannière.
-q, --quiet		Affiche moins de messages.
-v, --verbose		Affiche tous les messages pendant l'installation.

12.2 Installation interactive

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

12.2.1 Installation standard

Procédez comme suit pour effectuer une installation standard :

1. Téléchargez le fichier d'installation Sentinel depuis la page Web des téléchargements NetIQ :
   - **1a** Dans le champ **Product or Technology (Produit ou technologie)**, sélectionnez **SIEM-Sentinel**.
   - **1b** Cliquez sur **Rechercher**.
   - **1c** Dans la colonne **Télécharger**, cliquez sur le bouton d'**évaluation de Sentinel** .
   - **1d** Cliquez sur **Proceed to download (Poursuivre le téléchargement)**, puis indiquez le nom et le mot de passe du client.
   - **1e** Cliquez sur **Télécharger** pour installer la version correspondant à votre plate-forme.
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 Web de Sentinel, indiquez l'adresse URL suivante dans votre navigateur Internet :

`https://<IP_Address_Sentinel_server>:8443.`

L'adresse <*adresse_IP_serveur_Sentinel*> est l'adresse IP ou le nom DNS du serveur Sentinel, et le numéro 8443 est le port par défaut du serveur Sentinel.

12.2.2 Installation personnalisée

Si vous installez Sentinel avec une configuration personnalisée, vous pouvez indiquer la clé de licence, modifier le mot de passe des différents utilisateurs et spécifier les valeurs des ports utilisés pour interagir avec les composants internes.

1. Téléchargez le fichier d'installation Sentinel depuis la page Web des téléchargements NetIQ :
   - **1a** Dans le champ **Product or Technology (Produit ou technologie)**, sélectionnez **SIEM-Sentinel**.
   - **1b** Cliquez sur **Rechercher**.
   - **1c** Dans la colonne **Télécharger**, cliquez sur le bouton d'**évaluation de Sentinel 7.2**.
   - **1d** Cliquez sur **Proceed to download (Poursuivre le téléchargement)**, puis indiquez le nom et le mot de passe du client.
   - **1e** Cliquez sur **Télécharger** pour installer la version correspondant à votre plate-forme.
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. 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>`
4. 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.
5. Appuyez sur la barre d'espacement pour lire l'intégralité de l'accord de licence.
6. 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.
7. Indiquez `2` pour effectuer une configuration personnalisée de Sentinel.
8. 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.
9. Indiquez le mot de passe de l'utilisateur administrateur `admin` et confirmez-le en le ressaisissant.

10 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.

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

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

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

14 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`.

15 ***Pour que Sentinel utilise le mode FIPS 140-2*** , appuyez sur `y`.

   15a 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.

   15b 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`.

   15c Terminez la configuration du mode FIPS 140-2 en effectuant les tâches mentionnées au Chapitre 21, « Fonctionnement de Sentinel en mode FIPS 140-2 », page 111.

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 Web de Sentinel, indiquez l'adresse URL suivante dans votre navigateur Internet :

`https://<IP_Address_Sentinel_server>:8443.`

L'adresse *<adresse_IP_serveur_Sentinel>* est l'adresse IP ou le nom DNS du serveur Sentinel, et le numéro 8443 est le port par défaut du serveur Sentinel.

12.3 Installation silencieuse

L'installation silencieuse ou sans surveillance est utile si vous devez installer plusieurs serveurs Sentinel 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. Vous pouvez enregistrer les paramètres d'installation lors de l'installation de Sentinel avec la configuration standard ou une configuration personnalisée.

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 Section 12.2.1, « Installation standard », page 70 ou à la Section 12.2.2, « Installation personnalisée », page 71.

Pour que Sentinel utilise 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 depuis la page Web des téléchargements NetIQ.
2. Loguez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez installer Sentinel.
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 installer Sentinel en mode silencieux :

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

   L'installation se poursuit et utilise les valeurs stockées dans le fichier de réponses.
5. **(Conditionnel) Si vous avez choisi d'activer le mode FIPS 140-2,** configurez-le en suivant la procédure mentionnée au Chapitre 21, « Fonctionnement de Sentinel en mode FIPS 140-2 », page 111.

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.

12.4 Installation de gestionnaires des collecteurs et de moteurs de corrélation

Par défaut, Sentinel installe un gestionnaire des collecteurs et un moteur de corrélation. Pour les environnements de production, NetIQ Corporation recommande de configurer un déploiement distribué, car il isole les composants de collecte de données sur une machine distincte, ce qui s'avère important pour gérer les pointes de trafic et les autres anomalies avec une stabilité maximale du système. Pour en savoir plus sur les avantages liés à l'installation de composants supplémentaires, reportez-vous à la Section 6.1, « Avantages des déploiements distribués », page 39.

IMPORTANT : vous devez installer le moteur de corrélation ou le gestionnaire des collecteurs supplémentaire sur des systèmes distincts. Veillez également à ne pas les installer sur le système où se trouve déjà le serveur Sentinel.

12.4.1 Liste de contrôle de 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 37.
- ❒ Synchronisez l'heure à l'aide du protocole NTP (Network Time Protocol).
- ❒ Un gestionnaire des collecteurs requiert une connectivité réseau vers le port de bus de messages (61616) sur le serveur Sentinel Avant d'installer le gestionnaire des collecteurs, vérifiez que tous les paramètres réseau et du pare-feu sont définis pour pouvoir communiquer sur ce port.

12.4.2 Installation de gestionnaires des collecteurs et de moteurs de corrélation

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

   ```
   https://<IP_Address_Sentinel_server>:8443.
   ```

   L'adresse <*adresse_IP_serveur_Sentinel*> est l'adresse IP ou le nom DNS du serveur Sentinel, et le numéro 8443 est le port par défaut du serveur Sentinel.

   Loguez-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 le gestionnaire des collecteurs ou le moteur de corrélation :

   Pour le gestionnaire des collecteurs :

   ```
   ./install-cm
   ```

Pour le moteur de corrélation :

```
./install-ce
```

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

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

    Le certificat du serveur Sentinel s'affiche.

13. Indiquez les références utilisateur ActiveMQ du gestionnaire des collecteurs ou du moteur de corrélation.

    Les références utilisateur ActiveMQ sont stockées dans le fichier `/<répertoire_installation>/etc/opt/novell/sentinel/config/activemqusers.properties` situé sur le serveur Sentinel.

14. Lorsque vous êtes invité à accepter le certificat, vérifiez-le à l'aide de la commande suivante :

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

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

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

16. Entrez `yes` ou `y` pour que Sentinel utilise le mode FIPS 140-2, puis configurez FIPS.

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

12.4.3 Ajout d'un utilisateur ActiveMQ personnalisé pour le gestionnaire des collecteurs ou le moteur de corrélation

Sentinel vous recommande d'utiliser les noms d'utilisateur ActiveMQ par défaut du gestionnaire des collecteurs et du moteur de corrélation distants. Toutefois, si vous avez installé plusieurs gestionnaires des collecteurs distants et que vous souhaitez les identifier séparément, vous pouvez créer de nouveaux utilisateurs ActiveMQ :

1. Connectez-vous au serveur en tant qu'utilisateur Sentinel disposant de droits d'accès sur les fichiers d'installation.

2. Ouvrez le fichier `activemqgroups.properties`.

   Ce fichier se trouve dans le répertoire `/<répertoire_installation>/etc/opt/novell/sentinel/config/`.

3. Ajoutez les noms d'utilisateur ActiveMQ en les séparant par une virgule comme suit :

   Pour le gestionnaire des collecteurs, ajoutez les nouveaux utilisateurs dans la section cm. Par exemple :

   ```
   cm=collectormanager,cmuser1,cmuser2,...
   ```

Pour le moteur de corrélation, ajoutez les nouveaux utilisateurs dans la section admins. Par exemple :

```
admins=system,correlationengine,ceuser1,ceuser2,...
```

4. Enregistrez et fermez le fichier.
5. Ouvrez le fichier `activemqusers.properties`.

   Ce fichier se trouve dans le répertoire */<répertoire_installation>*`/etc/opt/novell/sentinel/config/`.
6. Ajoutez le mot de passe de l'utilisateur ActiveMQ créé à l'Étape 3.

   Le mot de passe peut être toute chaîne aléatoire. Par exemple :

   Pour les utilisateurs du gestionnaire des collecteurs :

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   collectormanager=1c51ae56
   cmuser1=1b51de55
   cmuser2=1a51ce57
   ```

   Pour les utilisateurs du moteur de corrélation :

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   correlationengine=68790d7a
   ceuser1=69700c6d
   ceuser2=70701b5c
   ```
7. Enregistrez et fermez le fichier.
8. Redémarrez le serveur Sentinel.

12.5 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 ». Bien que l'installation s'effectue correctement, NetIQ Corporation n'assure pas le support des installations par un utilisateur non-root quand cet utilisateur n'est pas un utilisateur « novell ».

1. Téléchargez les fichiers d'installation depuis la page Web des téléchargements NetIQ.
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. Loguez-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`
Gestionnaire des collecteurs	**Emplacement par défaut:** `./install-cm`
	Emplacement personnalisé : `./install-cm --location=/foo`
Moteur de corrélation	**Emplacement par défaut:** `./install-ce`
	Emplacement personnalisé : `./install-cm --location=/foo`
Gestionnaire des collecteurs NetFlow	**Emplacement par défaut:** `./install-netflow`
	Emplacement personnalisé : `./install-netflow --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 Section 12.2.1, « Installation standard », page 70 ou à la Section 12.2.2, « Installation personnalisée », page 71.

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>`
Gestionnaire des collecteurs	**Emplacement par défaut:** `./install-cm -u <fichier_réponse>` **Emplacement personnalisé :** `./install-cm --location=/foo -u <fichier_réponse>`
Moteur de corrélation	**Emplacement par défaut:** `./install-ce -u <fichier_réponse>` **Emplacement personnalisé :** `./install-ce --location=/foo -u <fichier_réponse>`
Gestionnaire des collecteurs NetFlow	**Emplacement par défaut:** `./install-netflow -u <fichier_réponse>` **Emplacement personnalisé :** `./install-netflow --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 Section 12.2.1, « Installation standard », page 70.
- Si vous choisissez de passer à une configuration personnalisée, suivez les étapes Étape 7 à Étape 14 dans la Section 12.2.2, « Installation personnalisée », page 71.

