Guide d'installation

Novell®
Sentinel Log Manager

1.1

July 08, 2010

www.novell.com

Mentions légales

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

Documentation en ligne : pour accéder à la documentation en ligne la plus récente de ce produit et des autres produits Novell ou pour obtenir des mises à jour, reportez-vous au site Web de documentation Novell (http://www.novell.com/documentation).

Marques de Novell

Pour connaître les marques commerciales de Novell, reportez-vous à la liste des marques commerciales et des marques de service de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Éléments tiers

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

Table des matières

À propos de ce guide

Ce guide fournit un aperçu de Novell Sentinel Log Manager et de son installation.

Public

Ce guide est destiné aux administrateurs du gestionnaire des journaux Novell Sentinel et à ses utilisateurs finals.

Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce guide et les autres documentations fournies avec ce produit. Utilisez la fonction Commentaires de l'utilisateur au bas de chaque page de la documentation en ligne ou accédez au site Web Novell de commentaires sur la documentation (http://www.novell.com/documentation/feedback.html) pour y entrer vos commentaires.

Documentation supplémentaire

Pour plus d'informations sur la création de vos propres plug-ins (par exemple JasperReports), reportez-vous à la page Web du SDK de Sentinel (http://developer.novell.com/wiki/index.php/Develop_to_Sentinel). L'environnement de création de plug-ins de rapport Sentinel Log Manager est identique à celui décrit pour Novell Sentinel.

Pour plus d'informations sur la documentation de Sentinel, reportez-vous au site Web de documentation de Sentinel (http://www.novell.com/documentation/sentinel61/index.html).

Pour obtenir de la documentation supplémentaire concernant la configuration de Sentinel Log Manager, consultez le *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

Contacter Novell

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

- Auto-assistance Novell (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Site de téléchargement des correctifs (http://download.novell.com/index.jsp)
- Support Novell 24 heures sur 24, 7 jours sur 7 (http://www.novell.com/company/contact.html)
- Sentinel TIDS (http://support.novell.com/products/sentinel)
- Forum de support de la communauté Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)

Introduction

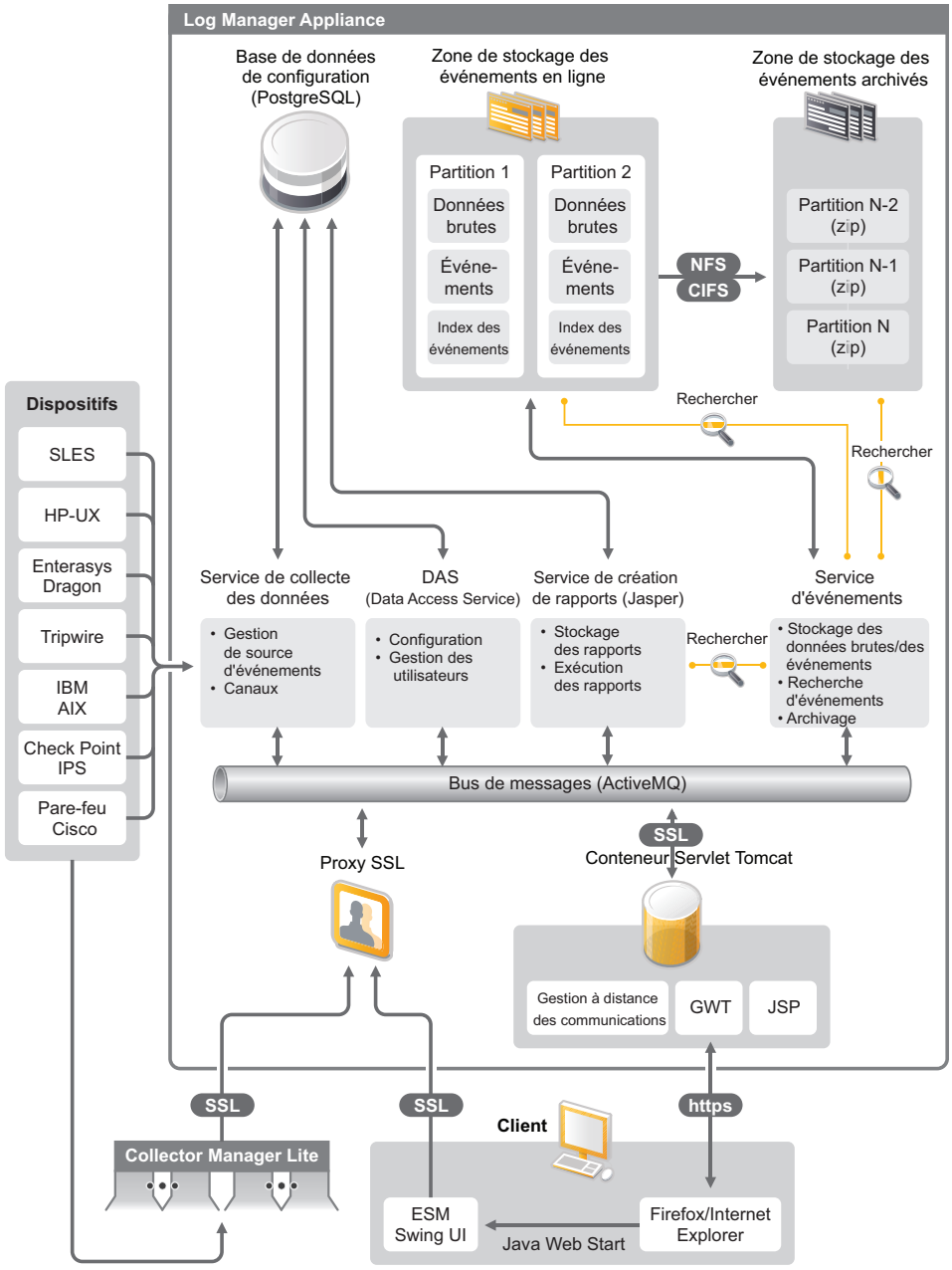
1

Novell Sentinel Log Manager collecte et gère les données de nombreux types de périphériques et d'applications, y compris les systèmes de détection d'intrusions, les pare-feux, les systèmes d'exploitation, les routeurs, les serveurs Web, les bases de données, les commutateurs, les gros systèmes et les sources d'événements d'antivirus. Il permet de traiter un taux d'événements élevé, de conserver des données à long terme ainsi que sur la base de stratégies, de regrouper des données régionales et fournit des fonctions simples de recherche et de création de rapports pour une vaste gamme d'applications et de périphériques.

1.1 Présentation du produit

Novell Sentinel Log Manager 1.1 fournit aux organisations une solution flexible et évolutive pour la gestion des journaux. Capable de surmonter les difficultés liées à la gestion et la collecte de base des journaux, Novell Sentinel Log Manager se positionne également comme une solution complète axée sur la réduction des coûts et de la complexité du risque de gestion, tout en simplifiant les exigences de mise en conformité.

Figure 1-1 *Architecture de Novell Sentinel Manager*



Novell Sentinel Log Manager intègre les fonctions suivantes :

- des fonctionnalités de recherche distribuée qui permettent aux clients de rechercher des événements collectés, non seulement sur le serveur Sentinel Log Manager local, mais également sur un ou plusieurs serveurs Sentinel Log Manager à partir d'une console centralisée ;
- des rapports de conformité précréés pour simplifier la tâche de génération des rapports de conformité pour une analyse d'audit ou d'investigation ;

- la mise à la disposition des clients d'une technologie de stockage non propriétaire leur permettant d'utiliser leur infrastructure existante pour une meilleure gestion des coûts.
- une interface utilisateur améliorée basée sur un navigateur prenant en charge la collecte, le stockage, la création de rapports ainsi que la recherche de données dans les journaux afin de simplifier considérablement les tâches de surveillance et de gestion.
- des contrôles granulaires et efficaces ainsi de options de personnalisation pour les administrateurs IT par le biais de nouvelles fonctions d'autorisations pour les groupes et les utilisateurs afin d'améliorer la transparence des activités au sein de l'infrastructure IT.

Cette section contient les informations suivantes :

1.1.1 Sources d'événements

Novell Sentinel Log Manager collecte des données à partir de sources d'événements qui génèrent des journaux dans syslog, le journal des événements, les fichiers, les bases de données Windows, SNMP, Novell Audit, SDEE (Security Device Event Exchange), OPSEC (Open Platforms for Security) de Check Point et d'autres mécanismes et protocoles de stockage.

Sentinel Log Manager prend en charge toutes les sources d'événements à condition que des connecteurs soient adaptés à l'analyse des données provenant de ces dernières. Novell Sentinel Log Manager fournit des collecteurs pour de nombreuses sources d'événements. Le collecteur générique des événements collecte et traite les données provenant de sources d'événements non reconnues mais pour lesquelles il existe des connecteurs appropriés.

Vous pouvez configurer les sources d'événements pour la collecte de données à l'aide de l'interface Gestion de source d'événements.

Pour obtenir une liste complète des sources d'événements prises en charge, reportez-vous à la Section 2.6, « Sources d'événements prises en charge », page 22.

1.1.2 Gestion de source d'événements

L'interface Gestion de source d'événements permet d'importer et de configurer les connecteurs et collecteurs Sentinel 6.0 et 6.1.

Vous pouvez effectuer les tâches suivantes à partir de la vue en direct de la fenêtre Gestion de source d'événements :

- ajouter ou éditer des connexions aux sources d'événements à l'aide des assistants de configuration ;
- afficher l'état en temps réel des connexions aux sources d'événements ;

- importer ou exporter la configuration des sources d'événements dans la vue en direct ou à partir de cette dernière ;
- afficher et configurer des connecteurs et collecteurs installés avec Sentinel ;
- importer ou exporter des connecteurs et collecteurs vers un espace de stockage centralisé ou à partir de ce dernier ;
- surveiller les flux de données à l'aide des collecteurs et des connecteurs configurés.
- afficher des informations sur les données brutes ;
- concevoir, configurer et créer les composants de la hiérarchie de la source d'événements et exécuter les opérations requises à l'aide de ces composants.

Pour plus d'informations, reportez-vous à la section Gestion de source d'événements du *Guide de l'utilisateur de Sentinel* (http://www.novell.com/documentation/sentinel61/#admin).

1.1.3 Collecte des données

Novell Sentinel Log Manager collecte les données à partir de sources d'événements configurées à l'aide des connecteurs et collecteurs.

Les collecteurs sont des scripts qui analysent les données à partir d'une multitude de sources d'événements dans la structure d'événements Sentinel normalisée ou dans certains cas, qui collectent d'autres formes de données à partir de sources de données externes. Chaque collecteur doit être déployé avec un connecteur compatible. Les connecteurs facilitent la connectivité entre les collecteurs Sentinel Log Manager et les sources de données ou d'événements.

Novell Sentinel Log Manager prend en charge l'interface utilisateur Web améliorée pour syslog et Novell Audit afin de collecter aisément des journaux à partir de différentes sources d'événements.

Pour collecter les données, Novell Sentinel Log Manager utilise de nombreuses méthodes de connexion :

- Le connecteur syslog accepte et configure automatiquement les sources de données syslog qui envoient des données sur les protocoles UDP (User Datagram Protocol), TCP (Transmission Control Protocol) ou le protocole sécurisé TLS (Transport Layer System).
- Le connecteur d'audit accepte et configure automatiquement les sources de données Novell activées pour l'audit.
- Le connecteur de fichier lit les fichiers journaux.
- Le connecteur SNMP reçoit les trappes SNMP.
- Le connecteur JDBC lit à partir des tables de base de données.
- Le connecteur WMS accède aux journaux des événements Windows sur les bureaux et les serveurs.
- Le connecteur SDEE se connecte aux périphériques qui prennent en charge le protocole SDEE, tels que les périphériques Cisco.
- Le connecteur LEA (Log Export API) de Check Point facilite l'intégration entre les collecteurs Sentinel et les serveurs pare-feu Check Point.
- Le connecteur de lien Sentinel accepte les données d'autres serveurs Novell Sentinel Log Manager.
- Le connecteur de processus accepte les données de processus personnalisés qui génèrent des journaux d'événements.

Vous pouvez également acheter une licence supplémentaire afin de télécharger des connecteurs pour des systèmes d'exploitation SAP et gros systèmes.

Pour obtenir une licence, appelez le 001-800-529-3400 ou contactez le support technique de Novell (http://support.novell.com).

Pour plus d'informations sur la configuration des connecteurs, consultez les documents relatifs aux connecteurs sur le site Web de contenu Sentinel (http://support.novell.com/products/sentinel/sentinel61.html).

Pour plus d'informations sur la configuration de la collecte des données, reportez-vous à la section « Configuring Data Collection » (Configuration de la collecte des données) du *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

Remarque : vous devez toujours télécharger et importer la dernière version des collecteurs et des connecteurs. Les collecteurs et connecteurs mis à jour sont régulièrement publiés sur le site Web de contenu Sentinel 6.1 (http://support.novell.com/products/sentinel/sentinel61.html). Les mises à jour des connecteurs et collecteurs incluent des correctifs, la prise en charge d'événements supplémentaires ainsi que des améliorations de performances.

