AUTHORIZED DOCUMENTATION

Guide de l'utilisateur

October 31, 2008

Novell®
Identity Audit

1.0

www.novell.com

Mentions légales

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

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

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

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

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

Documentation en ligne : pour accéder à la 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 Novell de documentation (http://www.novell.com/documentation).

Marques de Novell

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

Éléments tiers

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

Tables des matières

À propos de ce guide

Ce guide traite de l'installation et de la configuration de Novell® Identity Audit.

Public

Ce guide s'adresse aux administrateurs de Novell Identity Audit.

Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce guide et les autres documentations fournies avec ce produit. Utilisez la fonction Commentaires proposée au bas de chaque page de la documentation en ligne ou accédez à la page Web www.novell.com/documentation/feedback.html (en anglais).

Mises à jour de la documentation

Pour consulter la dernière version du *Novell Identity Audit 1.0 Guide* (Guide de Novell Identity Audit 1.0), visitez le site Web de documentation de Identity Audit (http://www.novell.com/documentation/identityaudit).

Conventions relatives à la documentation

Dans la documentation Novell, le symbole « supérieur à » (>) est utilisé pour séparer deux opérations dans une étape de procédure, ainsi que deux éléments dans un chemin de références croisées.

Un symbole de marque déposée (®, ™, etc.) indique qu'il s'agit d'une marque de Novell. L'astérisque (*) indique une marque de fabricant tiers.

Introduction

1

Novell® Identity Audit offre des fonctions de création de rapports et de surveillance pour tous les événements survenant au sein de l'environnement Novell Identity and Security Management (ISM), composé notamment de Novell eDirectory™, Novell Identity Manager, Novell Access Manager, Novell Modular Authentication Services (NMAS™), Novell SecureLogin et Novell SecretStore®.

1.1 Présentation du produit

Novell Identity Audit 1.0 est un outil convivial et peu encombrant conçu pour faciliter la collecte, le regroupement et le stockage des événements de Novell Identity Manager, Novell Access Manager, Novell eDirectory ainsi que d'autres technologies et produits Novell relatifs à la gestion des identités et de la sécurité. Ses principales fonctionnalités sont les suivantes :

- Interfaces d'administration et de création de rapports basées sur le Web
- Outil complet permettant des recherches d'événement sur plusieurs champs
- Sortie d'événements sélectionnée vers plusieurs canaux
- Moteur Jasper Reports intégré permettant l'utilisation d'outils Open Source pour personnaliser les rapports existants ou en créer de nouveaux
- Base de donnes intégrée qui supprime la nécessité d'administrer des bases de données externes ou de disposer de licences pour ces dernières
- Outils de gestion de données simples et intuitifs

1.1.1 Comparaison avec Novell Audit 2.0.2

Le programme Novell Identity Audit 1.0 est destiné à remplacer la gamme de produits Novell Audit, qui ne bénéficiera plus du support général à partir de février 2009. Il est comparable d'un point de vue fonctionnel, mais présente des améliorations majeures en termes d'architecture, de création de rapports et de gestion des données. Novell Identity Audit 1.0 est un substitut direct du serveur de consignation sécurisée de Novell Audit 2.0.2 pour les produits de la gamme Novell Identity et Novell Security. Étant donné que Novell Identity Audit utilise une nouvelle base de données intégrée, il est préférable que les clients conservent les événements Novell Audit existants dans la base de données Novell Audit archivée plutôt que de tenter de migrer les données héritées.

Le composant client Novell Audit, également appelé agent de plate-forme, est toujours utilisé comme mécanisme de transport des données pour Novell Identity Audit. Sa prise en charge se poursuivra en fonction des cycles de vie des produits Novell de gestion des accès et des identités, qui l'utilisent encore.

1.1.2 Comparaison avec Novell Sentinel

Novell Identity Audit s'appuie sur des technologies éprouvées dans la mesure où une grande part du code sous-jacent est commune à Novell Sentinel. Toutefois, ce dernier collecte des données auprès d'un plus grand éventail de périphériques, prend en charge un taux d'événements plus élevé et fournit davantage d'outils que Novell Identity Audit. Par ailleurs, Sentinel met à disposition des fonctions de gestion des événements et des informations de sécurité (SIEM), telles que des tableaux de bord en temps réel, une corrélation multi-événement, un suivi des incidents, un traitement automatisé et la collecte de données provenant de produits non-Novell. Identity Audit est conçu pour s'intégrer dans un déploiement Sentinel ultérieur.