12 Loguez-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 Web de Sentinel, indiquez l'adresse URL suivante dans votre navigateur Internet :

`https://<IP_Address_Sentinel_server>:8443.`

L'adresse <*adresse_IP_serveur_Sentinel*> est l'adresse IP ou le nom DNS du serveur Sentinel, et le numéro 8443 est le port par défaut du serveur Sentinel.

13 Installation de l'applicatif

L'applicatif Sentinel est un applicatif logiciel prêt à être utilisé, basé sur SUSE Studio. Il associe un système d'exploitation SLES renforcé et le service de mise à jour du logiciel Sentinel. L'expérience utilisateur est simple et transparente, et les clients peuvent tirer bénéfice des investissements existants. Avant d'installer l'applicatif Sentinel, consultez les nouvelles fonctionnalités et les problèmes connus dans les notes de version du SLES pris en charge.

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 NetIQ Sentinel.

13.1 Installation de l'applicatif ISO Sentinel

Cette section fournit des informations sur l'installation de Sentinel, des gestionnaires des collecteurs et des moteurs de corrélation 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.

13.1.1 Conditions préalables

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

- (Facultatif) 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, décompressez le fichier et créez un DVD.
- Pour pouvoir effectuer l'installation, vérifiez que le système sur lequel vous souhaitez installer l'image de disque ISO dispose d'une mémoire minimale de 4,5 Go.
- Vérifiez que le disque dur dispose d'un espace disponible minimal de 50 Go pour que le programme d'installation propose une partition automatique.

13.1.2 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 NetIQ.
2. (Facultatif) 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

   Copiez l'image ISO sur un DVD, configurez la machine virtuelle à l'aide du DVD et mettez-la sous tension.
3. (Facultatif) 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** Exécutez l'image de l'applicatif Live DVD en sélectionnant la toute première entrée dans le menu de démarrage.

     Le programme d'installation vérifie d'abord si la mémoire et l'espace disque disponibles sont suffisants. Si la mémoire disponible est inférieure à 2.5 Go, l'installation s'arrête automatiquement. Si la mémoire disponible est supérieure à 2.5 Go mais inférieure à 6.7 Go, le programme d'installation affiche un message vous indiquant que la mémoire dont vous disposez est inférieure aux recommandations. Entrez y si vous souhaitez poursuivre l'installation ou n dans le cas contraire.
4. Sélectionnez la langue de votre choix, puis cliquez sur **Suivant**.
5. Sélectionnez la configuration du clavier, puis cliquez sur **Suivant**.
6. Lisez et acceptez l'accord de licence du logiciel SUSE Enterprise Server. Cliquez sur **Suivant**
7. Lisez et acceptez l'accord de licence de l'utilisateur final de NetIQ Sentinel. Cliquez sur **Suivant**
8. Dans la page Nom d'hôte et Nom de domaine, spécifiez le nom d'hôte et le nom de domaine. Désélectionnez l'option **Assign Hostname to Loopback IP** (Assigner le nom d'hôte à l'adresse IP en boucle).
9. Cliquez sur **Next** (Suivant).
10. Choisissez l'une des deux options suivantes pour les paramètres de connexion :
    - Pour utiliser les paramètres de connexion réseau actuels, sélectionnez **Utiliser la configuration suivante** dans la page Configuration réseau II.
    - Pour modifier les paramètres de connexion réseau, cliquez sur **Changer**, puis effectuez les modifications souhaitées.
11. Cliquez sur **Next** (Suivant).
12. Indiquez l'heure et la date, cliquez sur **Suivant**.

    pour modifier la configuration NTP après l'installation, utilisez YaST dans la ligne de commande de l'applicatif. Vous pouvez utiliser WebYast pour modifier les paramètres de date et d'heure, mais pas la configuration NTP.

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

    ```
    rcntp restart
    ```
13. Définissez le mot de passe `root`, puis cliquez sur **Suivant**.
14. Définissez le mot de passe admin de Sentinel, puis cliquez sur **Suivant**.

Assurez-vous que l'option **Installez l'applicatif Sentinel sur le disque dur (pour l'image Live DVD uniquement)** est sélectionnée pour installer l'application sur le serveur physique. Par défaut, cette case est cochée.

Si vous désélectionnez cette case, l'applicatif n'est pas installé sur le serveur physique et ne s'exécute qu'en mode LIVE DVD. Passez à l'Étape 21.

15 Dans la console du programme d'installation LIVE YaST2, sélectionnez **Suivant**.

La console du programme d'installation LIVE YaST2 installe l'applicatif sur le disque dur. La console du programme d'installation LIVE YaST2 répète certaines des étapes d'installation précédentes.

16 L'écran **Suggested Partitioning** (Partitionnement proposé) affiche la configuration de partition recommandée. Passez en revue la configuration de partition, configurez-la (si nécessaire), puis sélectionnez **Suivant**. Ne modifiez ces paramètres que si vous êtes habitué à configurer des partitions dans SLES.

Vous pouvez définir la configuration de partition en utilisant les différentes options de partitionnement disponibles à l'écran. Pour plus d'informations sur la configuration des partitions, reportez-vous à la section Using the YaST Partitioner (Utilisation du partitionneur YaST) dans la *documentation de SLES* et à la Section 6.6, « Planification des partitions pour le stockage de données », page 45.

17 Entrez le mot de passe root, puis sélectionnez **Suivant**.

18 L'écran **Live Installation Settings** (Paramètres d'installation en direct) Paramètres d'installation LIVE affiche les paramètres d'installation sélectionnés. Passez les paramètres en revue, configurez-les (si nécessaire), puis sélectionnez **Installer**.

19 Sélectionnez **Installer** pour confirmer l'installation.

Attendez que l'installation soit terminée. Après l'installation, le démarrage de tous les services peut prendre quelques minutes, car le système effectue une initialisation unique.

20 Cliquez sur **OK** pour redémarrer le système.

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

22 Entrez le nom d'utilisateur et le mot de passe root dans la console pour vous connecter à l'applicatif.

La valeur par défaut du nom d'utilisateur est `root` et le mot de passe est celui défini à l'Étape 17.

23 Reportez-vous à la Section 13.3, « Configuration post-installation de l'applicatif », page 85.

13.1.3 Installation de gestionnaires des collecteurs et de moteurs de corrélation

La procédure d'installation est identique pour un gestionnaire des collecteurs et un moteur de corrélation, si ce n'est que vous devez télécharger le fichier d'applicatif ISO approprié à partir du site Web de téléchargement NetIQ.

1 Suivez la procédure de l'étape 1 à l'Étape 13 de la Section 13.1.2, « Installation de Sentinel », page 80.

2 Spécifiez la configuration suivante pour le gestionnaire des collecteurs ou le moteur de corrélation :

- **Nom d'hôte ou adresse IP du serveur Sentinel :** indiquez le nom d'hôte ou l'adresse IP du serveur Sentinel auquel le gestionnaire des collecteurs ou le moteur de corrélation 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`.

- **Nom d'utilisateur du canal de communication :** indiquez le nom d'utilisateur du canal de communication, c'est-à-dire le nom d'utilisateur du gestionnaire des collecteurs ou du moteur de corrélation.
- **Mot de passe de l'utilisateur du canal de communication :** indiquez le mot de passe de l'utilisateur du canal de communication.

  Les références utilisateur du canal de communication sont stockées dans le fichier `/<répertoire_installation>/etc/opt/novell/sentinel/config/activemqusers.properties` situé sur le serveur Sentinel.

  Pour vérifier les références, consultez la ligne suivante du fichier `activemqusers.properties` :

  Pour le gestionnaire des collecteurs :

  `collectormanager=<password>`

  Dans cet exemple, `collectormanager` est le nom de l'utilisateur et la valeur correspondante est le mot de passe.

  Pour le moteur de corrélation :

  `correlationengine=<password>`

  Dans cet exemple, `correlationengine` est le nom de l'utilisateur et la valeur correspondante est le mot de passe.
- **Installez l'applicatif Sentinel sur le disque dur (pour l'image Live DVD uniquement) :**

  veillez à cocher cette case pour installer l'applicatif sur le serveur physique.

  Si vous désélectionnez cette case à cocher, l'applicatif ne sera pas installé sur le serveur physique et s'exécutera uniquement en mode LIVE DVD.

3. Cliquez sur **Suivant**.
4. Acceptez le certificat lorsque vous y êtes invité.
5. Effectuez les opérations de l'Étape 15 à l'Étape 20 de la Section 13.1.2, « Installation de Sentinel », page 80.
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 le gestionnaire des collecteurs ou le moteur de corrélation Sentinel (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 22 à l'Étape 23 de la Section 13.1.2, « Installation de Sentinel », page 80.

13.2 Installation de l'applicatif OVF Sentinel

Cette section fournit des informations sur l'installation de Sentinel, du gestionnaire des collecteurs et du moteur de corrélation 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.

- Section 13.2.1, « Installation de Sentinel », page 83
- Section 13.2.2, « Installation de gestionnaires des collecteurs et de moteurs de corrélation », page 84

13.2.1 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 NetIQ.
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, puis cliquez sur **Suivant**.
6. Sélectionnez la disposition du clavier, puis cliquez sur **Suivant**.
7. Lisez et acceptez l'accord de licence du logiciel SUSE Linux Enterprise Server (SLES) 11 SP3.
8. Lisez et acceptez l'accord de licence de l'utilisateur final de NetIQ Sentinel.
9. Dans la page Nom d'hôte et Nom de domaine, spécifiez le nom d'hôte et le nom de domaine. Désélectionnez l'option **Assign Hostname to Loopback IP** (Assigner le nom d'hôte à l'adresse IP en boucle).
10. Cliquez sur **Suivant**. Les configurations du nom d'hôte sont enregistrées.
11. Choisissez l'une des options suivantes pour la connexion réseau :
    - Pour utiliser les paramètres actuels de connexion réseau, sélectionnez **Utiliser la configuration suivante** dans la page Configuration réseau II, puis cliquez sur **Suivant**.
    - Pour changer les paramètres de connexion réseau, sélectionnez **Changer**, effectuez les modifications souhaitées, puis cliquez sur **Suivant**.