1.1.4 Gestionnaire des collecteurs

Le gestionnaire des collecteurs fournit un point flexible de collecte de données pour Sentinel Log Manager. Novell Sentinel Log Manager installe un gestionnaire des collecteurs par défaut pendant l'installation. Vous pouvez toutefois installer des gestionnaires des collecteurs à distance aux emplacements appropriés de votre réseau. Ces gestionnaires des collecteurs distants exécutent des connecteurs et des collecteurs et transfèrent les données collectées à Novell Sentinel Log Manager 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 « Installation de gestionnaires des collecteurs supplémentaires » page 54.

1.1.5 Stockage des données

Les données sont transférées des composants de collecte de données vers des composants de stockage de données. Ces composants utilisent un système d'indexation et de stockage des données basé sur les fichiers pour conserver les données des journaux de périphérique collectées ainsi qu'une base de données PostgreSQL pour conserver les données de configuration Novell Sentinel Log Manager.

Les données sont d'abord stockées dans un format compressé sur le système de fichiers du serveur avant d'être stockées à long terme à un emplacement configuré. Leur stockage peut être local ou s'effectuer via un partage NFS ou SMB (CIFS) monté à distance. Les fichiers de données sont supprimés des emplacements de stockage locaux et réseau selon une planification configurée dans la stratégie de conservation des données.

Vous pouvez configurer des stratégies de conservation des données afin que les données situées à l'emplacement de stockage spécifié soient supprimées lorsque leur limite de conservation est atteinte ou lorsque l'espace disponible passe sous la limite de la valeur d'espace disque spécifiée.

Pour plus d'informations sur la configuration du stockage des données, reportez-vous à la section « Configuring Data Storage » (Configuration du stockage des données) du *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

1.1.6 Recherche et création de rapports

Les composants de recherche et de création de rapports vous aident à rechercher et à créer des rapports sur les données de journaux d'événements contenues dans les systèmes d'indexation et de stockage des données locaux et réseau. Les données d'événement stockées peuvent être recherchées de façon générique ou par rapport à des champs d'événement spécifiques tels qu'un nom d'utilisateur source. Les résultats de recherche peuvent encore être affinés ou filtrés et enregistrés en tant que modèle de rapport à utiliser ultérieurement.

Sentinel Log Manager est livré avec des rapports préinstallés. Des rapports supplémentaires peuvent toutefois être téléchargés. Vous pouvez exécuter des rapports à un moment planifié ou lorsque cela est nécessaire.

Pour plus d'informations sur la liste des rapports par défaut, reportez-vous à la section « Reporting » (Création de rapports) du *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

Pour plus d'informations sur la recherche d'événements et la génération de rapports, reportez-vous aux sections « Searching » (Recherche) et « Reporting » (Création de rapports) du *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

1.1.7 Lien Sentinel

Le lien Sentinel (Sentinel Link) permet de transférer des données d'événements d'un gestionnaire des journaux Sentinel à un autre. Lorsque les gestionnaires des journaux Sentinel sont hiérarchisés, des journaux complets peuvent être conservés à plusieurs emplacements régionaux tandis que les événements plus importants sont réacheminés vers un seul gestionnaire de journaux Sentinel utilisé pour les recherches centralisées et la création de rapports.

En outre, le lien Sentinel peut transférer les événements importants à Novell Sentinel, un système SIEM (Security Information Event Management) complet pour une corrélation avancée, le traitement des incidents et l'apport d'informations contextuelles très importantes, telles que des informations sur l'identité ou le niveau de gravité du serveur provenant d'un système de gestion des identités.

1.1.8 Interface utilisateur Web

Novell Sentinel Log Manager est livré avec une interface utilisateur Web pour configurer et utiliser le gestionnaire des journaux. La fonctionnalité de l'interface utilisateur est fournie par un serveur Web et une interface graphique basée sur Java Web Start. Toutes les interfaces utilisateur communiquent avec le serveur à l'aide d'une connexion codée.

L'interface Web du gestionnaire des journaux Novell Sentinel vous permet d'effectuer les opérations suivantes :

- rechercher des événements ;
- enregistrer des critères de recherche sous la forme d'un modèle de rapport ;
- afficher et gérer des rapports ;
- lancer l'interface de gestion de source d'événements pour configurer la collecte de données pour les sources de données autres que les applications Novell et syslog (fonction réservée aux administrateurs) ;

- configurer le réacheminement des données (fonction réservée aux administrateurs) ;
- télécharger le programme d'installation de Sentinel Collector Manager pour une installation à distance (fonction réservée aux administrateurs) ;
- afficher l'état de santé des sources d'événements (fonction réservée aux administrateurs) ;
- configurer la collecte des données pour les sources de données syslog et Novell (fonction réservée aux administrateurs) ;
- configurer le stockage des données et afficher l'état de santé de la base de données (fonction réservée aux administrateurs) ;
- configurer l'archivage des données (fonction réservée aux administrateurs) ;
- configurer des opérations associées pour envoyer les données d'événement correspondantes aux canaux de sortie (fonction réservée aux administrateurs) ;
- gérer les comptes et autorisations utilisateur (fonction réservée aux administrateurs).

1.2 Présentation de l'installation

Novell Sentinel Log Manager peut être installé en tant qu'applicatif ou sur un système d'exploitation SLES (SUSE Linux Enterprise Server) 11 existant. Lorsque Sentinel Log Manager est installé en tant qu'applicatif, le serveur du gestionnaire des journaux est installé sur un système d'exploitation SLES 11.

Novell Sentinel Log Manager installe par défaut les composants suivants :

- le serveur Sentinel Log Manager ;
- un serveur de communication ;
- un serveur Web et une interface utilisateur Web ;
- un serveur de création de rapports ;
- un gestionnaire des collecteurs.

Certains de ces composants requièrent une configuration supplémentaire.

Novell Sentinel Log Manager installe un gestionnaire des collecteurs par défaut. Si vous en souhaitez d'autres, vous pouvez les installer séparément sur des machines distantes. Pour plus d'informations, reportez-vous à la Chapitre 7, « Installation de gestionnaires des collecteurs supplémentaires », page 53.

Configuration système requise

2

Les sections suivantes décrivent le matériel, le système d'exploitation, le navigateur, les connecteurs pris en charge ainsi que les exigences de compatibilité de la source d'événements pour Novell Sentinel Log Manager.

2.1 Configuration matérielle requise

2.1.1 Serveur Sentinel Log Manager

Novell Sentinel Log Manager est pris en charge sur des processeurs Intel Xeon et AMD Opteron 64 bits, mais pas sur des processeurs Itanium.

Remarque : cette configuration est requise pour une taille d'événement moyenne de 300 octets.

La configuration matérielle requise suivante est recommandée pour un système de production qui conserve les données en ligne pendant 90 jours :

Tableau 2-1 *Configuration matérielle requise pour Sentinel Log Manager*

Configuration requise	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2 500 EPS)	Sentinel Log Manager (7 500 EPS)
Compression	Jusqu'à 10:1	Jusqu'à 10:1	Jusqu'à 10:1
Nbre max. de sources d'év.	Jusqu'à 1 000	Jusqu'à 1 000	Jusqu'à 2 000
Taux max. d'év.	500	2 500	7 500

Configuration requise	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2 500 EPS)	Sentinel Log Manager (7 500 EPS)
UC	Une UC Intel Xeon E5450 3 GHz (4 coeurs) ou Deux UC Intel Xeon L5240 3-(2 coeurs) (total de 4 coeurs)	Une UC Intel Xeon E5450 3 GHz (4 coeurs) ou Deux UC Intel Xeon L5240 3-(2 coeurs) (total de 4 coeurs)	Deux UC Intel Xeon X5470 3,33 GHz (4 coeurs) (total de 8 coeurs)
Mémoire RAM (Random Access Memory)	4 Go	4 Go	8 Go
Stockage	2x 500 Go, unités RPM 7,2 k (RAID matériel avec cache de 256 Mo, RAID 1)	2x 1 To, unités RPM 7,2 k (RAID matériel avec cache de 256 Mo, RAID 1)	6x 450 Go, unités RPM 15 k (RAID matériel avec cache de 512 Mo, RAID 10)

Remarque :

- Une machine peut inclure plusieurs sources d'événements. Par exemple, un serveur Windows peut inclure deux sources d'événements Sentinel pour pouvoir collecter simultanément les données d'un système d'exploitation Windows et d'une base de données SQL Server hébergée sur cette machine.
- Vous devez configurer l'emplacement de stockage en réseau sur un sous-réseau de stockage (SAN) multi-unité externe ou un stockage en réseau (NAS).
- Le volume d'état stable recommandé est 80 % du nombre maximum d'EPS sous licence. Novell recommande d'ajouter des instances Sentinel Log Manager supplémentaires si cette limite est atteinte.

Remarque : les limites maximales de sources d'événements ne sont pas des limites fixes, mais sont des recommandations basées sur des tests de performances effectués par Novell et supposent un faible taux d'événements moyen par seconde par source d'événements (moins de 3 EPS). Des taux d'EPS plus élevés donnent lieu à des sources d'événements moins durables. Vous pouvez utiliser l'équation (nombre maximum de sources d'événements) x (moyenne d'EPS par source d'événements) = taux d'événement maximum pour obtenir les limites approximatives de votre taux d'EPS moyen ou nombre d'événements sources spécifiques, pour autant que le nombre maximum de sources d'événements ne dépasse pas la limite indiquée ci-dessus.

2.1.2 Serveur de gestionnaire des collecteurs

- ❑ Une UC Intel Xeon L5240 3 GHz (2 coeurs) ;
- ❑ 256 Mo de RAM ;
- ❑ 10 Go d'espace sur le disque dur.

2.1.3 Estimation des conditions de stockage des données

Sentinel Log Manager permet de conserver des données brutes pendant longtemps pour satisfaire à des exigences légales ou autres. Il utilise la compression pour vous permettre d'utiliser efficacement votre espace de stockage local et réseau. Les besoins en stockage peuvent toutefois augmenter au fil du temps.

Pour ne pas devoir supporter les coûts engendrés par des systèmes volumineux, vous pouvez utiliser des systèmes de stockage de données économiques pour conserver les données à long terme. Les systèmes de stockage sur bande magnétique constituent la solution à la fois la plus courante et la moins onéreuse. Toutefois, ils présentent l'inconvénient de ne pas permettre un accès aléatoire aux données stockées, une condition pourtant nécessaire pour effectuer des recherches rapides. Dès lors, une approche hybride en la matière est souhaitable pour que les données sur lesquelles effectuer vos recherches soient disponibles sur un système de stockage à accès aléatoire et que celles à conserver (non utilisées pour les recherches) soient enregistrées sur un support économique, tel qu'une bande. Pour obtenir des instructions sur la mise en oeuvre de cette approche hybride, reportez-vous à la section « Using Sequential-Access Storage for Long Term Data Storage » (Utilisation d'un stockage à long terme à accès séquentiel) du *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

Pour déterminer la quantité d'espace de stockage à accès aléatoire requise pour Sentinel Log Manager, estimez d'abord le nombre de jours de données pour lesquels vous devez régulièrement effectuer des recherches ou exécuter des rapports. Vous devez disposer de suffisamment d'espace à utiliser pour l'archivage des données sur le disque dur soit en local sur la machine Sentinel Log Manager, soit à distance sur les protocoles SMB (Server Message Block), CIFS, NFS (Network File System) ou sur le sous-réseau de stockage (SAN) pour Sentinel Log Manager.

En plus de la configuration minimale requise, vous devez disposer d'une quantité d'espace supplémentaire sur le disque dur :

- pour pouvoir assimiler les taux de données supérieurs à ceux prévus ;
- pour pouvoir recopier les données des bandes dans Sentinel Log Manager afin d'effectuer des recherches et de créer des rapports sur des données historiques.

Utilisez les formules suivantes pour estimer la quantité d'espace requise pour stocker les données :

- **Taille du stockage des données d'événement :** {nombre de jours} x {événements par seconde} x {taille moyenne de l'événement en octets} x 0,000012 = nombre de Go de stockage requis.

  La taille d'un événement est généralement comprise entre 300 et 1 000 octets.
- **Taille du stockage des données brutes :** {nombre de jours} x {événements par seconde} x {taille moyenne des données brutes en octets} x 0,000012 = nombre de Go de stockage requis.

  La taille moyenne des données brutes est généralement de 200 octets.
- **Taille de stockage totale :** ({taille moyenne de l'événement en octets} + {taille moyenne des données brutes en octets}) x {nombre de jours} x {événements par seconde} x 0,000012 = nombre total de Go de stockage requis.

Remarque : il ne s'agit là que d'estimations et ces nombres dépendent de la taille de vos données d'événement ainsi que de la taille des données compressées.

Les formules qui précèdent calculent l'espace de stockage minimum requis pour conserver des données entièrement compressées sur le système de stockage externe. Au fur et à mesure que le stockage local se remplit, Sentinel Log Manager compresse et déplace les données d'un système de stockage local (partiellement compressé) vers un externe (entièrement compressé). Par conséquent, l'estimation des besoins d'espace de stockage externe devient plus critique pour la conservation des données. Pour améliorer les performances de recherche de données récentes et de création de rapports sur ces dernières, vous pouvez augmenter l'espace de stockage local au-delà de la configuration matérielle requise de Sentinel Log Manager ; sans que cela ne constitue pour autant une obligation.