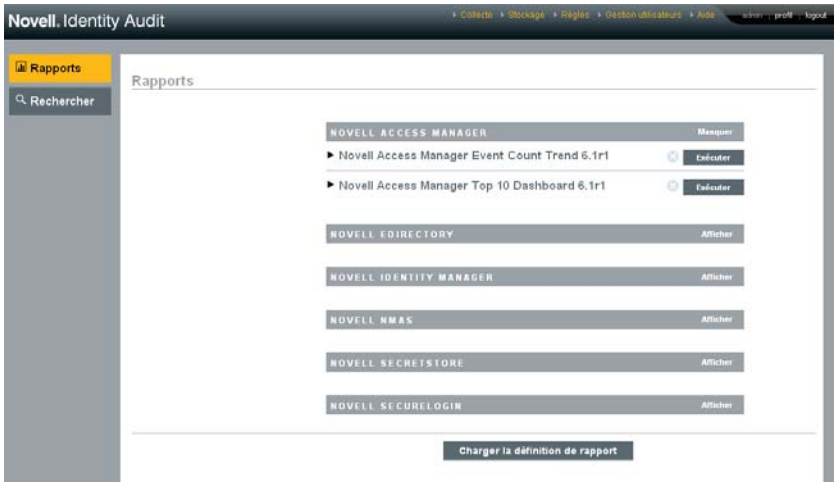
Étant donné qu'il ne fait pas partie de la plate-forme de gestion de la conformité (CMP, Compliance Management Platform) Novell, Novell Identity Audit 1.0 n'inclut pas les fonctions avancées d'intégration de la sécurité et de l'identité de cette dernière. Sentinel 6.1 constitue actuellement le composant d'audit et de surveillance des identités de la plate-forme CMP.

1.2 Interface

L'interface Web de Novell Identity Audit permet d'effectuer les tâches suivantes :

- télécharger, exécuter, consulter et supprimer des rapports ;
- rechercher des événements ;
- éditer les détails des profils utilisateur ;
- créer, éditer et supprimer des utilisateurs, ainsi qu'assigner des droits d'administration (fonctionnalités exclusivement réservées aux administrateurs) ;
- configurer la collecte des données et afficher l'état de santé des sources d'événements (fonctionnalités exclusivement réservées aux administrateurs) ;
- configurer le stockage des données et afficher l'état de santé de la base de données (fonctionnalités exclusivement réservées aux administrateurs) ;
- créer des règles de filtre et configurer des opérations associées pour envoyer les données d'événement correspondantes aux canaux de sortie (fonctionnalités exclusivement réservées aux administrateurs).

Figure 1-1 *Interface de Novell Identity Audit (vue de l'administrateur)*



L'interface se rafraîchit automatiquement toutes les 30 secondes pour afficher les mises à jour effectuées par les autres utilisateurs, le cas échéant.

L'interface est disponible en plusieurs langues (anglais, français, allemand, italien, japonais, portugais, espagnol, chinois simplifié et traditionnel). La langue par défaut de l'interface est celle du navigateur, mais l'utilisateur peut en sélectionner une autre au moment du login.

Remarque : bien que l'interface soit localisée dans des langues à double octet, la version actuelle de Identity Audit ne traite pas les données d'événement à double octet.

1.3 Architecture

Identity Audit collecte des données de plusieurs applications d'identité et de sécurité Novell. Ces serveurs d'application sont configurés pour générer des enregistrements d'événement et chacun héberge un agent de plate-forme, lequel fait partie de l'application Novell Audit. Les données d'événement sont transférées par l'agent de plate-forme vers un connecteur d'audit qui réside sur le serveur Identity Audit.

Le connecteur d'audit transmet les événements au composant Collecte des données qui analyse les événements et les place dans le bus de communications, lequel constitue l'épine dorsale du système et négocie toutes les communications entre les composants. Dans le cadre de la collecte des données, les événements entrants sont évalués par un ensemble de règles de filtre. Ces règles filtrent les événements et les envoient à des canaux de sortie tels qu'un fichier ou un relais Syslog.

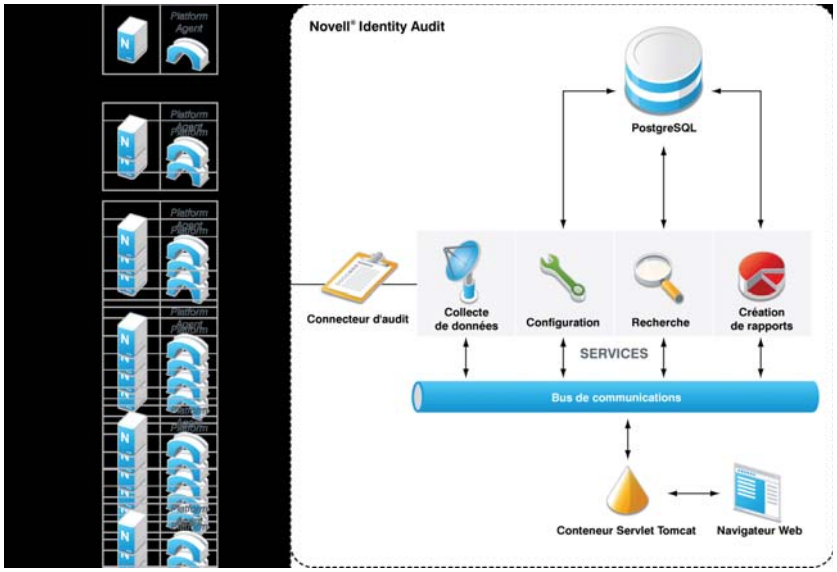
Par ailleurs, tous les événements sont stockés dans la base de données Identity Audit (optimisée par PostgreSQL*), dans des tables partitionnées.