    Les paramètres de connexion réseau sont enregistrés.
12. Indiquez l'heure et la date, puis cliquez sur **Suivant**.

    pour modifier la configuration NTP après l'installation, utilisez YaST dans la ligne de commande de l'applicatif. Vous pouvez utiliser WebYast pour modifier l'heure et la date, mais pas pour la configuration NTP.

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

    ```
    rcntp restart
    ```
13. Définissez le mot de passe `root`, puis cliquez sur **Suivant**.

L'installation vérifie si la mémoire et l'espace disque disponibles sont suffisants. Si la mémoire disponible est inférieure à 2.5 Go, le programme d'installation ne vous permet pas de poursuivre et le bouton **Suivant** est grisé.

Si la mémoire disponible est supérieure à 2.5 Go mais inférieure à 6.7 Go, le programme d'installation affiche un message vous indiquant que la mémoire dont vous disposez est inférieure aux recommandations. Lorsque ce message apparaît, cliquez sur **Suivant** pour poursuivre l'installation.

14 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.

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

13.2.2 Installation de gestionnaires des collecteurs et de moteurs de corrélation

Pour installer un gestionnaire des collecteurs ou un moteur de corrélation sur un serveur VMware ESX en tant qu'image d'applicatif OVF :

1 Suivez la procédure des étapes 1 à 10 de la Section 13.2.1, « Installation de Sentinel », page 83.

2 Indiquez le nom d'hôte/l'adresse IP du serveur Sentinel auquel le gestionnaire des collecteurs doit se connecter.

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

4 Indiquez le nom d'utilisateur ActiveMQ, c'est-à-dire le nom d'utilisateur du gestionnaire des collecteurs ou du moteur de corrélation. Le nom d'utilisateur par défaut est `collectormanager` pour le gestionnaire des collecteurs et `correlationengine` pour le moteur de corrélation.

5 Indiquez le mot de passe de l'utilisateur ActiveMQ.

Les références utilisateur ActiveMQ sont stockées dans le fichier `/<répertoire_installation>/etc/opt/novell/sentinel/config/activemqusers.properties` situé sur le serveur Sentinel.

6 (Facultatif) Pour vérifier le mot de passe, consultez la ligne suivante du fichier `activemqusers.properties`.

Pour le gestionnaire des collecteurs :

```
collectormanager=<password>
```

Dans cet exemple, `collectormanager` est le nom de l'utilisateur et la valeur correspondante est le mot de passe.

Pour le moteur de corrélation :

```
correlationengine=<password>
```

Dans cet exemple, `correlationengine` est le nom de l'utilisateur et la valeur correspondante est le mot de passe.

7 Cliquez sur **Suivant**.

8 Acceptez le certificat.

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

Une fois l'installation terminée, le programme d'installation affiche un message indiquant que cet applicatif est le gestionnaire des collecteurs Sentinel ou le moteur de corrélation Sentinel (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.

13.3 Configuration post-installation de l'applicatif

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

13.3.1 Configuration de WebYaST

L'interface utilisateur de l'applicatif Sentinel est équipée de WebYaST. Il s'agit d'une console distante sur Internet qui permet de contrôler les applicatifs basés sur SUSE Linux Enterprise. Vous pouvez accéder, configurer et surveiller les applicatifs Sentinel avec WebYaST. La procédure suivante décrit brièvement les étapes de configuration de WebYaST. Pour plus d'informations sur la configuration détaillée, consultez le manuel *WebYaST User Guide (Guide de l'utilisateur WebYaST)* (http://www.novell.com/documentation/webyast/).

1 Loguez-vous à l'applicatif Sentinel.

2 Cliquez sur **Applicatif**.

3 Configurez le serveur Sentinel pour qu'il reçoive les mises à jour tel que décrit à la Section 13.3.3, « Enregistrement pour obtenir les mises à jour », page 86.

4 Cliquez sur **Suivant** pour terminer la configuration initiale.

13.3.2 Création de partitions

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 Section 6.6, « Planification des partitions pour le stockage de données », page 45. 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 Loguez-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 au Centre de contrôle YaST2 :

   ```
   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
    ```

13.3.3 Enregistrement pour obtenir les mises à jour

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

Procédez comme suit pour permettre à l'applicatif de recevoir les mises à jour :

1. Loguez-vous à l'applicatif Sentinel.
2. Cliquez sur **Applicatif** pour démarrer WebYaST.
3. Cliquez sur **Enregistrement**.
4. Indiquez l'ID de la messagerie sur laquelle vous souhaitez recevoir les mises à jour, ainsi que le nom du système et le code d'enregistrement de l'applicatif.
5. Cliquez sur **Enregistrer**.

13.3.4 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 NetIQ Customer Center et offre les fonctions essentielles de NetIQ Customer Center.

- « Conditions préalables » page 87
- « Configuration de l'applicatif » page 87
- « Mise à niveau de l'applicatif » page 88

Conditions préalables

- Procurez-vous les références NetIQ Customer Center de Sentinel pour obtenir les mises à jour de NetIQ. Pour plus d'informations sur l'obtention des références, contactez le support NetIQ.
- Vérifiez que SLES 11 SP3 est installé avec les paquetages suivants sur la machine sur laquelle vous souhaitez installer l'outil 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 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

Pour plus d'informations sur la configuration de l'applicatif avec SMT, reportez-vous à la documentation en anglais Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

Pour activer les espaces de stockage de l'applicatif, exécutez les commandes suivantes :

```
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
```

Mise à niveau de l'applicatif

Pour plus d'informations sur la mise à niveau de l'applicatif, consultez la Section 25.3, « Mise à niveau de l'applicatif à l'aide de SMT », page 138.

13.4 Arrêt et démarrage du serveur à l'aide de WebYaST

Vous pouvez démarrer et arrêter le serveur Sentinel à l'aide de l'interface Web comme suit :

1. Loguez-vous à l'applicatif Sentinel.
2. Cliquez sur **Applicatif** pour démarrer WebYaST.
3. Cliquez sur **System Services** (Services système).
4. Pour arrêter le serveur Sentinel , cliquez sur **Arrêter**.
5. Pour démarrer le serveur Sentinel , cliquez sur **Démarrer**.

14 Installation du gestionnaire des collecteurs NetFlow

Vous devez installer le gestionnaire des collecteurs NetFlow sur un ordinateur différent de celui sur lequel est installé le serveur Sentinel, le gestionnaire de collecteurs ou un moteur de corrélation.

14.1 Liste de contrôle de 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 37.
- ❒ Synchronisez l'heure à l'aide du protocole NTP (Network Time Protocol).

14.2 Installation du gestionnaire des collecteurs NetFlow

Vous pouvez installer les gestionnaires des collecteurs NetFlow en suivant l'une des méthodes ci-dessous :

- **Standard :** utilise les valeurs par défaut pour la configuration NetFlow.
- **Personnalisé :** vous permet de personnaliser le numéro de port du serveur Sentinel.

REMARQUE

- Pour envoyer des données de flux réseau au serveur Sentinel, vous devez être un administrateur, appartenir au rôle Fournisseur NetFlow ou disposer de l'autorisation Envoyer les données NetFlow.
- Si vous envisagez d'installer plusieurs gestionnaires des collecteurs NetFlow, vous devez créer un compte utilisateur pour chacun d'eux afin d'envoyer des données de flux réseau à Sentinel. Le fait de disposer de comptes utilisateur différents pour chaque gestionnaire des collecteurs NetFlow vous garantit un niveau de contrôle accru au niveau des gestionnaires autorisés à envoyer des données à Sentinel.

Pour installer le gestionnaire des collecteurs NetFlow, procédez comme suit :

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

   `https://<IP_Address_Sentinel_server>:8443`

   L'adresse <adresse_IP_serveur_Sentinel> est l'adresse IP ou le nom DNS du serveur Sentinel, et le numéro 8443 est 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 Sous l'en-tête Gestionnaire des collecteurs NetFlow, cliquez sur **Télécharger le programme d'installation**.

4 Cliquez sur **Enregistrer le fichier** pour enregistrer le programme d'installation à l'emplacement souhaité.

5 À l'invite de commande, 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 :

```
cd <directory_name>
```

7 Indiquez la commande suivante pour installer le gestionnaire des collecteurs NetFlow :