Les formules ci-dessus vous permettent également de déterminer la quantité d'espace de stockage requise pour un système de stockage des données à long terme tel qu'une bande.

2.1.4 Environnement virtuel

Sentinel Log Manager a été testé de manière approfondie et est entièrement pris en charge sur les serveurs VMware ESX. Les résultats de performances dans un environnement virtuel sont comparables à ceux obtenus lors de tests sur une machine physique, mais l'environnement virtuel doit fournir des capacités de mémoire, d'UC, d'espace disque et d'E/S identiques aux recommandations pour les machines physiques.

2.2 Systèmes d'exploitation pris en charge

Cette section contient des informations sur les systèmes d'exploitation pris en charge pour le serveur Sentinel Log Manager et le gestionnaire des collecteurs distant :

- Section 2.2.1, « Sentinel Log Manager », page 20
- Section 2.2.2, « Gestionnaire des collecteurs », page 20

2.2.1 Sentinel Log Manager

Cette section n'est pertinente que si vous installez Sentinel Log Manager sur un système d'exploitation existant.

- ❑ SLES (SUSE Linux Enterprise Server) 11 64 bits ;
- ❑ un système de fichiers hautement performant.

Remarque : tous les tests d'évaluation Novell sont effectués avec un système de fichiers ext3.

2.2.2 Gestionnaire des collecteurs

Vous pouvez installer des gestionnaires des collecteurs supplémentaires sur les systèmes d'exploitation suivants :

- « Linux » page 21
- « Windows » page 21

Linux

- ❑ SUSE Linux Enterprise Server 10 SP2 (32 et 64 bits)
- ❑ SUSE Linux Enterprise Server 11 (32 et 64 bits)

Windows

- ❑ Windows Server 2003 (32 et 64 bits)
- ❑ Windows Server* 2003 SP2 (32 et 64 bits)
- ❑ Windows Server 2008 (64 bits)

2.3 Navigateurs pris en charge

L'interface Sentinel Log Manager est optimisée pour une résolution 1280 x 1024 ou ultérieure dans les navigateurs pris en charge suivants :

- Section 2.3.1, « Linux », page 21
- Section 2.3.2, « Windows », page 21

2.3.1 Linux

- ❑ Mozilla Firefox 3.6

2.3.2 Windows

- ❑ Mozilla Firefox 3 (optimisé pour 3.6)
- ❑ Microsoft Internet Explorer 8 (optimisé pour 8.0)

Conditions préalables pour Internet Explorer 8

- Si le niveau de sécurité Internet est défini sur Élevé, seule une page vide s'affiche après le login à Novell Sentinel Log Manager. Pour résoudre ce problème, accédez à *Outils* > *Options Internet* > *onglet Sécurité* > *Sites de confiance*. Cliquez sur le bouton *Sites* et ajoutez le site Web Sentinel Log Manager à la liste des sites de confiance.
- Vérifiez que dans le menu *Outils, l'option Affichage de compatibilité* n'est pas sélectionnée.
- Si l'option *Demander confirmation pour les téléchargements de fichiers* n'est pas cochée, la fenêtre contextuelle de téléchargement de fichiers est peut-être bloquée par le navigateur. Pour résoudre ce problème, accédez à *Outils* > *Options Internet* > *onglet Sécurité* > *Niveau personnalisé*, faites défiler la section de téléchargement, puis sélectionnez *Activer* pour activer l'option *Demander confirmation pour les téléchargements de fichiers*.

2.4 Environnement virtuel pris en charge

- ❑ VMware ESX/ESXi 3.5/4.0 ou version ultérieure
- ❑ VMPlayer 3 (uniquement en mode démo)
- ❑ Xen 3.1.1

2.5 Connecteurs pris en charge

Sentinel Log Manager prend en charge tous les connecteurs pris en charge par Sentinel et Sentinel RD.

- Connecteur d'audit
- Connecteur de processus LEA Check Point
- Connecteur de base de données
- Connecteur de générateur de données
- Connecteur de fichier
- Connecteur de processus
- Connecteur Syslog
- Connecteur SNMP
- Connecteur SDEE
- Connecteur de lien Sentinel
- Connecteur WMS
- Connecteur Mainframe
- Connecteur SAP

Remarque : les connecteurs Mainframe et SAP requièrent une licence distincte.

2.6 Sources d'événements prises en charge

Sentinel Log Manager prend en charge de nombreux périphériques et applications, y compris les systèmes de détection d'intrusions, les pare-feux, les systèmes d'exploitation, les routeurs, les serveurs Web, les bases de données, les commutateurs, les gros systèmes et les sources d'événements d'antivirus. Les données de ces sources d'événements sont analysées et normalisées à divers degrés selon que les données sont traitées à l'aide du collecteur générique d'événements qui place l'ensemble de la charge utile dans un champ commun ou à l'aide d'un collecteur spécifique à un périphérique qui analyse les données dans des champs individuels.

Sentinel Log Manager prend en charge les sources d'événements suivantes :

- Cisco Firewall (6 et 7)
- Cisco Switch Catalyst série 6500 (CatOS 8.7)
- Cisco Switch Catalyst série 6500 (IOS 12.2SX)
- Cisco Switch Catalyst série 5000 (CatOS 4.x)
- Cisco Switch Catalyst série 4900 (IOS 12.2SG)
- Cisco Switch Catalyst série 4500 (IOS 12.2SG)
- Cisco Switch Catalyst série 4000 (CatOS 4.x)
- Cisco Switch Catalyst série 3750 (IOS 12.2SE)
- Cisco Switch Catalyst série 3650 (IOS 12.2SE)
- Cisco Switch Catalyst série 3550 (IOS 12.2SE)
- Cisco Switch Catalyst série 2970 (IOS 12.2SE)

- Cisco Switch Catalyst série 2960 (IOS 12.2SE)
- Cisco VPN 3000 (4.1.5, 4.1.7 et 4.7.2)
- Extreme Networks Summit X650 (avec ExtremeXOS 12.2.2 et versions antérieures)
- Extreme Networks Summit X450a (avec ExtremeXOS 12.2.2 et versions antérieures)
- Extreme Networks Summit X450e (avec ExtremeXOS 12.2.2 et versions antérieures)
- Extreme Networks Summit X350 (avec ExtremeXOS 12.2.2 et versions antérieures)
- Extreme Networks Summit X250e (avec ExtremeXOS 12.2.2 et versions antérieures)
- Extreme Networks Summit X150 (avec ExtremeXOS 12.2.2 et versions antérieures)
- Enterasys Dragon (7.1 et 7.2)
- Collecteur générique d'événements
- HP HP-UX (11iv1 et 11iv2)
- IBM AIX (5.2, 5.3 et 6.1)
- Juniper Netscreen série 5
- McAfee Firewall Enterprise
- McAfee Network Security Platform (2.1, 3.x et 4.1)
- McAfee VirusScan Enterprise (8.0i, 8.5i et 8.7i)
- McAfee ePolicy Orchestrator (3.6 et 4.0)
- McAfee AV Via ePolicy Orchestrator 8.5
- Microsoft Active Directory (2000, 2003 et 2008)
- Microsoft SQL Server (2005 et 2008)
- Nortel VPN (1750, 2700, 2750 et 5000)
- Novell Access Manager 3.1
- Novell Identity Manager 3.6.1
- Novell Netware 6.5
- Novell Modular Authentication Services 3.3
- Novell Open Enterprise Server 2.0.2
- Novell Privileged User Manager 2.2.1
- Novell Sentinel Link 1
- Novell SUSE Linux Enterprise Server
- Novell eDirectory 8.8.3 et son correctif d'instrumentation sont disponibles sur le site Web de support Novell (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~).
- Novell iManager 2.7
- Red Hat Enterprise Linux
- Sourcefire Snort (2.4.5, 2.6.1, 2.8.3.2 et 2.8.4)
- Snare pour Windows Intersect Alliance (3.1.4 et 1.1.1)
- Sun Microsystems Solaris 10
- Symantec AntiVirus Corporate Edition (9 et 10)
- TippingPoint Security Management System (2.1 et 3.0)

- Websense Web Security 7.0
- Websense Web Filter 7.0

Remarque : pour activer la collecte de données à partir de sources d'événements Novell iManager et Novell Netware 6.5, ajoutez une instance d'un collecteur et d'un connecteur enfant (connecteur d'audit) dans l'interface de gestion de source d'événements pour chacune des sources d'événements. Lorsque cette opération est effectuée, ces sources d'événements apparaissent dans la console Web de Sentinel Log Manager sous l'onglet *Serveur d'audit*.

Les collecteurs prenant en charge des sources d'événements supplémentaires peuvent être obtenus sur le site Web de contenu Sentinel 6.1 (http://support.novell.com/products/sentinel/sentinel61.html) ou créés à l'aide des plug-ins SDK disponibles sur le site Web SDK de plug-ins Sentinel (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

Installation sur un système SLES 11 existant

3

La section décrit la procédure d'installation de Sentinel Log Manager sur un système SLES (SUSE Linux Enterprise Server) 11 existant à l'aide du programme d'installation de l'application. Vous pouvez installer le serveur Sentinel Log Manager de différentes manières : selon la procédure d'installation standard, la procédure d'installation personnalisée ou la procédure d'installation silencieuse lorsque l'installation ne nécessite pas d'intervention de la part de l'utilisateur et utilise les valeurs par défaut. Vous pouvez également installer Sentinel Log Manager en tant qu'utilisateur non-root.

Si vous choisissez la méthode d'installation personnalisée, vous pouvez installer le produit avec une clé de licence et sélectionner une option d'authentification. Vous pouvez paramétrer une authentification LDAP pour Sentinel Log Manager en plus de l'authentification de la base de données. Lorsque vous configurez Sentinel Log Manager pour une authentification LDAP, les utilisateurs peuvent se loguer au serveur à l'aide de leurs références Novell eDirectory ou Microsoft Active Directory.

Si vous souhaitez installer plusieurs serveurs Sentinel Log Manager dans votre déploiement, vous pouvez enregistrer les options d'installation dans un fichier de configuration, puis utiliser le fichier pour exécuter une installation sans surveillance. Pour plus d'informations, reportez-vous à la Section 3.4, « Installation en mode silencieux », page 29.

Avant de procéder à l'installation, vérifiez que vous remplissez les conditions de la configuration minimale requise spécifiée au Chapitre 2, « Configuration système requise », page 17.

3.1 Avant de commencer

- ❑ Vérifiez que votre matériel et vos logiciels satisfont aux conditions de la configuration minimale requise mentionnées au Chapitre 2, « Configuration système requise », page 17.
- ❑ Configurez le système d'exploitation de façon à ce que la commande `hostname -f` renvoie un nom d'hôte valide.
- ❑ Obtenez votre clé de licence à partir du Service clients de Novell (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) pour installer la version sous licence.
- ❑ Synchronisez l'heure à l'aide du protocole NTP (Network Time Protocol).
- ❑ Installez les commandes de système d'exploitation suivantes :
  - `mount`
  - `umount`

- `id`
- `df`
- `du`
- `sudo`

❑ Vérifiez que les ports suivants sont ouverts sur le pare-feu :

TCP 8080, TCP 8443, TCP 61616, TCP 10013, TCP 1289, TCP 1468, TCP 1443 et UDP 1514

3.2 Installation standard

La procédure d'installation standard installe Sentinel Log Manager avec toutes les options par défaut et une licence d'évaluation de 90 jours.

1. Téléchargez et copiez les fichiers d'installation à partir du site Web de téléchargement Novell.
2. Loguez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez installer Sentinel Log Manager.
3. 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.
4. Entrez la commande suivante pour exécuter le script `install-slm` afin d'installer Sentinel Log Manager :

   `./install-slm`

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

   `./install-slm -r responseFile`
5. Pour continuer dans la langue de votre choix, sélectionnez le nombre spécifié en regard de la langue.

   L'accord de licence utilisateur final s'affiche dans la langue sélectionnée.
6. Lisez l'accord de licence utilisateur final et tapez `oui` ou `o` pour l'accepter et poursuivre l'installation.

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

   L'installation crée un groupe `novell` ainsi qu'un utilisateur `novell` s'ils n'existent pas encore.
7. Lorsque vous y êtes invité, spécifiez l'option pour effectuer l'installation standard.

   L'installation utilise une clé de licence d'évaluation de 90 jours incluse avec le programme d'installation. Cette clé active l'ensemble des fonctions du produit pour une période d'essai de 90 jours. À tout moment, que ce soit pendant ou après la période d'essai, vous pouvez remplacer la clé de la licence d'évaluation par celle que vous avez achetée.
8. Spécifiez le mot de passe de l'administrateur.
9. Confirmez-le.

   Le programme d'installation sélectionne la méthode *S'authentifier auprès de la base de données uniquement* et poursuit l'installation.

L'installation de Sentinel Log Manager se termine et le serveur démarre. Il faut compter entre 5 et 10 minutes pour que tous les services démarrent après l'installation étant donné que le système effectue une initialisation unique. Patientez ce délai avant de vous loguer au serveur.

10 Pour vous loguer au serveur Sentinel Log Manager, utilisez l'URL spécifiée dans les résultats de l'installation. L'URL est similaire à `https://10.0.0.1:8443/novelllogmanager`.