Le composant Configuration récupère, ajoute et modifie les informations de configuration telles que les paramètres de collecte et de stokage des données ainsi que les définitions de règle et de rapport. Il gère également l'authentification utilisateur.

Le composant de recherche effectue des recherches rapides, indexées, et récupère des événements de la base de données pour présenter des ensembles de résultats de recherche à l'utilisateur.

Le composant de création de rapports exécute des rapports et en formate les résultats.

Figure 1-2 *Architecture de Identity Audit*



Les utilisateurs interagissent avec le serveur Identity Audit et l'ensemble de ses fonctionnalités via un navigateur Web, lequel se connecte à un serveur Web Apache Tomcat. Ce dernier envoie des appels aux différents composants Identity Audit via le bus de communications.

Configuration système requise

2

Outre les exigences en termes de matériel, système d'exploitation, navigateur et compatibilité de source d'événements décrites ci-après, l'installation nécessite un accès à la racine du système d'exploitation pour la création du groupe et de l'utilisateur novell, qui sont les propriétaires des processus s'exécutant pour Identity Audit.

2.1 Configuration matérielle requise

Novell Identity Audit™ est compatible avec le matériel Intel Xeon* et AMD Opteron* 64 bits. Il n'est pas pris en charge par le matériel Itanium. Novell recommande le matériel suivant pour un système de production qui conserve 90 jours de données en ligne :

- 1x Quad Core (x86-64)
- 16 Go de RAM
- 1,5 To d'espace disque utilisable - 3 disques de 500 Go (3 utilisables), 10 000 t/min en RAID
  - environ 2/3 de l'espace disque utilisable pour les fichiers de base de données ;
  - environ 1/3 de l'espace disque utilisable pour les fichiers temporaires et d'index de recherche ;
  - Une petite quantité d'espace de stockage est disponible pour les données archivées supprimées de la base de données, mais Novell recommande de déplacer les fichiers de données archivées vers un autre support.

Tableau 2-1 *Performances*

Valeur	métrique	Description
Événements par seconde (eps) - niveau stable	100	Taux d'événements moyen pendant les opérations normales
Événements par seconde (eps) - niveau élevé	500	Taux d'événements élevé pendant un pic (jusqu'à 10 minutes)

Valeur	métrique	Description
Événements par seconde (eps) - niveau élevé par application	300	Taux d'événements élevé pour chaque type d'application Novell ◆ Les taux d'événements sont généralement faibles (inférieurs à 15 eps) pour Identity Manager, SecureLogin, SecretStore® et NMAS™). ◆ Les taux d'événements peuvent être très élevés pour eDirectory™ et Access Manager. Le filtrage des événements doit être appliqué afin de maintenir le taux à un niveau gérable. ◆ Même lors d'un pic d'événements, aucune application ne peut envoyer un nombre d'événements par seconde supérieur à celui-ci.
Données en ligne	90 jours ou 750 millions d'événements	La quantité de données que Identity Audit peut stocker à un taux stable d'environ 100 eps, avec l'espace de stockage recommandé

2.2 Systèmes d'exploitation pris en charge

Identity Audit est certifié pour une exécution sous SuSE Linux Enterprise Server™ 64 bits 10 SP 1 et SP2.

2.3 Navigateurs pris en charge

Identity Audit prend en charge les navigateurs suivants. Les autres navigateurs risquent de ne pas afficher correctement les informations.

Tableau 2-2 *Navigateurs Web pris en charge par Novell Identity Audit*

Navigateur Web et version
Mozilla Firefox 2
Mozilla Firefox 3
Microsoft Internet Explorer 7

Les performances dans le cadre des recherches et de la consultation des rapports semblent varier d'un navigateur à l'autre. Novell a remarqué que les performances de Mozilla Firefox 3 étaient particulièrement bonnes.

2.4 Agent de plate-forme pris en charge

Identity Audit 1.0 prend en charge la collecte des événements de journal provenant de nombreuses applications qui étaient supportées par Novell Audit et son agent de plate-forme. Pour des sources d'événements 32 bits, Identity Audit requiert la version 2.0.2 FP6 (2.0.2.55) ou une version supérieure de l'agent de plate-forme. Pour des sources d'événements 64 bits, il convient d'utiliser la version 2.0.2 FP6 de l'agent de plate-forme.

Remarque : certaines applications Novell sont fournies avec une version antérieure de l'agent de plate-forme. La version conseillée comporte des résolutions de bogues importantes, raison pour laquelle Novell recommande d'effectuer la mise à niveau de l'agent de plate-forme.

2.5 Sources d'événements prises en charge

Identity Audit prend en charge la collecte de données des applications d'identité et de sécurité Novell. certaines applications nécessitent un niveau de correctif spécifique pour pouvoir collecter les données correctement.