```
./install-netflow
```

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

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

10 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.

11 Indiquez si vous souhaitez procéder à une installation standard ou personnalisée.

12 Indiquez le nom d'hôte ou l'adresse IP du serveur Sentinel qui doit recevoir les données de flux réseau.

13 Si vous optez pour une installation personnalisée, indiquez le numéro de port du serveur Sentinel.

Le numéro de port par défaut est 8443.

14 Indiquez le nom d'utilisateur et le mot de passe pour vous authentifier auprès du serveur Sentinel.

REMARQUE : Assurez-vous que les références utilisateur indiquées disposent de l'autorisation Envoyer les données NetFlow ou des privilèges d'administration. Dans le cas contraire, l'installation se termine, mais l'authentification échoue lorsque le gestionnaire des collecteurs NetFlow envoie des données au serveur Sentinel.

L'installation se termine. Cela peut prendre quelques minutes pour que le gestionnaire des collecteurs NetFlow établisse une connexion avec le serveur Sentinel.

15 (Facultatif) Vous pouvez déterminer si l'installation du gestionnaire des collecteurs NetFlow s'est déroulée correctement en effectuant l'une des opérations suivantes :

- Vérifiez si les services du gestionnaire des collecteurs NetFlow sont en cours d'exécution :

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

- Vérifiez si le gestionnaire des collecteurs NetFlow a établi une connexion avec le serveur Sentinel :

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

- Vérifiez si le gestionnaire des collecteurs NetFlow apparaît dans la console Web Sentinel en cliquant sur **Collecte** > **NetFlow**.

16 Activez le réacheminement de trafic du flux réseau sur le périphérique à partir duquel vous souhaitez collecter des données de flux réseau.

Dans le cadre de l'activation de NetFlow sur le périphérique, vous devez indiquer l'adresse IP du serveur Sentinel et le port sur lequel le gestionnaire des collecteurs NetFlow reçoit des données du périphérique compatible NetFlow. Le numéro de port par défaut est 3578. Pour plus d'informations, consultez la documentation du périphérique compatible NetFlow approprié.

15 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.

15.1 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. Loguez-vous à l'interface Web de Sentinel à l'adresse https://<*adresse_IP*>:8443, 8443 étant le port par défaut du serveur Sentinel.
3. Cliquez sur **applications** dans la barre d'outils, puis sur **Applications**.
4. Cliquez sur **Démarrer le centre de contrôle** pour lancer Sentinel Control Center.
5. Dans la barre d'outils, cliquez sur **Gestion de source d'événements** > **Vue en direct**, puis cliquez sur **Outils** > **Importer le plug-in**.
6. Accédez au fichier de collecteur que vous avez téléchargé à l'Étape 1 et sélectionnez-le, puis cliquez sur **Suivant**.
7. 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.

15.2 Installation d'un connecteur

Procédez comme suit pour installer un connecteur :

1. Téléchargez le connecteur souhaité à partir du site Web des plug-ins Sentinel.
2. Loguez-vous à l'interface Web de Sentinel à l'adresse https://<*adresse_IP*>:8443, 8443 étant le port par défaut du serveur Sentinel.
3. Cliquez sur **application** dans la barre d'outils, puis sur **Applications**.
4. Cliquez sur **Démarrer le centre de contrôle** pour lancer Sentinel Control Center.
5. Dans la barre d'outils, sélectionnez **Gestion de source d'événements** > **Vue en direct**, puis cliquez sur **Outils** > **Importer le plug-in**.
6. Accédez au fichier de connecteur que vous avez téléchargé à l'Étape 1 et sélectionnez-le, puis cliquez sur **Suivant**.
7. 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.

16 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 en cours d'exécution :

  ```
  /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.

- Accédez à l'interface Web de Sentinel :

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

     ```
     https://<IP_Address/DNS_Sentinel_server:8443>
     ```

     IP_Address/DNS_Sentinel_server correspond à l'adresse IP ou au nom DNS du serveur Sentinel et 8443 indique le numéro de 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.

17 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.

17.1 Présentation de l'heure dans Sentinel

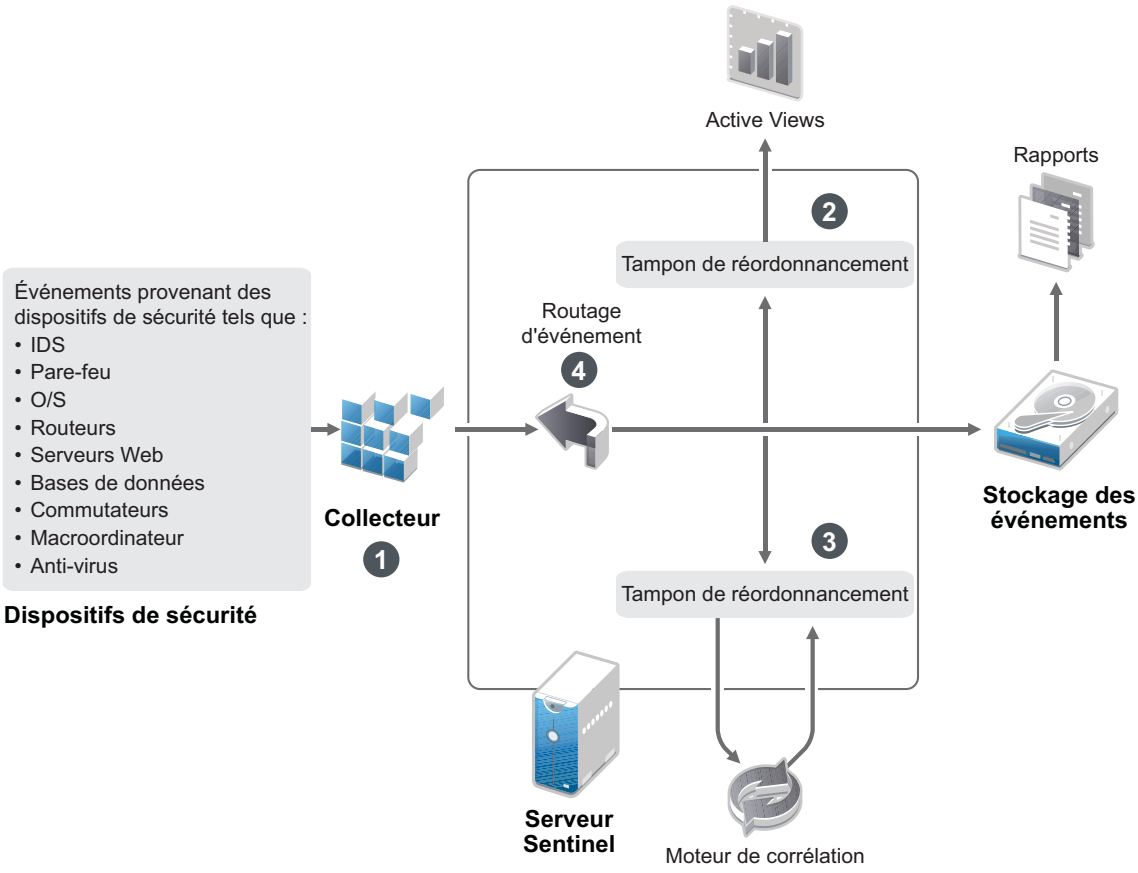
Sentinel est un système distribué constitué de plusieurs processus disséminés sur l'ensemble de votre réseau. En outre, la source d'événements peut être à l'origine d'un certain retard. Pour pallier cela, les processus Sentinel reclassent les événements dans l'ordre chronologique avant de les traiter.

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 du gestionnaire des collecteurs.
- **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 représente ces opérations effectuées par Sentinel :

Figure 17-1 *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 Active Views. Les événements dont l'heure a plus de 5 minutes d'avance par rapport à l'heure du serveur ne s'affichent pas dans Active Views, 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 le moteur de corrélation 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, le moteur de corrélation 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 du gestionnaire des collecteurs, Sentinel achemine directement l'événement vers le stockage d'événements, en ignorant les systèmes utilisant l'heure réelle tels que Correlation, Active Views et Security Intelligence.

17.2 Configuration de l'heure dans Sentinel

Le moteur de corrélation 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 le gestionnaire des collecteurs 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 le gestionnaire des collecteurs en tant que source de l'heure 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. Loguez-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 *NetIQ 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.