   Pour plus d'informations sur le login au serveur, reportez-vous au Chapitre 5, « Login à l'interface Web », page 45.

11 Pour configurer les sources d'événements en vue d'envoyer des données à Sentinel Log Manager, reportez-vous à la section « Configuring Data Collection » (Configuration de la collecte de données) du *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

3.3 Installation personnalisée

Si vous choisissez la méthode d'installation personnalisée, vous pouvez installer le produit avec une clé de licence et sélectionner une option d'authentification. Vous pouvez paramétrer une authentification LDAP pour Sentinel Log Manager en plus de l'authentification de la base de données. Lorsque vous configurez Sentinel Log Manager pour l'authentification LDAP, les utilisateurs peuvent se loguer au serveur à l'aide des références de l'annuaire LDAP.

Si vous ne configurez pas Sentinel Log Manager pour une authentification LDAP pendant la procédure d'installation, vous pourrez au besoin la configurer ultérieurement. Pour configurer l'authentification LDAP après l'installation, reportez-vous à la section « LDAP Authentication » (Authentification LDAP) du *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

1 Téléchargez et copiez les fichiers d'installation à partir du site Web de téléchargement Novell.

2 Loguez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez installer Sentinel Log Manager.

3 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.

4 Entrez la commande suivante pour exécuter le script `install-slm` afin d'installer Sentinel Log Manager :

   `./install-slm`

5 Pour continuer dans la langue de votre choix, sélectionnez le nombre spécifié en regard de la langue.

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

6 Lisez l'accord de licence utilisateur final et tapez `oui` ou `o` pour l'accepter et poursuivre l'installation.

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

   L'installation crée un groupe `novell` ainsi qu'un utilisateur `novell` s'ils n'existent pas encore.

7 Lorsque vous y êtes invité, spécifiez l'option pour effectuer l'installation personnalisée.

8 Lorsque vous êtes invité à indiquer l'option de clé de licence, entrez `2` pour spécifier la clé de licence pour le produit acheté.

9 Spécifiez la clé de licence, puis appuyez sur Entrée.

Pour plus d'informations sur les clés de licence, reportez-vous à la section « Managing License Keys » (Gestion des clés de licence) du *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

10 Spécifiez le mot de passe de l'administrateur.

11 Confirmez-le.

12 Définissez le mot de passe de l'administrateur de la base de données (dbauser).

13 Confirmez le mot de passe de l'administrateur de la base de données (dbauser).

14 Vous pouvez configurer n'importe quel numéro de port valide dans la plage spécifiée pour les services suivants :

- serveur Web ;
- JMS (Java Message Service) ;
- Service proxy client ;
- Service de base de données
- Passerelle interne de l'agent.

Si vous souhaitez continuer avec les ports par défaut, entrez l'option 6 pour poursuivre avec l'installation personnalisée.

15 Spécifiez l'option pour authentifier les utilisateurs par le bias d'un annuaire LDAP externe.

16 Spécifiez l'adresse IP ou le nom d'hôte du serveur LDAP.

La valeur par défaut est localhost. Toutefois, vous ne devez pas installer le serveur LDAP sur la même machine que le serveur Sentinel Log Manager.

17 Sélectionnez l'un des types de connexion LDAP suivants :

- **Connexion LDAP TLS/SSL :** établit une connexion sécurisée entre le navigateur et le serveur pour l'authentification. Entrez 1 pour utiliser cette option.
- **Connexion LDAP non codée :** établit une connexion non codée. Entrez 2 pour utiliser cette option.

18 Spécifiez le numéro de port du serveur LDAP. Le numéro de port SSL par défaut est le 636 et le numéro de port par défaut qui n'utilise pas SSL est le 389.

19 (Facultatif) Si vous avez sélectionné Connexion LDAP TLS/SSL, spécifiez si le certificat du serveur LDAP est signé par une autorité de certification reconnue.

20 (Facultatif) Si vous avez spécifié `n`, indiquez le nom de fichier du certificat de serveur LDAP.

21 Indiquez si vous souhaitez effectuer des recherches anonymes sur l'annuaire LDAP :

- **Effectuer des recherches anonymes sur l'annuaire LDAP :** le serveur Sentinel Log Manager effectue une *recherche anonyme* sur l'annuaire LDAP en fonction du nom d'utilisateur spécifié pour récupérer le nom distinctif (DN) de l'utilisateur LDAP correspondant. Entrez 1 pour utiliser cette méthode.
- **Ne pas effectuer de recherches anonymes sur l'annuaire LDAP :** entrez 2 pour utiliser cette option.

22 (Facultatif) Si vous avez sélectionné la recherche anonyme, spécifiez l'attribut de recherche et passez à l'Étape 25.

23 (Facultatif) Si vous n'avez pas sélectionné la recherche anonyme à l'Étape 21, indiquez si vous utilisez Microsoft Active Directory.

Pour Active Directory, l'attribut `userPrincipalName` dont la valeur est au format `nomUtilisateur@nomDomaine` peut éventuellement être utilisé pour authentifier l'utilisateur avant de rechercher l'objet utilisateur LDAP. La saisie du DN de l'utilisateur n'est alors pas nécessaire.

24 (Facultatif) Si vous souhaitez utiliser l'approche susmentionnée pour Active Directory, spécifiez le nom de domaine.

25 Spécifiez le DN de base.

26 Appuyez sur o pour confirmer que les options fournies sont correctes. Dans le cas contraire, appuyez sur n et modifiez la configuration.

27 Pour vous loguer au serveur Sentinel Log Manager, utilisez l'URL spécifiée dans les résultats de l'installation. L'URL est similaire à `https://10.0.0.1:8443/novelllogmanager`.

Pour plus d'informations sur le login au serveur, reportez-vous au Chapitre 5, « Login à l'interface Web », page 45.

3.4 Installation en mode silencieux

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

1 Téléchargez et copiez les fichiers d'installation à partir du site Web de téléchargement Novell.

2 Loguez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez installer Sentinel Log Manager.

3 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.

4 Entrez la commande suivante pour exécuter le script `install-slm` afin d'installer Sentinel Log Manager en mode silencieux :

```
./install-slm -u responseFile
```

Pour obtenir des informations sur la création du fichier de réponses, reportez-vous à la Section 3.2, « Installation standard », page 26. L'installation s'effectue avec les valeurs stockées dans le fichier de réponses.

5 Pour vous loguer au serveur Sentinel Log Manager, utilisez l'URL spécifiée dans les résultats de l'installation. L'URL est similaire à `https://10.0.0.1:8443/novelllogmanager`.

Pour plus d'informations sur le login au serveur, reportez-vous au Chapitre 5, « Login à l'interface Web », page 45.

6 Pour configurer les sources d'événements en vue d'envoyer des données à Sentinel Log Manager, reportez-vous à la section « Configuring Data Collection » (Configuration de la collecte de données) du « Sentinel Log Manager 1.1 Administration Guide » (Guide d'administration de Sentinel Log Manager 1.1).

3.5 Installation non-root

Si votre stratégie organisationnelle ne vous permet pas d'exécuter l'installation complète de Sentinel Log Manager en tant qu'utilisateur `root`, la plupart des étapes de l'installation peuvent être exécutées par un autre utilisateur.

1. Téléchargez et copiez les fichiers d'installation à partir du site Web de téléchargement Novell.
2. 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.
3. Loguez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez installer Sentinel Log Manager 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.

   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 `novell` que vous venez de créer : `novell` :

   ```
   su novell
   ```
7. Entrez la commande suivante :

   ```
   ./install-slm
   ```
8. Pour continuer dans la langue de votre choix, sélectionnez le nombre spécifié 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 et poursuivre l'installation.

   Le processus démarre en installant tous les paquetages RPM. Cette installation peut prendre quelques secondes.
10. Vous êtes invité à spécifier le mode d'installation.
    - Si vous choisissez de poursuivre avec l'installation standard, effectuez les étapes 8 à 11 de la Section 3.2, « Installation standard », page 26.
    - Si vous choisissez de poursuivre avec l'installation personnalisée, effectuez les étapes 8 à 23 de la Section 3.3, « Installation personnalisée », page 27.

    L'installation de Sentinel Log Manager se termine et le serveur démarre.
11. Entrez la commande suivante pour prendre l'identité de l'utilisateur `root` :

    ```
    su root
    ```
12. Entrez la commande suivante pour terminer l'installation :

    ```
    ./bin/root_install_finish
    ```

13 Pour vous loguer au serveur Sentinel Log Manager, utilisez l'URL spécifiée dans les résultats de l'installation. L'URL est similaire à `https://10.0.0.1:8443/novelllogmanager`.

Pour plus d'informations sur le login au serveur, reportez-vous au Chapitre 5, « Login à l'interface Web », page 45.

Installation de l'applicatif

4

L'applicatif Sentinel Log Manager est un logiciel prêt à l'emploi basé sur SUSE Studio qui combine un système d'exploitation SLES 11 (SUSE Linux Enterprise Server 11), le logiciel Novell Sentinel Log Manager et un service de mise à jour intégré afin d'offrir à l'utilisateur une expérience conviviale et transparente et de lui permettre de tirer parti des investissements existants. L'applicatif logiciel peut être installé sur du matériel ou dans un environnement virtuel.

4.1 Avant de commencer

- Vérifiez que les conditions de la configuration matérielle sont remplies. Pour plus d'informations, reportez-vous à la Section 2.1, « Configuration matérielle requise », page 17.
- Obtenez votre clé de licence à partir du Service clients de Novell (http://www.novell.com/center) pour installer la version sous licence.
- Obtenez votre code d'enregistrement à partir du Service clients de Novell (http://www.novell.com/center) pour enregistrer les mises à jour logicielles.
- Synchronisez l'heure à l'aide du protocole NTP (Network Time Protocol).
- (Facultatif) Si vous avez l'intention d'utiliser VMware, veillez à disposer de VMware pour charger simultanément l'image sur le serveur VMware ESX et la convertir dans un format exécutable pour le serveur ESX.

4.2 Ports utilisés

Il convient de signaler que l'applicatif Novell Sentinel Log Manager utilise les ports suivants pour la communication et que certains d'entre eux sont ouverts sur le pare-feu :

4.2.1 Ports ouverts sur le pare-feu

Tableau 4-1 *Ports réseau utilisés par Sentinel Log Manager*

Ports	Description
TCP 1289	Utilisé pour les connexions Novell Audit.
TCP 289	Réacheminé vers le port 1289 pour les connexions Novell Audit.
TCP 22	Utilisé pour un accès shell sécurisé à l'applicatif Sentinel Log Manager.
UDP 1514	Utilisé pour les messages syslog.
UDP 514	Réacheminé vers le port 1514 pour les messages syslog.
TCP 8080	Utilisé pour les communications HTTP. Également utilisé par l'applicatif Sentinel Log Manager pour le service de mise à jour.
TCP 80	Réacheminé vers le port 8080 pour le serveur Web Sentinel Log Manager pour les communications HTTP. Également utilisé par l'applicatif Sentinel Log Manager pour le service de mise à jour.
TCP 8443	Utilisé pour les communications HTTPS. Également utilisé par l'applicatif Sentinel Log Manager pour le service de mise à jour.
TCP 1443	Utilisé pour les messages syslog codés avec SSL.
TCP 443	Réacheminé vers le port 8443 pour le serveur Web Sentinel Log Manager pour les communications HTTPS. Également utilisé par l'applicatif Sentinel Log Manager pour le service de mise à jour.
TCP 61616	Utilisé pour les communications entre le gestionnaire des collecteurs et le serveur.
TCP 10013	Utilisé par le proxy SSL de l'interface utilisateur de la gestion de source d'événements.
TCP 54984	Utilisé par la console de gestion (WebYaST) de l'applicatif Sentinel Log Manager.
TCP 1468	Utilisé pour les messages syslog.

4.2.2 Ports utilisés localement

Tableau 4-2 *Ports utilisés pour les communications locales*

Ports	Description
TCP 61617	Utilisé pour les communications internes entre le serveur Web et le serveur.
TCP 5556	Utilisé sur l'interface en boucle pour les communications internes avec le serveur internal_gateway_server et la passerelle internal_gateway. Est également utilisé pour les communications entre le moteur de l'agent et le gestionnaire des collecteurs.

Ports	Description
TCP 5432	Utilisé pour la base de données PostgreSQL. Il n'est pas nécessaire d'ouvrir ce port par défaut. Toutefois, si vous développez des rapports à l'aide du SDK Sentinel, vous devez ouvrir ce port. Pour plus d'informations, reportez-vous au site Web SDK de plug-ins Sentinel (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).
Deux ports TCP supplémentaires sélectionnés aléatoirement	Utilisé pour les communications internes entre le moteur de l'agent et le gestionnaire des collecteurs.
TCP 8005	Utilisé pour les communications internes avec les processus Tomcat.
TCP 32000	Utilisé pour les communications internes entre le moteur de l'agent et le gestionnaire des collecteurs.

4.3 Installation de l'applicatif VMware

Pour exécuter l'image de l'applicatif à partir du serveur VMware ESX, importez et installez l'image de l'applicatif sur le serveur.