Tableau 2-3 *Applications prises en charge par Novell Identity Audit*

Application
Novell Access Manager 3.0
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 Identity Manager 3.6
Novell NMAS 3.1
Novell SecretStore 3.4
Novell SecureLogin 6.0

Installation

3

Ce chapitre explique comment installer Novell Identity Audit et comment configurer les sources d'événements pour lui envoyer des données. Ces instructions présupposent le respect de la configuration minimale requise pour chaque composant système. Pour plus d'informations, reportez-vous au Chapitre 2, « Configuration système requise », page 13.

3.1 Installation de Novell Identity Audit

Le paquetage d'installation de Identity Audit installe tous les éléments requis pour l'exécution de Identity Audit, à savoir l'application et le bus de messages Identity Audit, la base de données pour le stockage des événements et des informations de configuration, l'interface utilisateur Web, ainsi que le serveur de création de rapports. Il propose deux options : une installation simple qui peut être exécutée en tant qu'utilisateur root et une installation en plusieurs étapes, qui utilise le moins possible l'utilisateur root.

3.1.1 Installation rapide (en tant qu'utilisateur root)

Cette installation simple doit être exécutée en tant qu'utilisateur root.

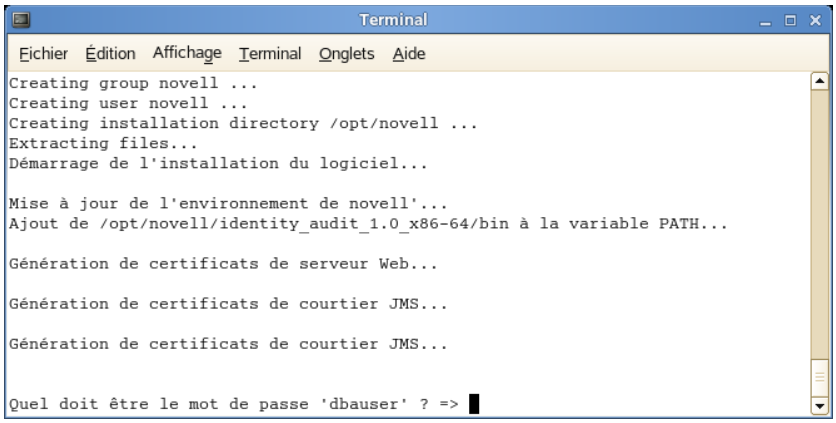
1. Loguez-vous en tant qu'utilisateur `root` au serveur sur lequel vous voulez installer Identity Audit.
2. Téléchargez ou copiez le fichier `identity_audit_1.0_x86-64.tar.gz` dans un répertoire temporaire.
3. Extrayez le script d'installation du fichier à l'aide de la commande suivante :

   ```
   tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup/root_install_all.sh
   ```
4. Exécutez le script `root_install_all.sh` à l'aide de la commande suivante :

   ```
   identity_audit_1.0_x86-64/setup/root_install_all.sh identity_audit_1.0_x86-64.tar.gz
   ```
5. Choisissez une langue en entrant un numéro.

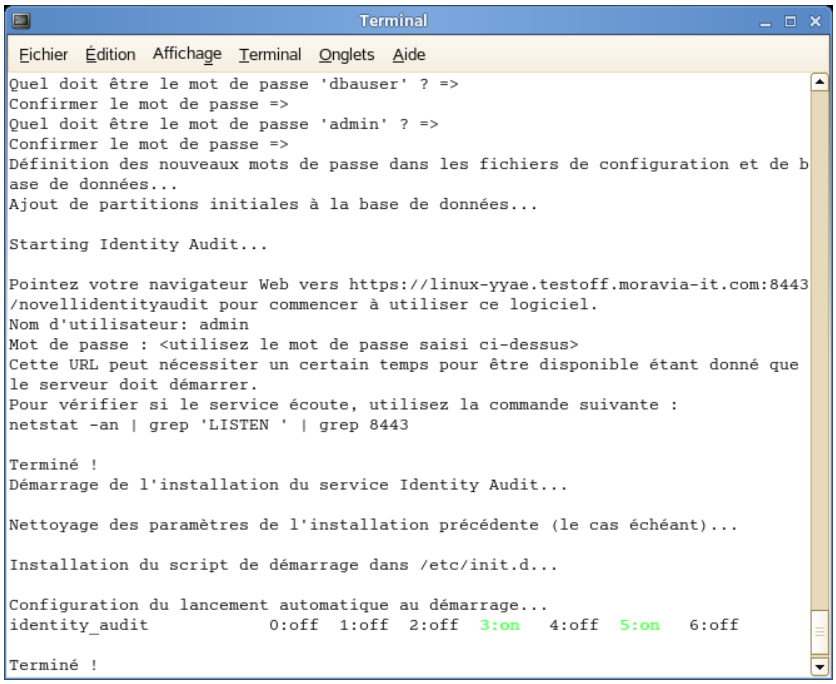
   L'accord de licence utilisateur final s'affiche dans la langue sélectionnée.
6. Après avoir lu l'accord de licence utilisateur final, entrez `1` ou `y` si vous en acceptez les termes et souhaitez continuer l'installation.

   L'installation démarre. Si la langue sélectionnée n'est pas disponible pour ce programme d'installation (par exemple, le polonais), le programme d'installation poursuit en anglais.