17.3 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>
```

17.4 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, le gestionnaire des collecteurs 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 du gestionnaire des collecteurs. 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 au serveur Sentinel depuis le gestionnaire des collecteurs et sont stockées dans la banque d'événements. Le fuseau horaire du gestionnaire des collecteurs 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 Internet, le champ EventTime en temps UTC est converti dans l'heure locale du navigateur, si bien que tous les événements sont présentés aux clients dans le fuseau horaire local. Si les utilisateurs souhaitent connaître l'heure locale de la source, ils peuvent consulter les champs ObserverTZ.

18 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 l'intermédiaire de la console Web 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`.

19 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.

19.1 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 Web de Sentinel à l'adresse `https://<adresse IP>:8443`, où 8443 est le port par défaut du serveur Sentinel.
2. Cliquez sur **Plug-ins** > **Catalogue**.

19.2 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

19.3 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 des Solution Packs) du manuel *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel)..

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 la console Web 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 *NetIQ Sentinel User Guide* (Guide de l'utilisateur NetIQ Sentinel).

19.4 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.

20 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`.

20.1 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. Terminez la configuration du mode FIPS 140-2 en effectuant les tâches mentionnées au Chapitre 21, « Fonctionnement de Sentinel en mode FIPS 140-2 », page 111.

20.2 Activation du mode FIPS 140-2 sur des gestionnaires des collecteurs et des moteurs de corrélation distants

Le mode FIPS 140-2 doit être activé sur le gestionnaire des collecteurs et le moteur de corrélation distants si vous souhaitez utiliser des communications certifiées FIPS lorsque le serveur Sentinel est exécuté en mode FIPS 140-2.

Pour configurer un gestionnaire des collecteurs ou un moteur de corrélation distant afin qu'il s'exécute en mode FIPS 140-2 :

1. Connectez-vous au système distant du gestionnaire des collecteurs ou du moteur de corrélation.
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 Terminez la configuration du mode FIPS 140-2 en effectuant les tâches mentionnées au Chapitre 21, « Fonctionnement de Sentinel en mode FIPS 140-2 », page 111.

21 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.

21.1 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 120.

21.2 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 120.
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>/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 120.
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>/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 120.
5. Redémarrez les services Sentinel sur l'ordinateur source.

21.3 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 120.
3. Connectez-vous à la console Web de Sentinel en tant qu'administrateur et configurez l'authentification LDAP.

   Pour plus d'informations, reportez-vous à la section « Configuring LDAP Authentication » (Configuration de l'authentification LDAP) du *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ 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`.

21.4 Mise à jour des certificats de serveur dans les gestionnaires des collecteurs et les moteurs de corrélation distants

Pour configurer des gestionnaires des collecteurs et des moteurs de corrélation distants existants afin qu'ils 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 le gestionnaire des collecteurs ou le moteur de corrélation en mode non-FIPS. Les gestionnaires des collecteurs distants 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 le gestionnaire des collecteurs ou le moteur de corrélation distant, vous devez copier le dernier certificat de serveur Sentinel sur le système distant afin de permettre au gestionnaire des collecteurs ou au moteur de corrélation de communiquer avec le serveur Sentinel.

Pour mettre à jour le certificat de serveur Sentinel dans le gestionnaire des collecteurs ou le moteur de corrélation distant :

1. Connectez-vous à l'ordinateur distant du gestionnaire des collecteurs ou du moteur de corrélation.
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.

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

21.5.1 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 120.

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 du gestionnaire des collecteurs 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 de gestionnaire des collecteurs 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.

21.5.2 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 120.

3 Configurez le connecteur.

21.5.3 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 120.

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.

21.5.4 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 120.

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 du gestionnaire des collecteurs distant 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 du gestionnaire des collecteurs distant 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.

21.5.5 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 120.

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 du gestionnaire des collecteurs distant 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 du gestionnaire des collecteurs distant 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 120.

21.5.6 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 un gestionnaire des collecteurs distant, vous devez copier le fichier `/etc/opt/novell/sentinel/config/rcm.cer` présent sur la machine du gestionnaire des collecteurs distant 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 120.

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.

21.5.7 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 120.

3 Configurez l'instance d'intégrateur.

21.5.8 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.

21.5.9 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 un gestionnaire des collecteurs distant en mode non-FIPS à connecter au serveur Sentinel en mode FIPS 140-2.

Pour plus d'informations, reportez-vous à la section Section 12.4, « Installation de gestionnaires des collecteurs et de moteurs de corrélation », page 73.

2 Déployez les connecteurs non-FIPS expressément sur le gestionnaire des collecteurs distant 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 un gestionnaire des collecteurs distant 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 7.1.

21.6 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 ces certificats à l'aide de l'interface utilisateur Sentinel comme d'habitude étant donné que le mode FIPS 140-2 est activé dans Sentinel. Vous devez les importer manuellement dans la base de données keystore FIPS.

Pour les sources d'événements qui utilisent des connecteurs déployés sur un gestionnaire des collecteurs distant, vous devez importer les certificats dans la base de données keystore FIPS du gestionnaire des collecteurs distant 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 le gestionnaire des collecteurs distant.
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 le gestionnaire des collecteurs distant.

21.7 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.

- Section 21.7.1, « Rétablissement du serveur Sentinel en mode non-FIPS », page 120
- Section 21.7.2, « Restauration des gestionnaires des collecteurs ou des moteurs de corrélation distants en mode non-FIPS », page 121

21.7.1 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. Loguez-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.

21.7.2 Restauration des gestionnaires des collecteurs ou des moteurs de corrélation distants en mode non-FIPS

Vous pouvez restaurer des gestionnaires des collecteurs ou des moteurs de corrélation distants en mode non-FIPS.

Pour restaurer un gestionnaire des collecteurs ou un moteur de corrélation distant en mode non-FIPS :

1. Connectez-vous au système distant du gestionnaire des collecteurs ou du moteur de corrélation.
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 le gestionnaire des collecteurs ou le moteur de corrélation distant.

V Mise à niveau de Sentinel

Cette section fournit des informations sur la mise à niveau de Sentinel et d'autres composants.

22 Liste de contrôle pour la mise en œuvre

Avant d'effectuer la mise à niveau de Sentinel, consultez la liste de contrôle suivante :

Tableau 22-1 *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 NetIQ 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

23 Conditions préalables

23.1 Conditions préalables pour Sentinel en mode FIPS

Les conditions préalables suivantes s'appliquent si vous avez mis à niveau Java vers une version antérieure en utilisant JRE 7 update 45 pour résoudre les problèmes de connexion entre les clients et Sentinel en mode FIPS, comme indiqué à la section Problèmes connus de Sentinel 7.2.2.

Si l'un des répertoires d'installation de Sentinel contient des liens symboliques, le programme d'installation de Sentinel ne procède pas à la mise à niveau. Lorsque vous téléchargez et installez JRE 7 update 45 pour mettre à niveau Java vers une version antérieure, le dossier JRE contient un sous-dossier nommé `man`, qui comporte des liens symboliques. Vous devez donc supprimer le dossier `man` pour réussir la mise à niveau vers Sentinel 7.3 ou version ultérieure. Cependant, si vous avez téléchargé et installé JDK 7 update 45 au lieu de JRE 7 update 45, le dossier `man` ne contient pas de liens symboliques. Il est donc inutile de le supprimer.

Pour supprimer le dossier man, procédez comme suit :

1. Connectez-vous au serveur Sentinel en tant qu'utilisateur novell.
2. Entrez la commande suivante pour changer de répertoire :

   ```
   cd /opt/novell/sentinel/jre/
   ```
3. Supprimez le dossier `man` :

   ```
   rm -rf man
   ```

23.2 Conditions préalables pour les versions antérieures à Sentinel 7.1.1

Sentinel 7.1.1 (et versions ultérieures) inclut MongoDB version 2.4.1. MongoDB 2.4 nécessite la suppression des noms d'utilisateur en double dans la base de données. Si vous effectuez la mise à niveau de Sentinel à partir d'une version antérieure à 7.1.1, vérifiez s'il existe des utilisateurs en double et, le cas échéant, supprimez-les.

Pour identifier les utilisateurs en double, procédez comme suit :

1. Connectez-vous au serveur Sentinel 7.1 ou version antérieure en tant qu'utilisateur Novell.
2. Accédez au répertoire suivant :

   ```
   cd opt/novell/sentinel/3rdparty/mongodb/bin
   ```
3. Exécutez les commandes suivantes pour vérifier la présence d'utilisateurs en double :

   ```
   ./mongo --port 27017 --host "localhost"
   ```

   ```
   use analytics
   ```

```
db.system.users.find().count()
```

Si le `nombre` est supérieur à 1, cela signifie qu'il existe des utilisateurs en double.

Pour supprimer les utilisateurs en double, procédez comme suit :

1. Exécutez la commande suivante pour dresser la liste des utilisateurs :

   ```
   db.system.users.find().pretty()
   ```

   Cette commande répertorie les utilisateurs, ainsi que le entrées en double. Le premier utilisateur de la liste est l'utilisateur initial. Vous devez conserver cet utilisateur et supprimer les autres.

2. Exécutez la commande suivante pour supprimer les utilisateurs en double :

   ```
   db.system.users.remove({ _id : ObjectId("object_ID") })
   ```

3. Exécutez la commande suivante pour vérifier que les utilisateurs en double ont bien été supprimés :

   ```
   db.system.users.find().pretty()
   ```

4. Basculez vers les informations de connexion de l'administrateur de la base de données :

   ```
   use admin
   ```

5. Répétez la procédure de l'Étape 1 à l'Étape 3 afin de vérifier la présence d'utilisateurs `dbauser` en double dans la base de données admin et, le cas échéant, supprimez-les.

24 Mise à niveau de l'installation traditionnelle de Sentinel

24.1 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
2. (Facultatif) 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
3. Téléchargez la dernière version du programme d'installation sur le site Web de téléchargement NetIQ.
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 (Conditionnel) Si vous effectuez une mise à niveau à partir de Sentinel 7.1.1 ou d'une version antérieure, par défaut, le programme d'installation ne fait pas migrer les données SI (Security Intelligence). Pour faire migrer des données SI à partir de Sentinel 7.1.1 ou d'une version antérieure, activez manuellement la migration des données SI en procédant comme suit :

   14a Connectez-vous en tant qu'utilisateur novell.

   ```
   su novell
   ```

   14b Ouvrez le fichier `/etc/opt/novell/sentinel/config/server.xml`.

   14c Ajoutez la propriété suivante dans la section du composant `BaseliningRuntime` :

   ```
   <property name="baselining.migration.check">true</property>
   ```

   14d Redémarrez le serveur Sentinel.

15 Pour mettre à niveau les systèmes du gestionnaire des collecteurs et du moteur de corrélation, reportez-vous à la Section 24.3, « Mise à niveau du gestionnaire des collecteurs ou du moteur de corrélation », page 132.

24.2 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

2. (Facultatif) 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
3. Téléchargez les fichiers d'installation sur le site Web de téléchargement NetIQ.
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 silencieux, 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 effectuez une mise à niveau à partir de Sentinel 7.1.1 ou d'une version antérieure, par défaut, le programme d'installation ne fait pas migrer les données SI (Security Intelligence). Pour faire migrer des données SI à partir de Sentinel 7.1.1 ou d'une version antérieure, activez manuellement la migration des données SI en procédant comme suit :

16a Connectez-vous en tant qu'utilisateur novell.

```
su novell
```

16b Ouvrez le fichier `/etc/opt/novell/sentinel/config/server.xml`.

16c Ajoutez la propriété suivante dans la section du composant `BaseliningRuntime` :

```
<property name="baselining.migration.check">true</property>
```

16d Redémarrez le serveur Sentinel.

24.3 Mise à niveau du gestionnaire des collecteurs ou du moteur de corrélation

Procédez comme suit pour mettre à niveau le gestionnaire des collecteurs ou le moteur de corrélation :

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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

2 Connectez-vous à l'interface Web Sentinel en tant qu'utilisateur avec le rôle d'administrateur.

3 Sélectionnez **Téléchargements**.

4 Cliquez sur **Télécharger le programme d'installation** dans la section du programme d'installation du gestionnaire des collecteurs.

La fenêtre qui s'affiche vous propose d'ouvrir ou d'enregistrer le fichier du programme d'installation sur la machine locale.

5 Enregistrez le fichier.

6 Copiez le fichier à un emplacement temporaire.

7 Dézippez le contenu du fichier.

8 Exécutez le script suivant :

Pour le gestionnaire des collecteurs :

```
./install-cm
```

Pour le moteur de corrélation :

```
./install-ce
```

9 Suivez les instructions affichées pour terminer l'installation.

25 Mise à niveau de l'applicatif Sentinel

Les procédures décrites dans ce chapitre vous guident pour mettre à niveau l'applicatif Sentinel, mais aussi les applicatifs de gestionnaire des collecteurs et de moteur de corrélation.

25.1 Mise à niveau de l'applicatif à l'aide de Zypper

Pour mettre à niveau l'applicatif à l'aide du correctif zypper :

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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
2. (Facultatif) 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).
3. Loguez-vous à la console d'appliance en tant qu'utilisateur `root`.
4. Exécutez la commande suivante :

   ```
   /usr/bin/zypper patch
   ```

5. (Conditionnel) Si vous effectuez une mise à niveau à partir de Sentinel 7.0.1 ou d'une version antérieure, entrez `1` pour accepter le changement de fournisseur (NetIQ au lieu de Novell).
6. (Conditionnel) Si vous effectuez une mise à niveau à partir d'une version de Sentinel antérieure à 7.2, le programme d'installation affiche un message vous demandant de résoudre les problèmes de dépendance pour certains paquetages d'applicatif. Entrez `1` pour désinstaller les paquetages dépendants.
7. Entrez `Y` pour continuer.
8. Entrez `Yes` pour accepter l'accord de licence.
9. Redémarrez l'applicatif Sentinel.
10. Videz le cache de votre navigateur Web pour afficher la dernière version de Sentinel.
11. 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.

12 (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.

12a Connectez-vous en tant qu'utilisateur novell.