1. Téléchargez le fichier d'installation de l'applicatif VMware.

   Le nom du fichier approprié pour l'applicatif VMware contient `vmx`. Par exemple, `Sentinel_Log_Manager_1.1.0.0_64_VMX.x86_64-0.777.0.vmx.tar.gz`
2. Définissez une banque de données ESX sur laquelle l'image de l'applicatif peut être installée.
3. Loguez-vous en tant qu'administrateur au serveur sur lequel vous souhaitez installer l'applicatif.
4. Entrez la commande suivante pour extraire l'image de l'applicatif compressée à partir de la machine sur laquelle le VM Converter est installé :

   `tar zxvf <fichier_installation>`

   Remplacez <*fichier_installation*> par le nom réel du fichier.
5. Pour importer l'image VMware sur le serveur ESX, utilisez VMware Converter et suivez les instructions à l'écran dans l'assistant d'installation.
6. Loguez-vous à la machine du serveur ESX.
7. Sélectionnez l'image VMware importée de l'applicatif, puis cliquez sur l'icône d'*alimentation*.
8. Sélectionnez la langue de votre choix, puis cliquez sur *Suivant*.
9. Sélectionnez la disposition du clavier, puis cliquez sur *Suivant*.
10. Lisez et acceptez l'accord de licence du logiciel Novell SUSE Enterprise Server.
11. Lisez et acceptez l'accord de licence utilisateur final de Novell Sentinel Log Manager.
12. Dans l'écran Nom d'hôte et Nom de domaine, spécifiez le nom d'hôte et le nom de domaine. Vérifiez que l'option *Write hostname to /etc/hosts* (Écrire le nom d'hôte dans /etc/hosts) est sélectionnée.
13. Cliquez sur *Suivant*. Les configurations du nom d'hôte sont enregistrées.

14 Effectuez l'une des opérations suivantes :

- Pour utiliser les paramètres de connexion réseau actuels, sélectionnez *Use the following configuration* (Utiliser la configuration suivante) dans l'écran *Network Configuration II* (Configuration réseau II).
- Pour modifier les paramètres de connexion réseau, sélectionnez *Changer*.

15 Indiquez l'heure et la date, cliquez sur *Suivant*, puis sur *Terminer*.

Remarque : 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
```

---

16 Définissez le mot de passe `root` Novell SUSE Enterprise Server, puis cliquez sur *Suivant*.

17 Définissez le mot de passe `root`, puis cliquez sur *Suivant*.

18 Définissez les mots de passe admin et dbauser de Sentinel Log Manager, puis cliquez sur *Suivant*.

19 Cliquez sur *Suivant*. Les paramètres de connexion réseau sont enregistrés.

L'installation s'effectue et se termine. Prenez note de l'adresse IP de l'applicatif qui s'affiche dans la console.

20 Passez à la Section 4.6, « Configuration post-installation de l'applicatif », page 39.

4.4 Installation de l'applicatif Xen

1 Téléchargez et copiez le fichier d'installation de l'applicatif virtuel Xen dans `/var/lib/xen/images`.

Le nom de fichier correct de l'applicatif virtuel Xen contient `xen`. Par exemple, `Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.xen.tar.gz`

2 Entrez la commande suivante pour extraire le fichier :

```
tar -xvzf <install_file>
```

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

3 Accédez au nouveau répertoire d'installation. Ce répertoire contient les fichiers suivants :

- *fichier image* `<nom_fichier>.raw`
- *fichier* `<nom_fichier>.xenconfig`

4 Ouvrez le fichier `<nom_fichier>.xenconfig` à l'aide d'un éditeur de texte.

5 Modifiez le fichier comme suit :

Spécifiez le chemin complet du fichier `.raw` dans le paramètre `disk`.

Spécifiez le paramètre « bridge » pour votre configuration réseau. Par exemple, `"bridge=br0"` ou `"bridge=xenbr0"`.

Spécifiez des valeurs pour les paramètres `name` et `memory`.

Par exemple :

```
# -*- mode: python; -*-
name="Sentinel_Log_Manager_1.1.0.0_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.1.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```

6 Après avoir modifié le fichier *<nom_fichier>*.xenconfig, entrez la commande suivante pour créer la machine virtuelle :

```
xm create <nom_fichier>.xenconfig
```

7 (Facultatif) Pour vérifier que la machine virtuelle a été créée, entrez la commande suivante :

xm list

La machine virtuelle apparaît dans la liste.

Par exemple, si vous avez configuré `name="Sentinel_Log_Manager_1.1.0.0_64"` dans le fichier `.xenconfig`, ce nom de machine virtuelle apparaît.

8 Pour démarrer l'installation, entrez la commande suivante :

```
xm console <nom_vm>
```

Remplacez *<nom_vm>* par le nom spécifié dans le paramètre de nom du fichier `.xenconfig`, qui est également la valeur renvoyée à l'étape 7. Par exemple :

```
xm console Sentinel_Log_Manager_1.1.0.0_64
```

9 Sélectionnez la langue de votre choix, puis cliquez sur *Suivant*.

10 Sélectionnez la disposition du clavier, puis cliquez sur *Suivant*.

11 Lisez et acceptez l'accord de licence du logiciel Novell SUSE Enterprise Server.

12 Lisez et acceptez l'accord de licence utilisateur final de Novell Sentinel Log Manager.

13 Dans l'écran Nom d'hôte et Nom de domaine, spécifiez le nom d'hôte et le nom de domaine. Vérifiez que l'option *Write hostname to /etc/hosts* (Écrire le nom d'hôte dans /etc/hosts) est sélectionnée.

14 Cliquez sur *Suivant*. Les configurations du nom d'hôte sont enregistrées.

15 Effectuez l'une des opérations suivantes :

- Pour utiliser les paramètres de connexion réseau actuels, sélectionnez *Use the following configuration* (Utiliser la configuration suivante) dans l'écran *Network Configuration II* (Configuration réseau II).
- Pour modifier les paramètres de connexion réseau, sélectionnez *Changer*.

16 Indiquez l'heure et la date, cliquez sur *Suivant*, puis sur *Terminer*.

Remarque : 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
```

---

17 Définissez le mot de passe `root` Novell SUSE Enterprise Server, puis cliquez sur *Suivant*.

18 Définissez les mots de passe admin et dbauser de Sentinel Log Manager, puis cliquez sur *Suivant*.

L'installation s'effectue et se termine. Prenez note de l'adresse IP de l'applicatif qui s'affiche dans la console.

19 Passez à la Section 4.6, « Configuration post-installation de l'applicatif », page 39.

4.5 Installation de l'applicatif sur du matériel

Avant d'installer l'applicatif sur le matériel, vérifiez que l'image disque ISO de l'applicatif a été téléchargée à partir du site de support, qu'elle a été extraite et qu'elle est disponible sur un DVD.

1 Démarrez la machine physique à l'aide du DVD à partir de l'unité DVD.

2 Suivez les instructions de l'assistant d'installation qui s'affichent à l'écran.

3 Exécutez l'image de l'applicatif Live DVD en sélectionnant la toute première entrée dans le menu de démarrage.

4 Lisez et acceptez l'accord de licence du logiciel Novell SUSE Enterprise Server.

5 Lisez et acceptez l'accord de licence utilisateur final de Novell Sentinel Log Manager.

6 Cliquez sur *Suivant*.

7 Dans l'écran Nom d'hôte et Nom de domaine, spécifiez le nom d'hôte et le nom de domaine.

Vérifiez que l'option *Write hostname to /etc/hosts* (Écrire le nom d'hôte dans /etc/hosts) est sélectionnée.

8 Cliquez sur *Suivant*. Les configurations du nom d'hôte sont enregistrées.

9 Effectuez l'une des opérations suivantes :

- Pour utiliser les paramètres de connexion réseau actuels, sélectionnez *Use the following configuration* (Utiliser la configuration suivante) dans l'écran Network Configuration II (Configuration réseau II).
- Pour modifier les paramètres de connexion réseau, sélectionnez *Changer*.

10 Cliquez sur *Suivant*. Les paramètres de connexion réseau sont enregistrés.

11 Indiquez l'heure et la date, cliquez sur *Suivant*.

Remarque : 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
```

---

12 Définissez le mot de passe `root`, puis cliquez sur *Suivant*.

13 Définissez les mots de passe admin et dbauser de Sentinel Log Manager, puis cliquez sur *Suivant*.

14 Entrez le nom d'utilisateur et le mot de passe dans la console pour vous loguer à l'applicatif.

La valeur par défaut pour le nom d'utilisateur est `root` et pour le mot de passe, `password`.

15 Pour installer l'applicatif sur le serveur physique, exécutez la commande suivante :

```
/sbin/yast2 live-installer
```

L'installation s'effectue et se termine. Prenez note de l'adresse IP de l'applicatif qui s'affiche dans la console.

16 Passez à la Section 4.6, « Configuration post-installation de l'applicatif », page 39.

4.6 Configuration post-installation de l'applicatif

Pour vous loguer à la console Web de l'applicatif et initialiser le logiciel :

1 Ouvrez un navigateur Web et accédez à l'adresse https://*adresse_IP*>:*8443*. La page Web de Sentinel Log Manager s'affiche.

L'adresse IP de l'applicatif s'affiche sur la console de l'applicatif une fois l'installation terminée et le serveur redémarré.

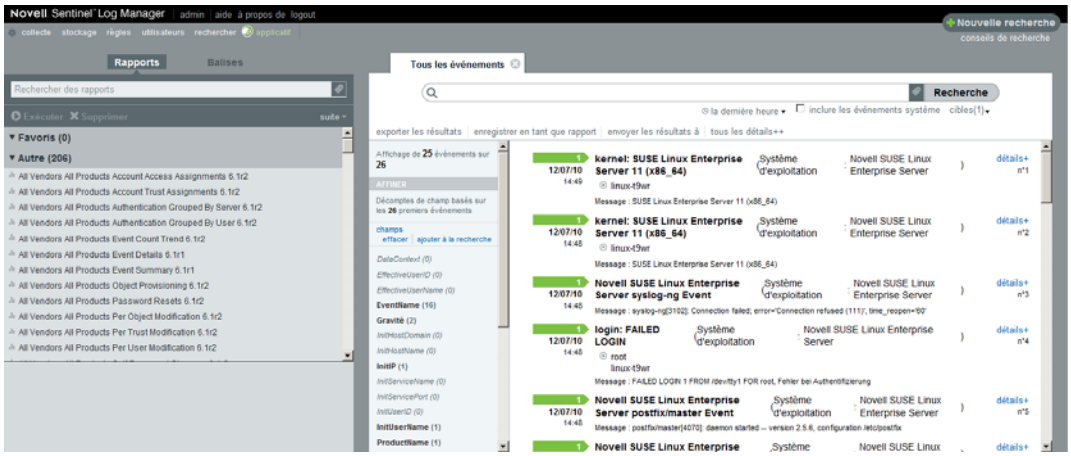
2 Vous pouvez configurer l'applicatif Sentinel Log Manager pour le stockage et la collecte de données. Pour plus d'informations sur la configuration de l'applicatif, reportez-vous au *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

3 Pour s'enregistrer afin de recevoir les mises à jour, reportez-vous à la Section 4.8, « Enregistrement pour obtenir les mises à jour », page 41.

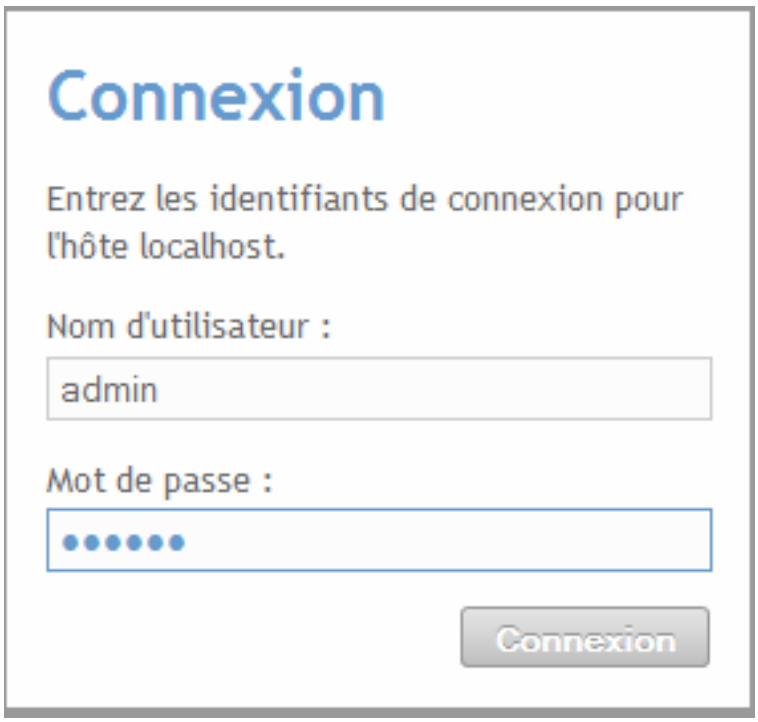
4.7 Configuration de WebYaST

L'interface utilisateur de l'applicatif Novell Sentinel Log Manager est équipée de WebYaST. WebYaST est une console à distance basée sur le Web qui contrôle les applicatifs basés sur SUSE Linux Enterprise. Vous pouvez accéder, configurer et surveiller les applicatifs Sentinel Log Manager avec WebYaST. La procédure suivante décrit brièvement les étapes de configuration de WebYaST. Pour plus d'informations sur la configuration détaillée, consultez le WebYaST User Guide (http://www.novell.com/documentation/webyast/) (Guide de l'utilisateur WebYaST).