L'utilisateur et le groupe novell sont créés, à moins qu'ils n'existaient déjà.

7. Entrez le mot de passe de l'administrateur de la base de données (dbauser).
8. Confirmez le mot de passe de l'administrateur de la base de données (dbauser).
9. Entrez le mot de passe de l'utilisateur admin.
10. Confirmez le mot de passe de l'utilisateur admin.



Les références dbauser sont utilisées pour la création de tables et de partitions dans la base de données PostgreSQL. Identity Audit est configuré pour démarrer avec des niveaux d'exécution 3 et 5 (mode multi-utilisateur avec programme amorce dans la console ou mode X-Windows).

Une fois le service Identity Audit démarré, vous pouvez vous loguer à l'URL spécifiée dans le résultat de l'installation (https://hostIP:8443/novellidentityaudit). Le système commencera immédiatement à traiter les événements d'audit interne et sera entièrement opérationnel lorsque vous aurez configuré les sources d'événements pour l'envoi de données à Identity Audit.

3.1.2 Installation non-root

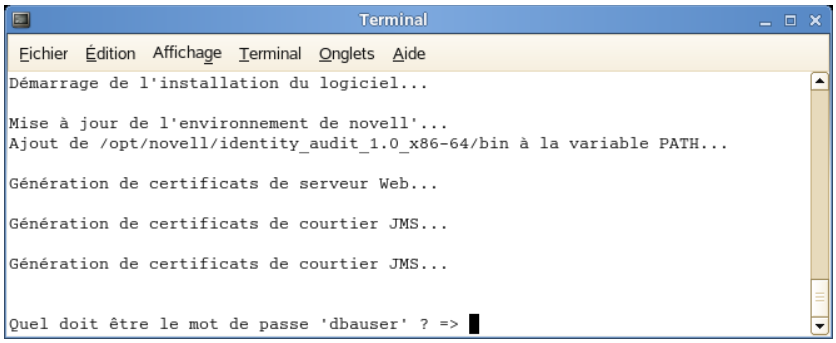
Si la stratégie organisationnelle empêche l'exécution de l'ensemble du processus d'installation en tant que `root`, l'installation peut être réalisée en deux étapes. La première doit être effectuée avec un accès au niveau root, tandis que la deuxième s'opère en tant qu'administrateur Identity Audit (créé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

1. Loguez-vous en tant qu'utilisateur `root` au serveur sur lequel vous voulez installer Identity Audit.
2. Téléchargez ou copiez le fichier `identity_audit_1.0_x86-64.tar.gz` dans le répertoire `/tmp`.
3. Si l'utilisateur et le groupe novell n'existent pas encore sur le serveur :
   1. Extrayez le script de création de l'utilisateur et du groupe novell à partir du fichier tar de Identity Audit. Exemples :
      ```
      tar xfz identity_audit_1.0_x86-64.tar.gz
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
   2. En tant que `root`, exécutez le script à l'aide de la commande suivante :
      ```
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
      L'utilisateur et le groupe novell seront les propriétaires de l'installation et des processus s'exécutant pour Identity Audit.
4. Créez un répertoire pour Identity Audit. Exemples :

   mkdir -p /opt/*novell*
5. Définissez le répertoire devant appartenir à l'utilisateur et au groupe novell. Exemples :
   ```
   chown -R novell:novell /opt/novell
   ```
6. Loguez-vous en tant qu'utilisateur novell :
   ```
   su novell
   ```
7. Extrayez le fichier tar de Identity Audit dans le répertoire que vous venez de créer. Exemples :
   ```
   cd /opt/novell
   tar xfz /tmp/identity_audit_1.0_x86-64.tar.gz
   ```
8. Exécutez le script d'installation. Exemples :
   ```
   /opt/novell/identity_audit_1.0_x86-64/setup/install.sh
   ```
9. Choisissez une langue en entrant un numéro.

   L'accord de licence utilisateur final s'affiche dans la langue sélectionnée.
10. Après avoir lu l'accord de licence utilisateur final, entrez `1` ou `y` si vous en acceptez les termes et souhaitez continuer l'installation.

    L'installation démarre. Si la langue sélectionnée n'est pas disponible pour ce programme d'installation (par exemple, le polonais), le programme d'installation poursuit en anglais.



11 Entrez le mot de passe de l'administrateur de la base de données (dbauser).

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

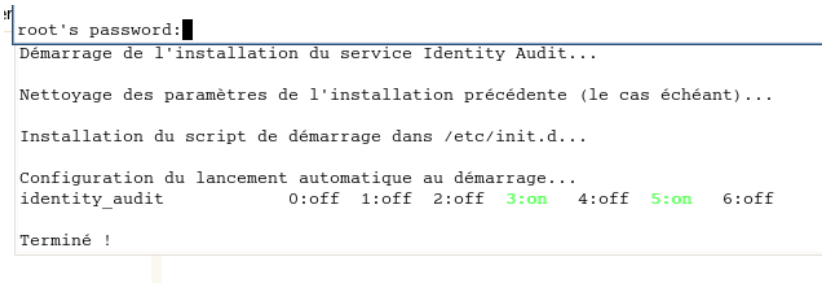
13 Entrez le mot de passe de l'utilisateur admin.