```
su novell
```

12b Accédez au dossier `bin` :

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

12c Supprimez tous les anciens fichiers postgreSQL à l'aide de la commande suivante :

```
./delete_old_cluster.sh
```

13 (Conditionnel) Si vous effectuez une mise à niveau à partir de Sentinel 7.1.1 ou d'une version antérieure, par défaut, le programme d'installation ne fait pas migrer les données SI (Security Intelligence). Pour faire migrer des données SI à partir de Sentinel 7.1.1 ou d'une version antérieure, activez manuellement la migration des données SI en procédant comme suit :

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

```
su novell
```

13b Ouvrez le fichier `/etc/opt/novell/sentinel/config/server.xml`.

13c Ajoutez la propriété suivante dans la section du composant `BaseliningRuntime` :

```
<property name="baselining.migration.check">true</property>
```

13d Redémarrez le serveur Sentinel.

REMARQUE : pour mettre à niveau le gestionnaire de collecteurs ou le moteur de corrélation, suivez la procédure de l'Étape 3 à l'Étape 9.

25.2 Mise à niveau de l'applicatif à l'aide de WebYast

REMARQUE : en cas de mise à niveau de l'applicatif à partir de versions antérieures à Sentinel 7.2, vous devez utiliser l'utilitaire de ligne de commande Zypper, car une intervention de l'utilisateur est requise pour effectuer cette opération. WebYaST ne permet pas ce type d'intervention. Pour plus d'informations sur l'utilisation de zypper pour mettre à niveau l'applicatif, reportez-vous à la Section 25.1, « Mise à niveau de l'applicatif à l'aide de Zypper », page 135.

---

1 Loguez-vous à l'applicatif Sentinel en tant qu'utilisateur avec le rôle d'administrateur.

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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

3 (Facultatif) 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

4 **Si vous souhaitez mettre à niveau l'applicatif Sentinel**, cliquez sur **Applicatif** pour lancer WebYaST.

5 **Si vous souhaitez mettre à niveau un applicatif de gestionnaire de collecteurs ou de moteur de corrélation**, indiquez l'URL de l'ordinateur concerné en utilisant le port 4984 pour lancer WebYaST, sous la forme `https://<adresse_IP>:4984`, où `<adresse_IP>` est l'adresse IP du gestionnaire de collecteurs ou du moteur de corrélation. Effectuez les opérations de l'Étape 7 à l'Étape 10.

6 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

7 (Facultatif) Si vous n'avez pas encore enregistré l'applicatif pour les mises à jour automatiques, enregistrez-le.

Pour plus d'informations, reportez-vous à la section Section 13.3.3, « Enregistrement pour obtenir les mises à jour », page 86.

Si l'applicatif n'est pas enregistré, Sentinel vous l'indique en affichant un avertissement en jaune.

8 Pour vérifier si des mises à jour sont disponibles, cliquez sur **Mises à jour**.

Les mises à jour disponibles s'affichent.

9 Sélectionnez les mises à jour et appliquez-les.

Les mises à jour peuvent prendre quelques minutes. Une fois la mise à jour effectuée, la page de connexion de WebYaST apparaît.

Avant de mettre à jour l'applicatif, WebYaST arrête automatiquement le service Sentinel. Vous devez redémarrer ce service manuellement une fois la mise à niveau terminée.

10 Redémarrez le service Sentinel à l'aide de l'interface Web.

Pour plus d'informations, reportez-vous à la section Section 13.4, « Arrêt et démarrage du serveur à l'aide de WebYaST », page 88.

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 Connectez-vous en tant qu'utilisateur 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 (Conditionnel) Si vous effectuez une mise à niveau à partir de Sentinel 7.1.1 ou d'une version antérieure, par défaut, le programme d'installation ne fait pas migrer les données SI (Security Intelligence). Pour faire migrer des données SI à partir de Sentinel 7.1.1 ou d'une version antérieure, activez manuellement la migration des données SI en procédant comme suit :

14a Passez à l'utilisateur Novell :

```
su novell
```

14b Ouvrez le fichier `/etc/opt/novell/sentinel/config/server.xml`.

14c Ajoutez la propriété suivante dans la section du composant `BaseliningRuntime` :

```
<property name="baselining.migration.check">true</property>
```

14d Redémarrez le serveur Sentinel.

25.3 Mise à niveau de l'applicatif 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 Section 13.3.4, « Configuration de l'applicatif avec l'outil SMT (Subscription Management Tool) », page 86.

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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

3 (Facultatif) 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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

4 Loguez-vous à la console d'appliance 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
```

26 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 Déploiement de Sentinel pour une haute disponibilité

Cette annexe décrit comment installer NetIQ 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 oeuvre de la haute disponibilité et de la reprise après sinistre dans votre environnement Sentinel, contactez le support NetIQ.

REMARQUE : la configuration en mode Haute disponibilité (HA) est prise en charge uniquement sur le serveur Sentinel. Cependant, les gestionnaires de collecteurs et les moteurs de corrélation peuvent toujours communiquer avec le serveur Sentinel HA.

27 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.

27.1 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).

27.2 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 cluster 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.

REMARQUE : 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.

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 cluster. 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'un cluster qui utilise le système de stockage partagé iSCSI et place les fichiers binaires/la configuration de l'application sur chaque noeud de cluster.

27.3 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.

27.4 Fencing (Isolement)

Au sein d'un cluster 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.

28 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 SUSE Linux Enterprise Server (SLES) 11 SP3
  - Paquetage SUSE Linux Enterprise Server High Availability Extension (SLES HAE)
  - Logiciel Sentinel (y compris RPM HA)
- ❒ **(Conditionnel) Pour les installations HA traditionnelles**, vérifiez que le programme d'installation de Sentinel (fichier TAR) et l'image ISO SLE HAE (SUSE Linux High Availability Extension) avec licences valides sont disponibles.
- ❒ **(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 :

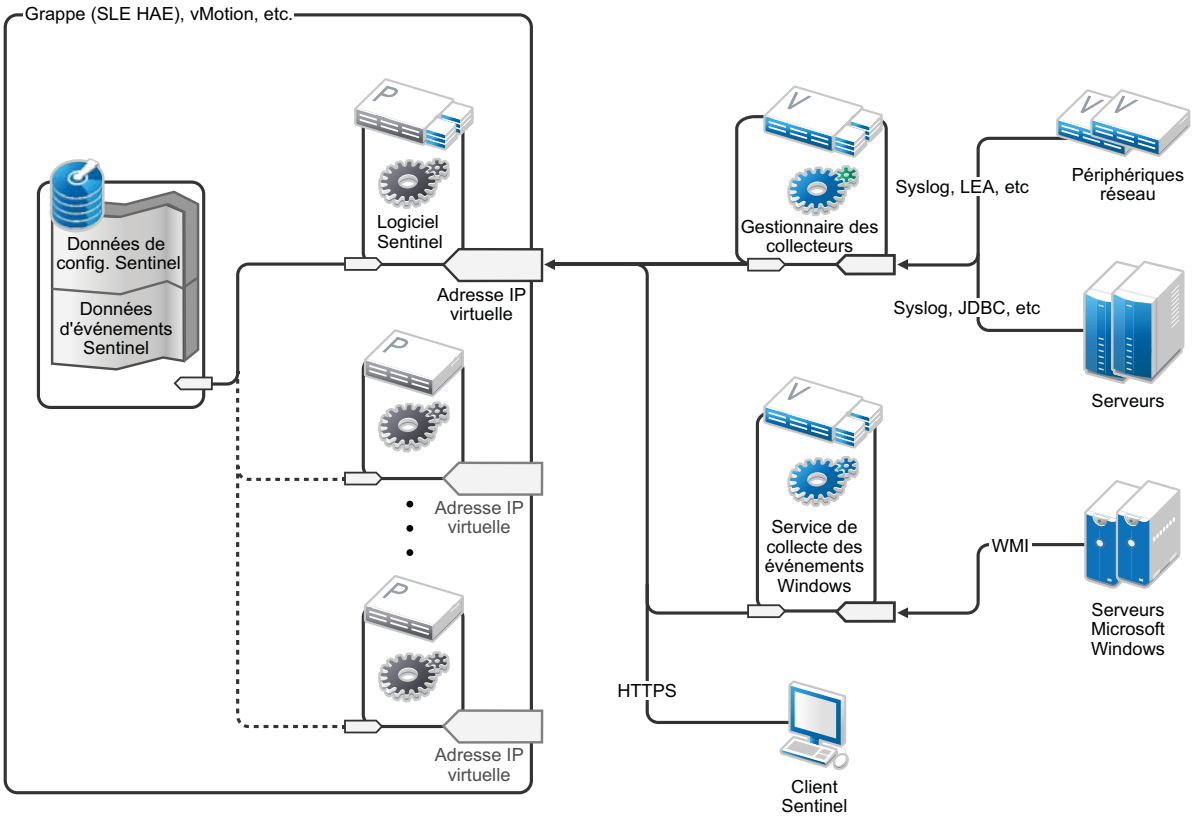
     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```
- ❒ Assurez-vous que chaque noeud de grappe qui héberge les services Sentinel respecte la configuration requise spécifiée au Chapitre 5, « Configuration du système », page 37.
- ❒ Veillez à disposer d'un espace de stockage suffisant 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 37. NetIQ recommande une machine virtuelle SUSE Linux standard configurée avec les cibles iSCSI pour l'espace de stockage partagé.
- ❒ Veillez à disposer, au minimum, de deux noeuds de grappe disposant des ressources nécessaires pour exécuter Sentinel dans l'environnement du client. NetIQ recommande deux machines virtuelles SUSE Linux.
- ❒ 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). NetIQ recommande une adresse IP dédiée pour se connecter à la cible iSCSI.