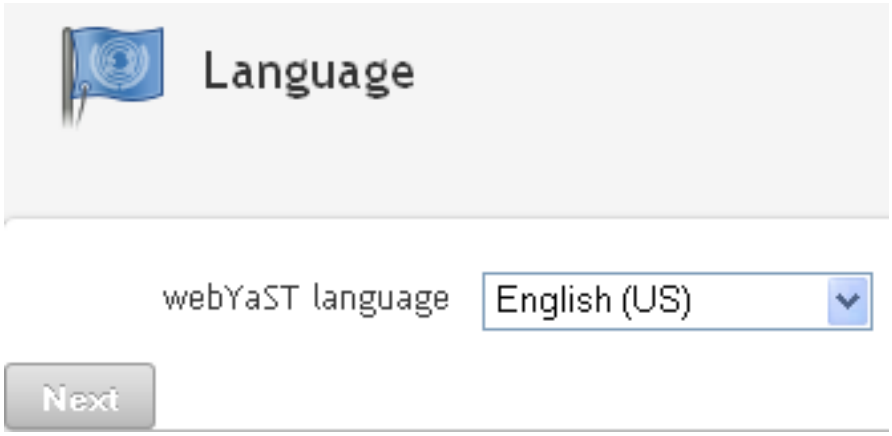
1 Loguez-vous à l'applicatif Sentinel Log Manager.



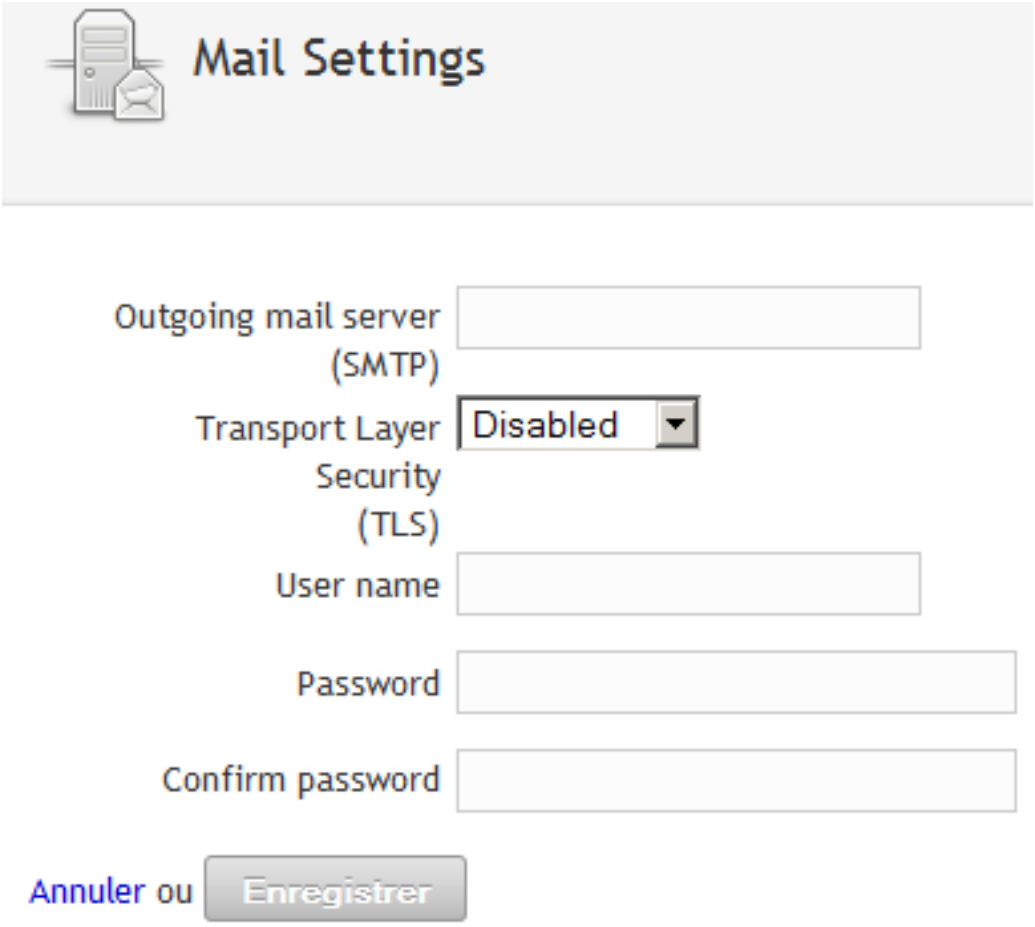
2 Cliquez sur *Applicatif*.



3 Spécifiez les références de login du système, puis cliquez sur *Login*.



4 Sélectionnez la langue de votre choix, puis cliquez sur *Suivant*.



5 Spécifiez les détails pour configurer le serveur de messagerie, puis cliquez sur *Enregistrer*.

La page relative à l'enregistrement s'affiche.

6 Configurez le serveur Sentinel Log Manager pour qu'il reçoive les mises à jour tel que décrit à la Section 4.8, « Enregistrement pour obtenir les mises à jour », page 41.

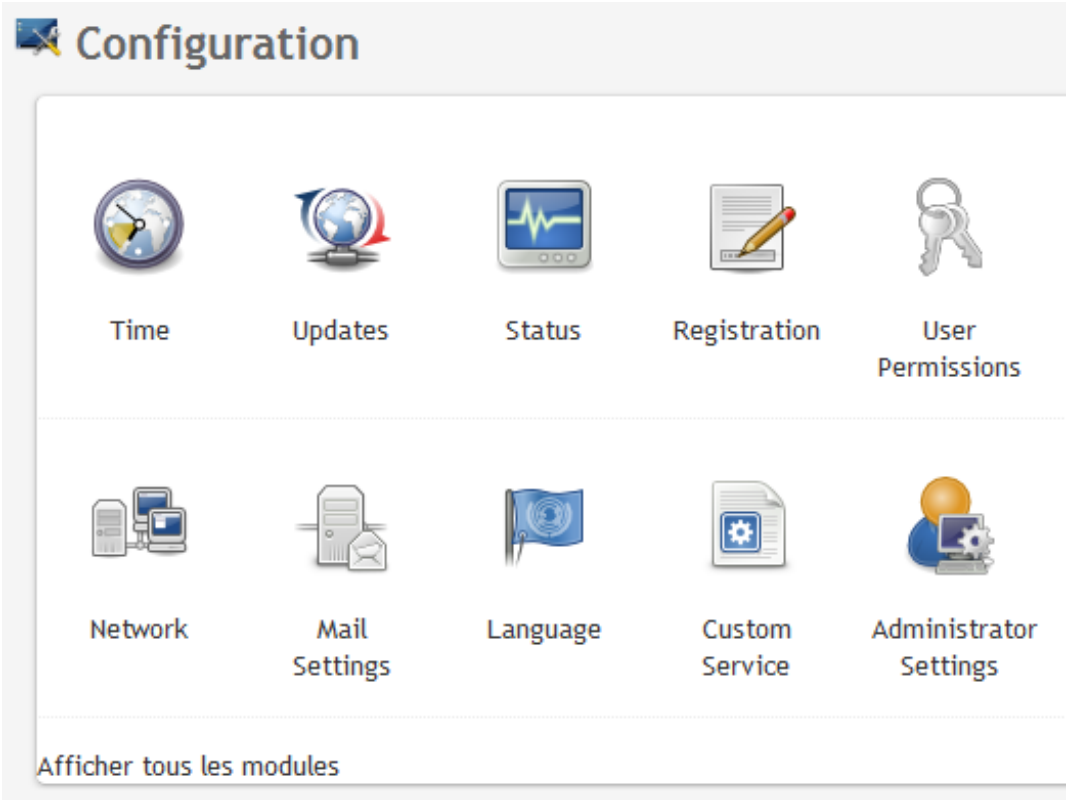
7 Cliquez sur *Suivant* pour terminer la configuration initiale.

4.8 Enregistrement pour obtenir les mises à jour

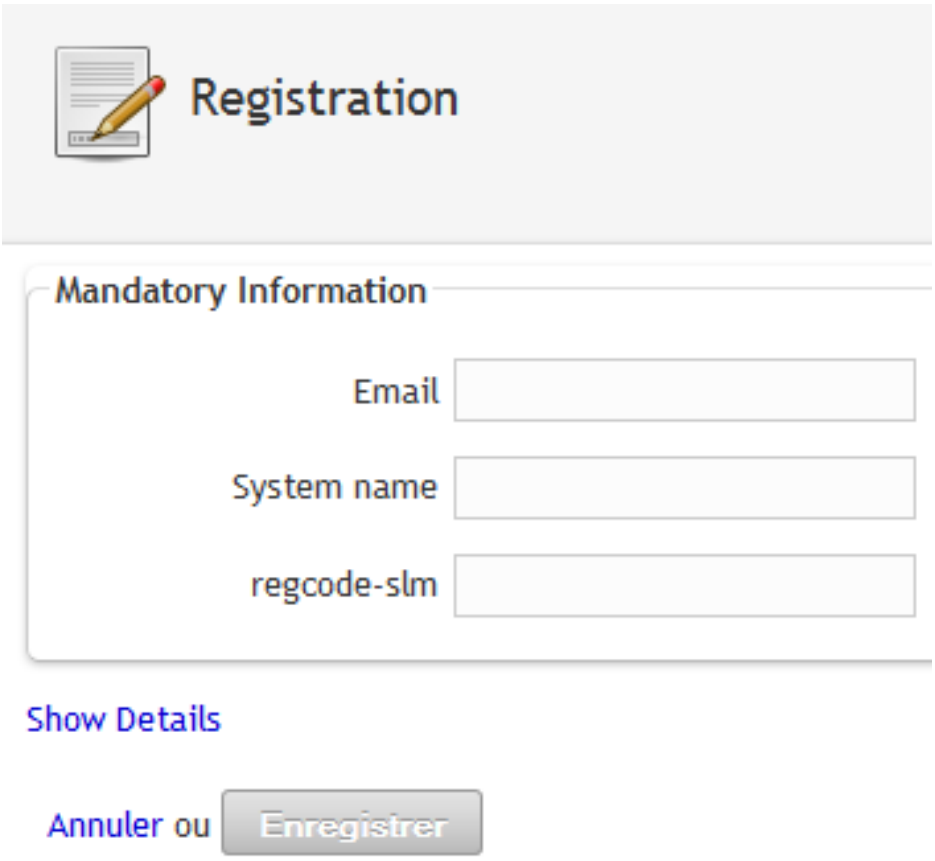
1 Loguez-vous à l'applicatif Sentinel Log Manager.

L'interface utilisateur Web de Sentinel Log Manager s'affiche.

2 Cliquez sur *Applicatif* pour démarrer WebYaST.



3 Cliquez sur *Enregistrement*.

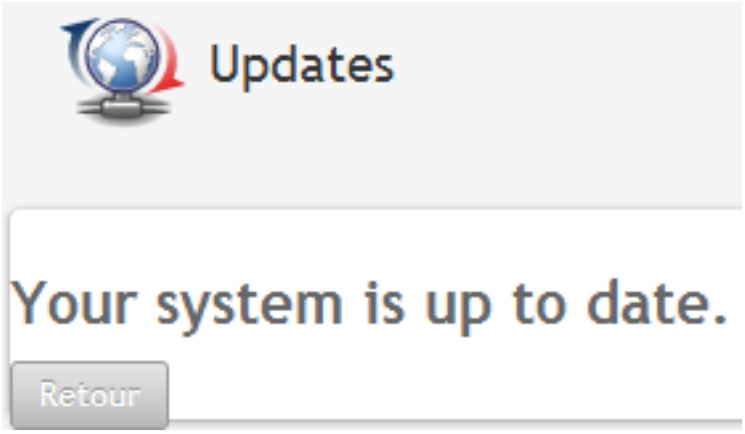


4 Spécifiez le code d'enregistrement de l'applicatif.

5 Cliquez sur *Enregistrer*.

6 Pour vérifier si des mises à jour sont disponibles, cliquez sur *Mettre à jour*.

La page qui s'affiche indique les éventuelles mises à jour.