14 Confirmez le mot de passe de l'utilisateur admin.

15 Déloguez-vous, puis reloguez-vous en tant qu'utilisateur novell. Ceci permet de charger les modifications apportées à la variable d'environnement PATH par le script `install.sh`.

16 Exécutez le script `root_install_service.sh` pour permettre à Identity Audit de démarrer en tant que service. Cette étape nécessite un accès au niveau `root`. Exemples :

```
sudo /opt/novell/identity_audit_1.0_x86-64/setup/
root_install_service.sh
```



17 Saisissez le mot de passe `root`.

Identity Audit est configuré pour démarrer avec des niveaux d'exécution 3 et 5 (mode multi-utilisateur avec programme amorce dans la console ou mode X-Windows).

Une fois le service Identity Audit démarré, vous pouvez vous loguer à l'URL spécifiée dans le résultat de l'installation (https://hostIP:8443/novellidentityaudit). Le système commencera immédiatement à traiter les événements d'audit interne et sera entièrement opérationnel lorsque vous aurez configuré les sources d'événements pour l'envoi de données à Identity Audit.

3.2 Configuration des sources d'événements

Identity Audit 1.0 prend en charge la collecte des événements de journal provenant des applications qui étaient supportées par l'ancien produit Novell Audit et son agent de plate-forme. Avant d'effectuer la procédure de cette section, vérifiez que vos produits Novell sont pris en charge. Pour plus d'informations, reportez-vous à la Section 2.4, « Agent de plate-forme pris en charge », page 15.

- Section 3.2.1, « Installation de l'agent de plate-forme », page 21

- Section 3.2.2, « Configuration de l'agent de plate-forme », page 21
- Section 3.2.3, « Configuration du niveau d'audit », page 22

3.2.1 Installation de l'agent de plate-forme

L'agent de plate-forme doit au moins prendre en charge la version minimale recommandée pour Identity Audit. Pour plus d'informations, reportez-vous à la Section 2.4, « Agent de plate-forme pris en charge », page 15. L'agent de plate-forme approprié (32 ou 64 bits) doit être installé ou mis à jour sur toutes les machines de source d'événements. L'agent de plate-forme est inclus dans le téléchargement de Novell Audit à partir du site Web de téléchargement Novell (http://download.novell.com).

Pour installer ou mettre à niveau l'agent de plate-forme 32 bits :

1. Téléchargez lefichier `iso` pour Audit 2.0.2 FP6 ou version ultérieure dans le répertoire /tmp sur la machine de source d'événements.
2. Créez un répertoire pour Audit. Par exemple, `mkdir -p audit202fp6`
3. Loguez-vous en tant qu'utilisateur `root`.
4. Montez le fichier `.iso` de Audit.

   ```
   mount -o loop ./NAudit202.iso ./audit202fp6
   ```
5. Accédez au répertoire `audit202fp6`.
6. Accédez au répertoire approprié pour le système d'exploitation sur la source d'événements. Par exemple :

   ```
   cd Linux
   ```
7. Exécutez `pinstall.lin`.

   ```
   ./pinstall.lin
   ```
8. Lisez l'accord de licence et tapez `y` si vous en acceptez les termes.
9. Entrez la lettre `P` pour installer l'agent de plate-forme.
10. Saisissez la lettre `Y` pour conserver toutes les configurations précédentes dans le fichier `logevent.conf`.

    L'agent de plate-forme est installé.
11. Pour vérifier que la version de l'agent de plate-forme est correcte, entrez la commande suivante :

    ```
    rpm -qa | grep AUDT
    ```

    La version de l'agent de plate-forme novell-AUDT doit au moins être la version listée à la Section 2.4, « Agent de plate-forme pris en charge », page 15.

Pour installer ou mettre à niveau l'agent de plate-forme 64 bits, téléchargez NAudit 2.0.2 FP6 et suivez les instructions incluses dans le correctif.

3.2.2 Configuration de l'agent de plate-forme

Après l'installation, l'agent de plate-forme doit être configuré pour transmettre des données au serveur Identity Audit et, si vous le souhaitez, pour envoyer des signatures d'événement à partir des sources d'événements.

Avertissement : la configuration de l'agent de plate-forme pour la génération de signatures peut nuire aux performances des machines de source d'événements.

Pour configurer l'agent de plate-forme :

1. Loguez-vous à la machine de source d'événements.
2. Ouvrez le fichier `logevent` pour l'éditer. L'emplacement du fichier varie en fonction du système d'exploitation :
   - Linux : `/etc/logevent.conf`
   - Windows : `C:\WINDOWS\logevent.cfg`
   - NetWare : `SYS:\etc\logevent.cfg`
   - Solaris : `/etc/logevent.conf`
3. Définissez LogHost sur l'adresse IP du serveur Identity Audit.
4. Définissez LogEnginePort=1289. (Ajoutez cette entrée si elle n'existe pas encore.)
5. Entrez LogSigned=always si vous souhaitez que la source d'événements envoie des signatures d'événement.
6. Enregistrez le fichier.
7. Redémarrez l'agent de plate-forme. La méthode varie en fonction du système d'exploitation et de l'application. Redémarrez la machine ou reportez-vous à la documentation spécifique à l'application sur le site Web de documentation Novell (http://www.novell.com/documentation) pour obtenir des instructions.