- ❒ Veillez à disposer d'une adresse IP virtuelle pouvant être migrée d'un noeud de grappe à 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. NetIQ recommande une simple adresse IP de monodiffusion. Cependant, l'utilisation d'une adresse de multidiffusion est recommandée pour les environnements de production.

29 Installation et configuration

Cette section fournit les procédures d'installation et de configuration de Sentinel dans un environnement à haute disponibilité (HA).

Le diagramme suivant illustre une architecture haute disponibilité active-passive :



29.1 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 cluster doit respecter la configuration système requise définie au Chapitre 5, « Configuration du système », page 37 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 37 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 55 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).

NetIQ recommande la configuration suivante :

- **(Conditionnel) Pour les installations à haute disponibilité traditionnelles :**
  - Deux machines virtuelles de noeud de cluster SUSE Linux 11 SP3.
  - (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'applicatif 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 Section 13.1.2, « Installation de Sentinel », page 80.
- 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 cluster, l'espace temporaire, etc. Consultez la configuration système requise pour SUSE Linux et SLE HAE, ainsi que la configuration requise pour l'application Sentinel.
- Une machine virtuelle SUSE Linux 11 SP3 configurée avec les 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 les configurations système requises pour SUSE Linux et le stockage des données d'événements de Sentinel.

REMARQUE : dans un cluster 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 de cluster internes.

29.2 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.

Exemple de configuration de l'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 : NetIQ conseille de configurer l'espace de stockage partagé et de le tester en le montant sur chaque noeud de la grappe. Toutefois, la configuration de grappe gérera le montage réel de l'espace de stockage.

NetIQ recommande d'appliquer la procédure suivante pour créer des cibles iSCSI hébergées par une machine virtuelle SUSE Linux :

1. Connectez-vous à la machine virtuelle `storage03` créée à l'étape de Configuration initiale, et démarrez une session de console.
2. Utilisez la commande `dd` pour créer un fichier vide de la taille souhaitée pour l'espace de stockage primaire de Sentinel :

   ```
   dd if=/dev/zero of=/localdata count=10240000 bs=1024
   ```

3. Créez un fichier de 10 Go rempli de zéros (copié à partir du fichier `/dev/zero pseudo-device`). Pour en savoir plus sur les options de ligne de commande, consultez la page d'information ou la page principale de la commande `dd`.
4. Répétez les étapes 1 à 3 afin de créer un fichier pour l'espace de stockage secondaire :

   ```
   dd if=/dev/zero of=/networkdata count=10240000 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.

29.2.1 Configuration des cibles iSCSI

Configurez les fichiers `localdata` et `networkdata` en tant que cibles iSCSI :

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 servira pour les communications iSCSI internes.
6. Cliquez sur **Suivant**, puis sur **OK**.
7. Dans l'écran principal, sélectionnez **Network Services** (Services réseau) > **iSCSI Target** (Cible iSCSI).
8. Si vous y êtes invité, installez le logiciel requis (`RPM iscsitarget`) à partir du support SUSE Linux 11 SP3.
9. Cliquez sur **Service**, sélectionnez l'option **When Booting** (Au démarrage) pour que le service se lance au démarrage du système d'exploitation.
10. Cliquez sur **Global**, puis sélectionnez **No Authentication** (Pas d'authentification) car l'agent de ressource OCF actuel pour iSCSI ne prend pas en charge l'authentification.
11. 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.
12. Cliquez sur **Ajouter** pour ajouter un nouveau numéro d'unité logique.
13. 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`.

14 Répétez les étapes 12 et 13 et ajoutez le numéro d'unité logique 1 avec `/networkdata` cette fois.

15 Laissez les valeurs par défaut des autres options. Cliquez sur **OK**, puis sur **Suivant**.

16 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.

17 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.

29.2.2 Configuration des initiateurs iSCSI

Procédez comme suit pour formater les périphériques :

1 Connectez-vous à l'un des noeuds de cluster (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 open-iscsi) à partir du support SUSE Linux 11 SP3.

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 Spécifiez l'adresse IP iSCSI cible (10.0.0.3), sélectionnez **No Authentication** (Pas d'authentification), puis cliquez sur **Suivant**.

12 Sélectionnez la cible iSCSI découverte avec l'adresse IP 10.0.0.3, puis sélectionnez **Se connecter**.

13 Basculez sur l'option Automatique dans la liste déroulante **Startup** (Démarrage) et sélectionnez **No Authentication** (Pas d'authentification), puis 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 cluster.

16 Dans le menu principal de YaST, sélectionnez **Système** > **Partitioner** (Partitionneur).

17 Dans la vue du système, de nouveaux disques durs doivent apparaître dans la liste (notamment `/dev/sdb` et `/dev/sdc`). Ils présentent le type IET-VIRTUAL-DISK. 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 ext3 principale, mais ne le montez pas. Vérifiez que l'option Do not mount partition (Ne pas monter la partition) est sélectionnée.

19 Sélectionnez **Suivant**, puis **Terminer** après avoir contrôlé les modifications à apporter. Si vous créez une seule grande partition sur cette unité logique iSCSI partagée, vous devez obtenir une partition `/dev/sdb1` ou un disque au format similaire (appelé `/dev/<SHARED1>` comme ci-dessous).

20 Retournez dans le partitionneur et répétez le processus de partitionnement/formatage (étapes 16 à 19) pour `/dev/sdc` ou tout autre périphérique de bloc correspondant au système de 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 oeuvre 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 à l'étape 5 par une adresse IP différente.

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 5 par une autre adresse IP.

29.3 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.

NetIQ recommande d'installer Sentinel sur chaque noeud 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.

29.3.1 Installation sur le premier noeud

- « Installation HA traditionnelle » page 157
- « Installation de l'applicatif Sentinel HA » page 157

Installation HA traditionnelle

1. Connectez-vous à l'un des noeuds de cluster (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 cluster.
3. 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
   ```
4. Exécutez l'installation standard et configurez le produit comme il se doit. Le programme d'installation installe les fichiers binaires et de configuration, ainsi que les bases de données. Le programme d'installation configure également les références de connexion, les paramètres de configuration et les ports réseau.
5. Démarrez Sentinel et testez les fonctions de base. Vous pouvez utiliser l'adresse IP de noeud de cluster 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 cluster (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 Indiquez l'option pour sélectionner le type de configuration Sentinel.

   3c Indiquez `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/sentinel /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/
```

29.3.2 Installation sur les noeuds suivants

- « Installation HA traditionnelle » page 158
- « Installation de l'applicatif Sentinel HA » page 159

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 cluster 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 cluster (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
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props
```

```
cd /
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/sentinel
   ```

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 cluster.

29.4 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.

NetIQ recommande de suivre la procédure ci-dessous pour configurer SUSE Linux High Availability Extension avec une couche d'agents de ressource spécifique à 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 du cluster 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
```

29.5 Configuration du cluster

Le logiciel de cluster doit être configuré pour enregistrer chaque noeud en tant que membre du cluster. 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.

NetIQ recommande 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 SUSE Linux 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. Utilisez la commande `dd` pour créer un fichier vide de la taille souhaitée :

   ```
   dd if=/dev/zero of=/sbd count=1024 bs=1024
   ```

2. Créez un fichier de 1 Mo rempli de zéros (copié à partir de `/dev/zero` pseudo-device).
3. Exécutez YaST à partir de la ligne de commande ou utilisez l'interface graphique : `/sbin/yast`
4. Sélectionnez **Network Services** (Services réseau) > **iSCSI Target** (Cible iSCSI).
5. Cliquez sur **Cibles**, puis sélectionnez la cible existante.
6. Sélectionnez **Modifier**. L'interface utilisateur propose une liste des numéros d'unité logique disponibles.
7. Cliquez sur **Ajouter** pour ajouter un numéro d'unité logique.
8. 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.
9. Laissez 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.
10. Cliquez sur **Terminer** pour quitter la configuration. Redémarrez les services si nécessaire. Quittez YaST.

REMARQUE : la procédure suivante nécessite que chaque noeud de cluster puisse résoudre le nom d'hôte de l'ensemble des noeuds de cluster (faute de quoi le fichier csync2 de synchronisation des services échouera). Si 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 cluster (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 **automatique**, ni **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. Exécutez la commande `sleha-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 que vous avez trouvé ci-dessus (vous pouvez utiliser Tab pour compléter le chemin automatiquement).
14. Suivez les étapes de l'assistant et veillez à ce qu'aucune erreur ne soit signalée.
15. Démarrez YaST.
16. Sélectionnez **High Availability** (Haute disponibilité) > **Cluster** (ou simplement Cluster sur certains systèmes).
17. Dans la zone à gauche, veillez à ce que l'option **Communication Channels** (Canaux de communication) soit sélectionnée.
18. 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).
19. 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 cluster : 172.16.0.2.
20. Cliquez sur **Terminer** pour achever la configuration.
21. Quittez YaST.
22. 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 **automatique**, ni **No Authentication** (Pas d'authentification).

6 Sélectionnez **OK** pour quitter l'outil de l'initiateur iSCSI.

7 Exécutez la commande suivante :`sleha-join`

8 Entrez l'adresse IP du premier noeud de cluster.

(Conditionnel) Si la grappe ne démarre pas correctement, procédez comme suit :

1 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.

2 Exécutez `/etc/rc.d/openais start` sur `node02`.

(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`.

3 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
```

29.6 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.

NetIQ recommande la procédure suivante pour la configuration des ressources :

NetIQ fournit un script `crm` facilitant 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) Si vous rencontrez des problèmes lors de l'arrivée de nouvelles ressources dans la grappe, exécutez la commande `/etc/rc.d/openais restart` sur node02.

4. Le script `install-resources.sh` vous demande d'entrer quelques valeurs, à savoir l'adresse IP virtuelle que vous souhaitez voir utilisée 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 NetIQ, 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 le cluster. Vous pouvez examiner la façon dont elles sont configurées et groupées dans l'outil de gestion du cluster, par exemple, en exécutant l'état crm.

29.7 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 la console Web de Sentinel, cliquez sur **Stockage**.
2. Sélectionnez **Configuration**.
3. Sélectionnez l'une des cases d'option sous le stockage secondaire non configuré.