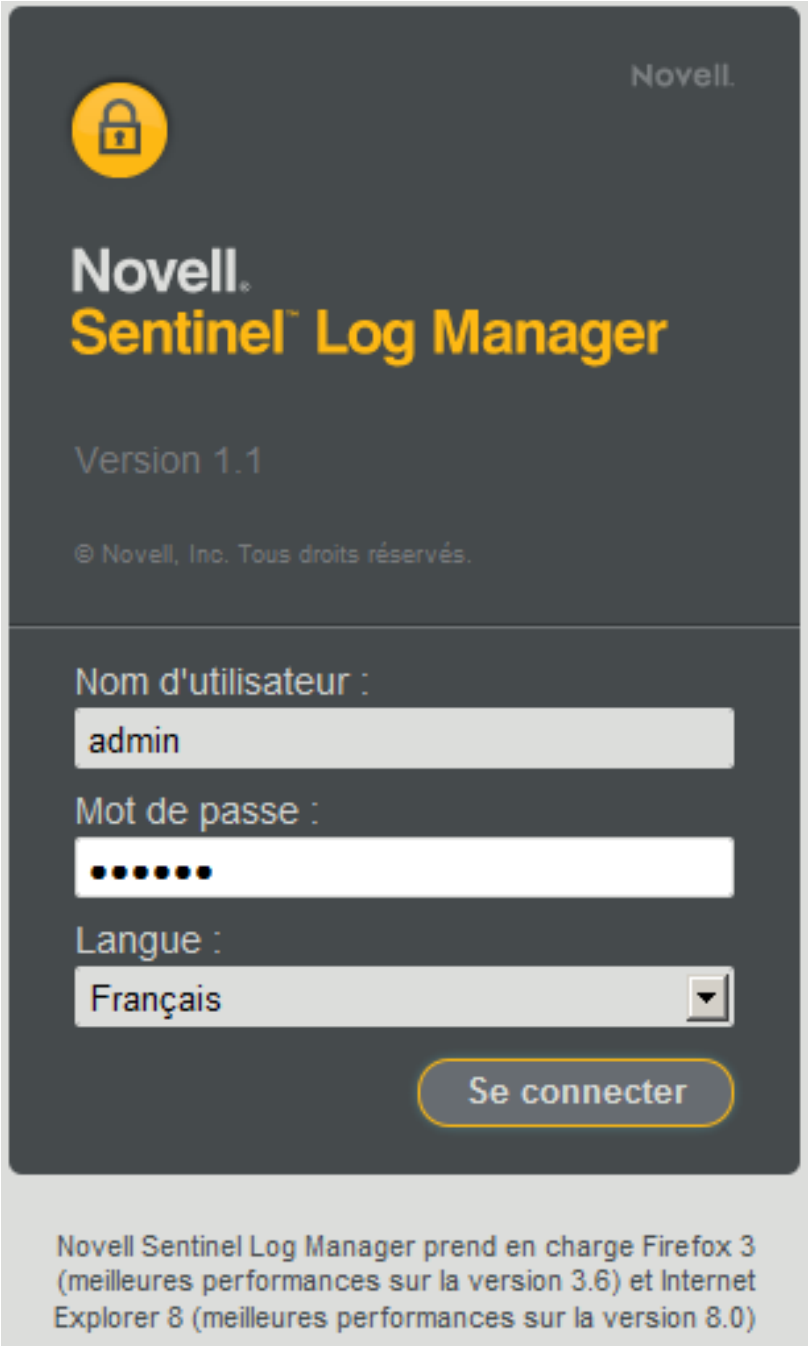


Login à l'interface Web

5

L'administrateur créé pendant l'installation peut se loguer à l'interface Web pour configurer et utiliser Sentinel Log Manager :

1. Ouvrez un navigateur Web pris en charge. Pour plus d'informations, reportez-vous à la Section 2.3, « Navigateurs pris en charge », page 21.
2. Spécifiez l'URL de la page Novell Sentinel Log Manager (par exemple, `https://10.0.0.1:8443/novelllogmanager`), puis appuyez sur Entrée.
3. (Facultatif) Lors de votre premier login à Sentinel Log Manager, vous êtes invité à accepter un certificat. Une fois accepté, la page de login de Sentinel Log Manager s'affiche.



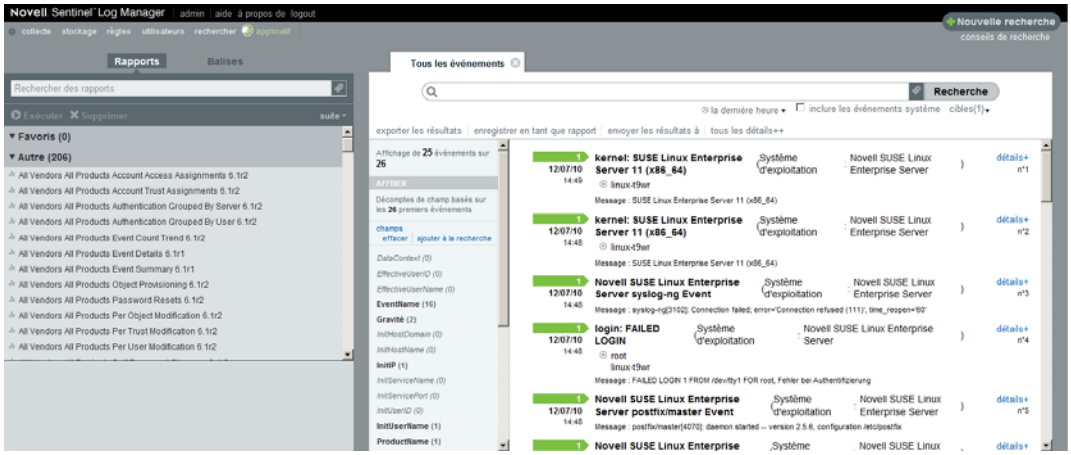
4 Spécifiez le nom d'utilisateur et le mot de passe de l'administrateur de Sentinel Log Manager.

5 Sélectionnez dans quelle langue utiliser l'interface Sentinel Log Manager.

L'interface utilisateur Sentinel Log Manager est disponible en anglais, portugais, français, italien, allemand, espagnol, japonais, chinois traditionnel ou simplifié.

6 Cliquez sur *Se connecter*.

L'interface utilisateur Web de Novell Sentinel Log Manager s'affiche.



Mise à niveau de Sentinel Log Manager

6

Vous pouvez mettre à niveau la version 1.0.0.4 de Novell Sentinel Log Manager ou une version ultérieure vers Sentinel Log Manager 1.1 à l'aide d'un script de mise à niveau.

6.1 Mise à niveau de la version 1.0 à la version 1.1

1. Si la version de votre serveur Sentinel Log Manager est antérieure à la version 1.0.0.4, vous devez d'abord la mettre à niveau vers la version 1.0.0.4 ou ultérieure.
2. Téléchargez et copiez les fichiers d'installation à partir du site Web de téléchargement Novell.
3. Loguez-vous en tant qu'utilisateur `root` au serveur sur lequel vous souhaitez installer Sentinel Log Manager.
4. Entrez la commande suivante pour arrêter le serveur Sentinel Log Manager :

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

   Par exemple, `/opt/novell/sentinel_log_mgr_1.0_x86-64/bin/server.sh stop`
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. Entrez la commande suivante pour exécuter le script `install-slm` afin de mettre à niveau Sentinel Log Manager :

   `./install-slm`
7. Pour continuer dans la langue de votre choix, sélectionnez le nombre spécifié en regard de la langue.

   L'accord de licence utilisateur final s'affiche dans la langue sélectionnée.
8. Lisez l'accord de licence utilisateur final et tapez `oui` ou `o` pour l'accepter et passer à l'installation.
9. Le script d'installation détecte qu'une version antérieure du produit existe déjà et vous demande si vous souhaitez mettre à niveau le produit. Si vous appuyez sur n, l'installation se termine. 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.

L'installation existante de Sentinel Log Manager 1.0 demeure intacte à quelques exceptions près :

- Si le répertoire de données 1.0 (par exemple, `/opt/novell/sentinel_log_manager_1.0_x86-64/data`) et le répertoire de données 1.1 (par exemple, `/var/opt/novell/sentinel_log_mgr/data`) se trouvent dans le même système de fichiers, les sous-répertoires `<1.0>/data/eventuate` et `<1.0>/data/rawdata` sont déplacés vers l'emplacement du répertoire 1.1 car les répertoires eventdata et rawdata sont généralement très volumineux. Si les répertoires de données 1.0 et 1.1 se trouvent dans différents systèmes de fichiers, les sous-répertoires eventdata et rawdata sont copiés à l'emplacement du répertoire 1.1 et les fichiers du répertoire 1.0 restent intacts.
- Si le répertoire de données existant 1.0 (par exemple, `/opt/novell/sentinel_log_mgr_1.0_x86-64`) se trouve sur un système de fichiers monté séparément et que l'espace est insuffisant sur le système de fichiers contenant le répertoire de données 1.1 (`/var/opt/novell/sentinel_log_mgr/data`), vous pouvez alors autoriser le programme d'installation à remonter le système de fichiers de l'emplacement 1.0 vers l'emplacement 1.1. Toute entrée du répertoire `/etc/fstab` est également mise à jour. Si vous décidez de ne pas autoriser le programme d'installation à remonter le système de fichiers existant, la mise à niveau est interrompue. Vous pouvez alors libérer l'espace suffisant sur le système de fichiers pour accueillir le répertoire de données 1.1.

10 Une fois Sentinel Log Manager 1.1 installé et le serveur fonctionnel, entrez la commande suivante pour supprimer manuellement le répertoire Sentinel Log Manager 1.0 :

```
rm -rf /opt/novell/slm_1.0_install_directory
```

Par exemple :

```
rm -rf /opt/novell/sentinel_log_mgr_1.0_x86-64
```

La suppression du répertoire d'installation supprime définitivement l'installation de Sentinel Log Manager 1.0.

6.2 Mise à niveau du gestionnaire des collecteurs

1 Loguez-vous à Sentinel Log Manager en tant qu'administrateur.

2 Sélectionnez *collecte* > *Avancé*.

3 Cliquez sur le lien *Download Installer* (Télécharger le programme d'installation) dans la section relative au programme d'installation de la mise à niveau du gestionnaire des collecteurs.

Une fenêtre s'affiche vous proposant d'ouvrir ou d'enregistrer le fichier `scm_upgrade_installer.zip` sur la machine locale. Enregistrez le fichier.

4 Copiez le fichier à un emplacement temporaire.

5 Dézippez le contenu du fichier `.zip`.

6 En tant que propriétaire de l'installation du gestionnaire des collecteurs, exécutez l'un des fichiers de mise à niveau suivants en fonction du logiciel que vous exécutez :

- Pour mettre à niveau le gestionnaire des collecteurs Windows, exécutez `service_pack.bat`.
- Pour mettre à niveau le gestionnaire des collecteurs Linux, exécutez `service_pack.sh`.

7 Suivez les instructions qui s'affichent à l'écran pour terminer l'installation.

8 Redémarrez la machine.

6.3 Migration de la version 1.0 vers la version 1.1 de l'applicatif

Si vous avez installé Sentinel Log Manager 1.0 et souhaitez migrer vers l'applicatif Sentinel Log Manager 1.1, suivez la procédure ci-dessous pour migrer les données et la configuration.

1 (Facultatif) Si la version de Sentinel Log Manager installée est antérieure à la version 1.0 avec la zone de réacheminent dynamique 4, procédez à la mise à niveau vers Sentinel Log Manager 1.0 avec la zone de réacheminent dynamique 5 (la dernière version de zone de réacheminent dynamique disponible). Téléchargez la zone de réacheminent dynamique à partir du site de téléchargement de correctifs Novell (http://download.novell.com/protected/Summary.jsp?buildid=VgZ3aerzjYc~).

Remarque : vous devez être un utilisateur enregistré pour télécharger des correctifs. Si vous n'êtes pas encore enregistré, cliquez sur Créer un compte pour créer un compte utilisateur et accéder au site de téléchargement des correctifs.

---

2 Effectuez une mise à niveau vers Sentinel Log Manager 1.1. Pour plus d'informations, reportez-vous à la Section 6.1, « Mise à niveau de la version 1.0 à la version 1.1 », page 49.

3 Entrez la commande suivante pour prendre l'identité de l'utilisateur `novell` :

```
su -novell
```

4 Entrez la commande suivante pour accéder au répertoire `/bin`.

```
cd /opt/novell/sentinel_log_mgr/bin
```

5 Entrez la commande suivante pour effectuer une sauvegarde complète des données et de la configuration de Sentinel Log Manager 1.1.

```
./backup_util.sh -m backup -c -e -l -r -s -w -f $APP_HOME/data/
<backupfilename>
```

Remplacez <*nom_fichier_sauvegarde*> par un nom de fichier dans lequel stocker les données de sauvegarde.

Pour plus d'informations sur la sauvegarde de données, reportez-vous à la section « Sauvegarde et restauration de données ».

6 Installez l'applicatif Sentinel Log Manager 1.1 sur une machine distincte. Pour plus d'informations, reportez-vous au Chapitre 4, « Installation de l'applicatif », page 33.

7 Copiez le fichier qui contient les données sauvegardées sur l'applicatif Sentinel Log Manager 1.1 qui vient d'être installé.

8 Entrez la commande suivante :

```
chown novell:novell <backfupfilename>
```

9 Entrez la commande suivante pour accéder au répertoire `/bin`.

```
cd /opt/novell/sentinel_log_mgr/bin
```

10 Entrez la commande suivante pour restaurer entièrement les données sauvegardées à partir de l'application Sentinel Log Manager 1.1 :

```
./backup_util.sh -m restore -f $APP_HOME/data/<backupfilename>
```

Pour plus d'informations, reportez-vous à la section « Sauvegarde et restauration de données ».

Installation de gestionnaires des collecteurs supplémentaires

7

Les gestionnaires des collecteurs gèrent la collecte de toutes les données et l'analyse de ces dernières pour Novell Sentinel Log Manager. Un gestionnaire des collecteurs est installé par défaut sur le serveur Sentinel Log Manager dans le cadre de la procédure d'installation de Sentinel Log Manager. Vous pouvez toutefois en installer plusieurs dans une configuration distribuée.