3.2.3 Configuration du niveau d'audit

Les événements pour lesquels chaque application génère des enregistrements sont configurés différemment pour chaque application surveillée par Identity Audit. Les URL ci-dessous reprennent des informations supplémentaires sur chaque application.

- Access Manager (http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b8cvd2l.html#b8cvd2l)
- eDirectory (http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/b296n3h.html)
- Identity Manager (http://www.novell.com/documentation/idm36/idm_sentinel/data/bookinfo.html)
- NMAS (http://www.novell.com/documentation/nmas32/admin/index.html?page=/documentation/nmas32/admin/data/ahefojr.html)
- SecretStore (http://www.novell.com/documentation/secretstore33/index.html?page=/documentation/secretstore33/nssadm/data/bsqdjxv.htm)
- SecureLogin (http://www.novell.com/documentation/securelogin60/index.html (see the Auditing link))

3.3 Mise en route

L'administrateur créé pendant l'installation peut se loguer à l'application Identity Audit, créer d'autres utilisateurs, exécuter des rapports préchargés, télécharger de nouveaux rapports, effectuer des recherches d'événements, etc.

Pour vous loguer à Identity Audit :

1. Ouvrez un navigateur Web pris en charge. Pour plus d'informations, reportez-vous à la Section 2.3, « Navigateurs pris en charge », page 14.
2. Accédez à la page de login de Identity Audit (https://hostIP:8443/novellidentityaudit).
3. S'il s'agit de votre premier login à Identity Audit, un certificat s'affiche. Vous devez l'accepter pour pouvoir continuer.
4. Entrez `admin`.
5. Entrez le mot de passe admin configuré lors de l'installation.
6. Sélectionnez la langue de l'interface Identity Audit (anglais, portugais, français, italien, allemand, espagnol, japonais et chinois traditionnel ou simplifié).
7. Cliquez sur *Se connecter*.

3.4 Désinstallation

Pour nettoyer complètement une installation de Identity Audit, vous devez exécuter le script de désinstallation et effectuer ensuite quelques opérations manuelles de nettoyage.

1. Loguez-vous au serveur Identity Audit en tant qu'utilisateur `root`.
2. Arrêtez le service Identity Audit :
   ```
   /etc/init.d/identity_audit stop
   ```
3. Exécutez le script de désinstallation :
   ```
   /opt/novell/identity_audit_1.0_x86-64/setup/
   root_uninstall_service.sh
   ```
4. Supprimez le répertoire privé de Identity Audit et son contenu.
   ```
   rm -rf /opt/novell/identity_audit_1.0_x86-64
   ```
5. Les étapes finales sont différentes si vous souhaitez conserver des informations relatives à l'utilisateur et au groupe novell.
   - Si vous ne souhaitez pas conserver d'informations sur l'utilisateur novell, exécutez la commande suivante pour supprimer l'utilisateur, son répertoire privé et le groupe :
     ```
     userdel -r novell && groupdel novell
     ```
   - Si vous voulez garder l'utilisateur novell et son répertoire privé mais que vous souhaitez supprimer tous les paramètres Identity Audit, procédez comme suit :
     1. Supprimez les entrées de variable d'environnement Identity Audit suivantes du profil de l'utilisateur novell (dans `~novell/.bashrc`) :
        ```
        APP_HOME=/opt/novell/identity_audit_1.0_x86-64 export
        PATH=$APP_HOME/bin:$PATH
        ```
     2. Supprimez l'entrée dbauser du fichier PostgreSQL `~novell/.pgpass`.
        `*:*:*:dbauser:`*`mot de passe`*

Remarque : bien que le mot de passe dbauser soit affiché en texte clair, le contenu de ce fichier n'est accessible qu'aux utilisateurs novell et root qui disposent déjà d'un accès complet à toutes les fonctions sur le serveur Identity Audit.

Recherches

4

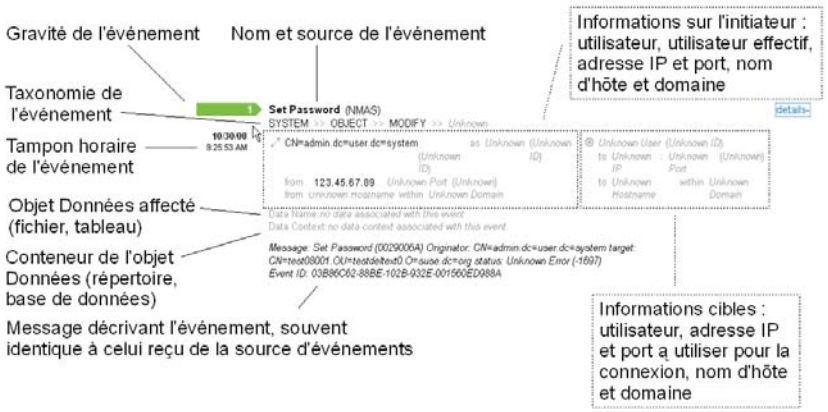
Cette section décrit les fonctions de recherche offertes par Novell® Identity Audit.