NetIQ conseille d'utiliser 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 : dans la mesure où NetIQ recommande d'utiliser une cible iSCSI pour cette solution, la cible est montée en tant que répertoire à utiliser comme espace de 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. Utilisez la console Web ou exécutez la commande :

   ```
   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 Web 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`.

NetIQ recommande l'utilisation des versions simples des ressources requises telles que l'agent de ressource simple du système de fichiers. Si les clients le souhaitent, ils peuvent utiliser des ressources de grappe plus sophistiquées telles que cLVM (une version de volume logique du système de fichiers).

30 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.

30.1 Conditions préalables

- Téléchargez la dernière version du programme d'installation depuis le site de téléchargement de NetIQ.
- 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. 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 <watchdog driver name>
     ```

30.2 Mise à niveau d'une installation Sentinel HA traditionnelle

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 <install_filename>
```

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 *NetIQ 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 <install_filename>
```

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 :

```
run 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
```

30.3 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, ainsi que par le biais de WebYast.

- Section 30.3.1, « Mise à niveau de l'applicatif Sentinel HA à l'aide de Zypper », page 169
- Section 30.3.2, « Mise à niveau de l'applicatif Sentinel HA à l'aide de WebYast », page 171

30.3.1 Mise à niveau de l'applicatif Sentinel HA à l'aide de Zypper

Avant de procéder à la mise à niveau, vous devez enregistrer toutes les grappes d'applicatif via WebYast. Pour plus d'informations, reportez-vous à la section Section 13.3.3, « Enregistrement pour obtenir les mises à jour », page 86. 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 Téléchargez les mises à jour de l'application Sentinel HA.

```
zypper -v patch -d
```

Cette commande télécharge les mises à jour des paquetages installés sur l'applicatif, y compris Sentinel, dans `/var/cache/zypp/packages`.

3b 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.

3c Une fois les mises à jour téléchargées, installez-les à l'aide de la commande suivante :

```
rpm -Uvh /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/rpm/
noarch/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/
rpm/x86_64/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-
Updates/rpm/i586/*.rpm --excludepath=/var/opt/novell/
```

3d Exécutez le script suivant pour terminer l'opération de mise à niveau :

```
/var/adm/update-scripts/sentinel_server_ha_x86_64-update-<version>-
overlay_files.sh
```

3e Une fois la mise à niveau terminée, redémarrez la pile de grappes.

```
rcopenais start
```

Répétez l'étape 3 pour tous les noeuds passifs de la grappe.

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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

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 à l'applicatif Sentinel en tant qu'administrateur.

4d Pour mettre à niveau l'applicatif Sentinel, cliquez sur **Applicatif** afin de lancer WebYaST.

4e Pour vérifier si des mises à jour sont disponibles, cliquez sur **Mises à jour**.

4f Sélectionnez les mises à jour et appliquez-les.

Les mises à jour peuvent prendre quelques minutes. Une fois la mise à jour effectuée, la page de connexion à WebYaST s'affiche.

Avant de mettre à jour l'applicatif, WebYaST arrête automatiquement le service Sentinel. Vous devez redémarrer ce service manuellement une fois la mise à niveau terminée.

4g Videz le cache de votre navigateur Web pour afficher la dernière version de Sentinel.

4h Une fois la mise à niveau terminée, redémarrez la pile de grappes.

```
rcopenais start
```

4i Exécutez la commande suivante pour synchroniser les éventuelles modifications dans les fichiers de configuration :

```
run 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 que 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
```

30.3.2 Mise à niveau de l'applicatif Sentinel HA à l'aide de WebYast

Avant de procéder à la mise à niveau, vous devez enregistrer toutes les grappes d'applicatif via WebYast. Pour plus d'informations, reportez-vous à la section Section 13.3.3, « Enregistrement pour obtenir les mises à jour », page 86. 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 les noeuds passifs de la grappe en procédant comme suit :

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 Indiquez l'URL du noeud passif de la grappe en utilisant le port 4984 afin de lancer WebYaST avec le format `https://<adresse_IP>:4984`, où *<adresse_IP>* est l'adresse IP du noeud passif. Connectez-vous à l'applicatif Sentinel en tant qu'administrateur.

3c Pour vérifier si des mises à jour sont disponibles, cliquez sur **Mises à jour**.

3d Sélectionnez les mises à jour et appliquez-les.

Les mises à jour peuvent prendre quelques minutes. Une fois la mise à jour effectuée, la page de connexion à WebYaST s'affiche.

3e Une fois la mise à niveau terminée, redémarrez la pile de grappes.

```
rcopenais start
```

Répétez l'Étape 4 pour tous les noeuds passifs de la grappe.

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 *NetIQ Sentinel Administration Guide* (Guide d'administration de NetIQ Sentinel).

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 à l'applicatif Sentinel en tant qu'administrateur.

4d Pour mettre à niveau l'applicatif Sentinel, cliquez sur **Applicatif** afin de lancer WebYaST.

4e Pour vérifier si des mises à jour sont disponibles, cliquez sur **Mises à jour**.

4f Sélectionnez les mises à jour et appliquez-les.

Les mises à jour peuvent prendre quelques minutes. Une fois la mise à jour effectuée, la page de connexion à WebYaST s'affiche.

Avant de mettre à jour l'applicatif, WebYaST arrête automatiquement le service Sentinel. Vous devez redémarrer ce service manuellement une fois la mise à niveau terminée.

4g Videz le cache de votre navigateur Web pour afficher la dernière version de Sentinel.

4h Une fois la mise à niveau terminée, redémarrez la pile de grappes.

```
rcopenais start
```

4i Exécutez la commande suivante pour synchroniser les éventuelles modifications dans les fichiers de configuration :

```
run 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 que 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
```

31 Sauvegarde et récupération

Le cluster 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 du cluster, celui-ci bascule automatiquement vers un autre noeud du cluster 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.

31.1 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 *NetIQ 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 le cluster car le noeud passif du cluster 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.

31.2 Récupération

31.2.1 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 du cluster peut être utilisée pour rétablir l'exécution du service sur le noeud de cluster initial, si vous le souhaitez.

31.2.2 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 au cluster décrites dans ce document, le noeud est restauré dans un état opérationnel. L'interface utilisateur de gestion du cluster peut être utilisée pour rétablir l'exécution du service sur le noeud de cluster initial, si vous le souhaitez.

31.2.3 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 *NetIQ 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 le cluster car le noeud passif du cluster 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 noeud sur lequel ils peuvent être utilisés.

VII Annexes

A Dépannage

Cette section présente certains des problèmes pouvant survenir pendant l'installation, ainsi que les actions à entreprendre pour les résoudre.

A.1 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.

A.2 L'UUID n'est pas créé pour les gestionnaires des collecteurs avec création d'image ou le moteur de corrélation

Si vous créez l'image d'un serveur de gestionnaire des collecteurs (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 du gestionnaire des collecteurs. Cela s'explique par la présence d'UUID dupliqués.

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

1. Supprimez le fichier `host.id` ou `sentinel.id` stocké dans le dossier `/var/opt/novell/sentinel/data`.
2. Redémarrez le gestionnaire des collecteurs.

   Le gestionnaire des collecteurs génère automatiquement l'UUID.

A.3 Après la connexion, l'interface Web 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**.

B Désinstallation

Cette annexe fournit des informations sur la désinstallation de Sentinel et les tâches à effectuer après la désinstallation.

B.1 Liste de contrôle pour la désinstallation

Utilisez la liste de contrôle suivante pour désinstaller Sentinel :

- ❒ Désinstallez le serveur Sentinel.
- ❒ Désinstallez le gestionnaire des collecteurs et le moteur de corrélation, le cas échéant.
- ❒ Effectuez les tâches de post-désinstallation pour finaliser la désinstallation de Sentinel.

B.2 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.

B.2.1 Désinstallation du serveur Sentinel

Procédez comme suit pour désinstaller le serveur Sentinel :

1. Loguez-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 :

   ```
   /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.

B.2.2 Désinstallation du gestionnaire des collecteurs et du moteur de corrélation

Procédez comme suit pour désinstaller le gestionnaire des collecteurs et le moteur de corrélation :

1 Connectez-vous en tant qu'utilisateur `root` au gestionnaire des collecteurs et au moteur de corrélation.

REMARQUE : Vous ne pouvez pas désinstaller le gestionnaire des collecteurs ni le moteur de corrélation distant 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 le gestionnaire des collecteurs ou le moteur de corrélation, ainsi que toutes les données associées, vont être intégralement supprimés.

4 Saisissez o pour supprimer le gestionnaire des collecteurs ou le moteur de corrélation.

Le script arrête d'abord le service et le supprime ensuite complètement. Toutefois, les icônes du gestionnaire des collecteurs et du moteur de corrélation sont toujours présentes à l'état inactif dans l'interface Web.

5 Effectuez les étapes suivantes pour supprimer manuellement le gestionnaire des collecteurs et le moteur de corrélation de l'interface Web :

Gestionnaire des collecteurs :

1. Accédez à **Gestion de source d'événements > Vue en direct**.
2. Cliquez avec le bouton droit de la souris sur le gestionnaire des collecteurs que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

Moteur de corrélation :

1. Loguez-vous à l'interface Web de Sentinel en tant qu'administrateur.
2. Développez l'option **Corrélation**, puis sélectionnez le moteur de corrélation à supprimer.
3. Cliquez sur le bouton **Supprimer** (icône de corbeille).

B.2.3 Désinstallation du gestionnaire des collecteurs NetFlow

Procédez comme suit pour désinstaller le gestionnaire des collecteurs NetFlow :

1 Connectez-vous à l'ordinateur sur lequel le gestionnaire des collecteurs NetFlow est installé.

REMARQUE : Vous devez vous connecter avec les mêmes droits d'utilisateur que ceux utilisés pour installer le gestionnaire des collecteurs NetFlow.

2 Accédez au répertoire suivant :

```
/opt/novell/sentinel/setup
```

3 exécutez la commande suivante :

```
./uninstall–sentinel
```

4 Entrez y pour désinstaller le gestionnaire des collecteurs.

Le script arrête d'abord le service, puis le désinstalle complètement.

B.3 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 Loguez-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.