7.1 Avant de commencer

- Vérifiez que votre matériel et vos logiciels satisfont aux conditions de la configuration minimale requise mentionnées au Chapitre 2, « Configuration système requise », page 17.
- 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 Log Manager. Avant d'installer le gestionnaire des collecteurs, vérifiez que tous les paramètres du pare-feu et autres paramètres réseau sont autorisés à communiquer sur ce port.

7.2 Avantages de l'installation de gestionnaires des collecteurs supplémentaires

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 codage de même que la compression des données peuvent être effectués à la source.
- **Possibilité de collecter des données à partir d'autres systèmes d'exploitation :** vous pouvez par exemple installer un gestionnaire des collecteurs sous Microsoft Windows pour permettre la collecte des données par le biais du protocole WMI.
- **Caching de fichiers :** lorsque vous activez le caching de fichiers, le gestionnaire des collecteurs distant est capable de mettre en cache de grandes quantités de données alors 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.

7.3 Installation de gestionnaires des collecteurs supplémentaires

1. Loguez-vous à Sentinel Log Manager en tant qu'administrateur.
2. Sélectionnez *collecte* > *Avancé*.
3. Cliquez sur le lien *Download Installer* (Télécharger le programme d'installation) dans la section relative au programme d'installation du gestionnaire des collecteurs.

   Une fenêtre s'affiche vous proposant d'ouvrir ou d'enregistrer le fichier `scm_installer_.zip` sur la machine locale. Enregistrez le fichier.
4. Copiez et extrayez le fichier à l'emplacement où vous souhaitez installer le gestionnaire des collecteurs.
5. En fonction de votre système d'exploitation, exécutez l'un des fichiers d'installation suivants :
   - Pour installer le gestionnaire des collecteurs sur un système Windows, exécutez `setup.bat`.
   - Pour installer le gestionnaire des collecteurs sur un système Linux, exécutez `setup.sh`.
6. Sélectionnez une langue et cliquez sur *OK*.

   Le mécanisme de protection de l'installation s'affiche.
7. Cliquez sur OK.
8. Lisez et acceptez l'accord de licence, puis cliquez sur *Suivant*.
9. Vous pouvez continuer en acceptant le répertoire d'installation par défaut ou parcourir les répertoires pour en sélectionner un, puis cliquer sur *Suivant*.
10. Utilisez le port de bus de messages par défaut (61616) et spécifiez le nom d'hôte du serveur de communication, puis cliquez sur *Suivant*.
11. Cliquez sur *Suivant* pour accepter la Configuration de mémoire automatique par défaut (256 mégaoctets).

    Un résumé de l'installation s'affiche.
12. Cliquez sur *Installer*.
13. Indiquez le nom d'utilisateur et le mot de passe du gestionnaire des collecteurs.

    Remarque : le nom d'utilisateur et le mot de passe sont stockés dans le fichier `/etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties` situé sur le serveur Sentinel Log Manager.

    ---
14. Acceptez définitivement le certificat lorsque vous y êtes invité.
15. Cliquez sur *Terminer* pour quitter le processus d'installation.
16. Redémarrez la machine.

Désinstallation de Sentinel Log Manager

8

Cette section aborde les procédures de désinstallation du gestionnaire des collecteurs et du serveur Novell Sentinel Log Manager.

8.1 Désinstallation de l'applicatif

Si vous souhaitez conserver des données de Sentinel Log Manager, vous devez les sauvegarder avant de désinstaller l'applicatif, afin de pouvoir restaurer les données par la suite. Pour plus d'informations, reportez-vous à la section « Backing Up and Restoring Data » (Sauvegarde et restauration des données) du *Sentinel Log Manager 1.1 Administration Guide* (Guide d'administration de Sentinel Log Manager 1.1).

Si vous ne souhaitez conserver aucune donnée, suivez les procédures suivantes pour désinstaller l'applicatif :

- **Applicatif VMware ESX :** pour désinstaller l'applicatif virtuel du gestionnaire des journaux, si la machine virtuelle est dédiée exclusivement à Novell Sentinel Log Manager et que vous n'avez pas besoin de conserver de données, supprimez la machine virtuelle.
- **Applicatif Xen :** pour désinstaller l'applicatif virtuel du gestionnaire des journaux, si la machine virtuelle Xen est dédiée exclusivement à Novell Sentinel Log Manager et que vous n'avez pas besoin de conserver de données, supprimez la machine virtuelle.
- **Applicatif matériel :** pour désinstaller le gestionnaire des journaux d'une machine physique, si le système est dédié exclusivement à Novell Sentinel Log Manager et que vous n'avez pas besoin de conserver de données, reformatez le disque dur.

8.2 Désinstallation à partir d'un système SLES 11 existant

1. Loguez-vous au serveur Sentinel Log Manager en tant qu'utilisateur `root`.
2. Pour exécuter le script de désinstallation, exécutez la commande suivante :

   ```
   /opt/novell/sentinel_log_mgr/setup/uninstall-slm
   ```
3. Lorsque vous êtes invité à confirmer que vous souhaitez procéder à la désinstallation, appuyez sur o.

   Le serveur Sentinel Log Manager est d'abord arrêté, puis désinstallé.

8.3 Désinstallation du gestionnaire des collecteurs

Cette section aborde les procédures de désinstallation de Sentinel Collector Manager installé sur des machines Windows ou Linux.

8.3.1 Désinstallation du gestionnaire des collecteurs sous Linux

1. Loguez-vous en tant qu'utilisateur `root`.
2. Dans la machine sur laquelle le gestionnaire des collecteurs est installé, naviguez jusqu'à l'emplacement suivant :

   ```
   $ESEC_HOME/_unist
   ```
3. Exécutez la commande suivante :

   ```
   ./uninstall.bin
   ```
4. Sélectionnez une langue et cliquez sur *OK*.
5. Cliquez sur *Suivant* dans l'assistant de protection de l'installation.
6. Sélectionnez les fonctions à désinstaller, puis cliquez sur *Suivant*.
7. Arrêtez toutes les applications Sentinel Log Manager en cours d'exécution, puis cliquez sur *Suivant*.
8. Cliquez sur *Désinstaller*.
9. Cliquez sur *Terminer*.
10. Sélectionnez *Reboot the system* (Redémarrer le système), puis cliquez sur *Terminer*.

8.3.2 Désinstallation du gestionnaire des collecteurs sous Windows

1. Loguez-vous en tant qu'administrateur.
2. Arrêtez le serveur Sentinel Log Manager.
3. Sélectionnez Démarrer > Exécuter.
4. Spécifiez les informations suivantes :

   ```
   %Esec_home%\_uninst
   ```
5. Double-cliquez sur le fichier `uninstall.exe` pour l'exécuter.
6. Sélectionnez une langue et cliquez sur *OK*.

   L'assistant de protection de l'installation s'affiche.
7. Cliquez sur Suivant.
8. Sélectionnez les fonctions à désinstaller, puis cliquez sur *Suivant*.

9 Arrêtez toutes les applications Sentinel Log Manager en cours d'exécution, puis cliquez sur *Suivant*.

10 Cliquez sur *Désinstaller*.

11 Cliquez sur *Terminer*.

12 Sélectionnez *Reboot the system* (Redémarrer le système), puis cliquez sur *Terminer*.

8.3.3 Nettoyage manuel des répertoires

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

Linux

1 Loguez-vous en tant qu'utilisateur `root` à la machine de laquelle vous souhaitez supprimer le gestionnaire des collecteurs.

2 Arrêtez tous les processus Sentinel Log Manager.

3 Supprimez le contenu du répertoire `/opt/novell/sentinel6`.

Windows

1 Loguez-vous en tant qu'administrateur à la machine de laquelle vous souhaitez supprimer le gestionnaire des collecteurs.

2 Supprimez le dossier `%CommonProgramFiles%\InstallShield\Universal` et l'ensemble de son contenu.

3 Supprimez le dossier `%ESEC_HOME%` situé à l'emplacement par défaut : `C:\Program Files\Novell\Sentinel6`.

Dépannage - installation

A

Cette section présente certains des problèmes pouvant survenir pendant l'installation ainsi que la procédure 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 Log Manager sur l'applicatif échoue.

Pour résoudre ce problème, veuillez configurer correctement les paramètres réseau. Lors de la vérification de la configuration, la commande `ifconfig` doit renvoyer une adresse IP valide, et la commande `hostname -f` doit renvoyer un nom d'hôte valide.

A.2 Problème de configuration du réseau avec VMware Player 3 sous SLES 11

L'erreur suivante risque de se produire lorsque vous essayez de configurer le réseau avec VMware Player 3 sous SLES 11 :

```
Jan 12 14:57:34.761: vmx| VNET: MACVNetPortOpenDevice: Ethernet0: can't open
vmnet device (No such device or address)
Jan 12 14:57:34.761: vmx| VNET: MACVNetPort_Connect: Ethernet0: can't open
data fd
Jan 12 14:57:34.761: vmx| Msg_Post: Error
Jan 12 14:57:34.761: vmx| [msg.vnet.connectvnet] Could not connect Ethernet0
to virtual network "/dev/vmnet0". More information can be found in the
vmware.log file.
Jan 12 14:57:34.761: vmx|[msg.device.badconnect] Failed to connect virtual
device Ethernet0.
Jan 12 14:57:34.761: vmx| --
```

Cette erreur signifie que le fichier VMX a peut-être été ouvert par une autre machine virtuelle. Pour corriger cette erreur, vous devez mettre à jour l'adresse MAC dans le fichier VMX comme suit :

1. Ouvrez le fichier VMX dans un éditeur de texte.
2. Copiez l'adresse MAC à partir du champ `ethernet0.generatedAddress`.
3. Ouvrez le fichier `/etc/udev/rules.d/70-persistent-net.rules` à partir du système d'exploitation invité.
4. Mettez en commentaire la ligne originale, puis tapez une ligne `SUBSYSTEM` comme suit :

```
SUBSYSTEM=="net", DRIVERS=="?*", ATTRS{address}==<MAC address>,
NAME="eth0"
```

5 Remplacez <*adresse MAC*> par l'adresse MAC copiée à l'Étape 2.

6 Enregistrez et fermez le fichier.

7 Ouvrez la machine virtuelle dans VMware Player.

A.3 Mise à niveau de Sentinel Log Manager installé par un utilisateur non-root autre que novell

La procédure de mise à niveau échoue si vous essayez de mettre à niveau le serveur Novell Sentinel Log Manager 1.0 installé avec l'identité d'un utilisateur non-root autre que `novell`. Ce problème survient en raison de la nature des autorisations de fichier définies lors de l'installation de Sentinel Log Manager 1.0.

Pour mettre à niveau le serveur Sentinel Log Manager 1.0 installé avec l'identité d'un utilisateur non-root autre que `novell`, procédez comme suit :

1 Créez l'utilisateur `novell`.

2 Modifiez la propriété de l'installation de Sentinel Log Manager 1.0 en `novell:novell`.

```
chown -R novell:novell /opt/novell/<install_directory>
```

Remplacez <*répertoire_installation*> par le nom du répertoire d'installation. Exemples

```
chown -R novell:novell /opt/novell/sentinel_log_mgr_1.0_x86-64
```

3 Modifiez l'entrée ESEC_USER dans le répertoire `config/esecuser.properties` en `novell`.

4 Loguez-vous en tant qu'utilisateur `root`, puis effectuez une mise à niveau vers Sentinel Log Manager 1.1. Pour plus d'informations sur la mise à niveau, reportez-vous à la Section 6.1, « Mise à niveau de la version 1.0 à la version 1.1 », page 49.

Terminologie Sentinel

Cette section décrit la terminologie employée dans ce document.

Collecteurs
Utilitaire qui analyse les données et fournit un flux d'événements plus riche en intégrant une taxonomie, une détection d'exploits et des informations pertinentes sur le plan professionnel au flux de données avant que les événements ne soient corrélés, analysés et envoyés à la base de données.

Connecteurs
Utilitaire qui emploie des méthodes normalisées pour le secteur pour se connecter à la source de données et obtenir des données brutes.

Conservation des données
Stratégie qui définit la durée de conservation des événements avant leur suppression du serveur Sentinel Log Manager.

Source d'événements
Applicateur ou système qui consigne l'événement.

Gestion de source d'événements
ESM. Interface qui permet de gérer et de surveiller les connexions entre Sentinel et ses sources d'événements, en employant des connecteurs et des collecteurs Sentinel.

Événements par seconde
EPS. Valeur qui mesure la vitesse à laquelle un réseau génère des données à partir de ses périphériques et applications de sécurité. Il s'agit également du taux auquel Sentinel Log Manager peut collecter et stocker les données des périphériques de sécurité.

Intégrateur
Plug-ins permettant aux systèmes Sentinel de se connecter à d'autres systèmes externes. Les opérations JavaScript peuvent utiliser les intégrateurs pour interagir avec d'autres systèmes.

Données brutes
Événements non traités reçus par le connecteur et directement envoyés au bus de messages Sentinel Log Manager, puis inscrits sur le disque sur le serveur Sentinel Log Manager. Les données brutes varient d'un connecteur à l'autre en raison du format des données stockées sur le périphérique.