4.1 Présentation de la recherche d'événements

Novell Identity Audit permet d'effectuer des recherches sur les événements. Celles-ci portent sur toutes les données en ligne contenues dans la base de données, mais pas sur les événements internes générés par le système Identity Audit, à moins que l'utilisateur sélectionne l'option *Inclure les événements système*. Par défaut, les événements sont triés en fonction de l'algorithme de pertinence du moteur de recherche.

Les informations de base concernant un événement incluent le nom de l'événement, la source, l'heure, la gravité, des informations sur l'initiateur (représenté par une flèche) et des information sur la cible (représentée par des yeux de taureau).

Figure 4-1 *Champs d'événement*



4.2 Exécution d'une recherche d'événements

Les utilisateurs peuvent effectuer des recherches simples ou avancées.

4.2.1 Recherche simple

Une recherche simple porte sur tous les champs d'événement mentionnés dans le Tableau 4-1 page 30. À titre d'exemple, voici quelques recherches de base :

- `root`
- `127.0.0.1`
- `Lock*`
- `driverset0`

Remarque : si l'heure de la machine de l'utilisateur final n'est pas synchronisée avec celle du serveur Identity Audit (par exemple, une machine présente un retard de 25 minutes), votre recherche peut donner des résultats inattendus. Des recherches portant sur *La dernière heure* ou *Les dernières 24 heures* sont basées sur l'heure de la machine de l'utilisateur final.

---

1. Cliquez sur le lien *Rechercher* à gauche.

   Identity Audit est configuré pour exécuter une recherche par défaut des événements non système d'une gravité de 3 à 5 la première fois qu'un utilisateur clique sur le lien *Rechercher*. Dans les autres cas, la recherche porte par défaut sur la dernière entrée recherchée par l'utilisateur.

2. Pour effectuer une autre recherche, tapez un terme dans le champ prévu à cet effet (par exemple, `admin`). La recherche n'est pas sensible à la casse.
3. Sélectionnez une période de temps sur laquelle doit porter la recherche. La plupart des paramètres de temps sont explicites ; la valeur par défaut est *les 30 derniers jours*.
   - *Personnalisé* permet de sélectionner les dates et heures de début et de fin de la période pour la recherche. La date de début doit être antérieure à la date de fin et l'heure est basée sur l'heure locale du serveur Identity Audit.
   - *Tout* applique la recherche à toutes les données contenues dans la base de données.
4. Sélectionnez *Inclure les événements système* si vous souhaitez inclure les événements générés par les opérations système de Identity Audit.
5. Sélectionnez *Trier par date/heure* pour classer les données dans l'ordre chronologique.

Remarque : le tri chronologique prend plus de temps que le tri par pertinence (option par défaut).

6 Cliquez sur *Rechercher*.

Le texte spécifié est recherché dans tous les champs de l'index. Une icône animée indique que la recherche est en cours.

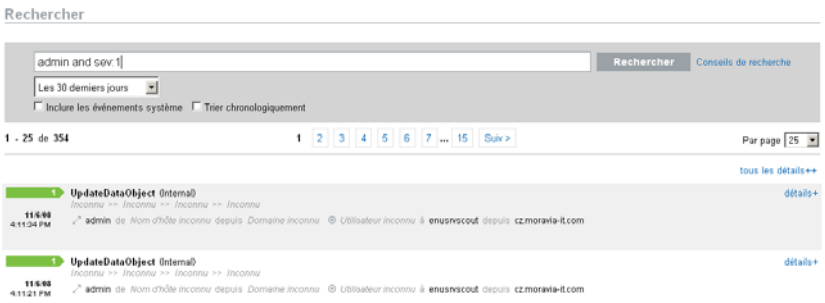
Les récapitulatifs d'événements apparaissent.

4.2.2 Recherche avancée

Une recherche avancée permet de rechercher une valeur dans un ou plusieurs champs d'événement spécifiques. Les critères des recherches avancées se basent sur les noms abrégés de chaque champ d'événement et sur la logique de recherche de l'index. Le tableau suivant décrit les champs, indique les noms abrégés pour les recherches avancées et spécifie si les champs sont visibles dans les vues détaillées et de base des événements.

Pour rechercher une valeur dans un champ spécifique, utilisez le nom abrégé du champ (pour plus d'informations, reportez-vous au Tableau 4-1 page 30), deux-points et la valeur. Par exemple, pour rechercher une tentative d'authentification de user2 auprès de Identity Audit, entrez le texte suivant dans le champ de recherche :

- `evt:authentication AND sun:user2`
- `pn:NMAS AND sev:5`
- `sip:123.45.67.89 AND evt:“Set Password”`



Il est ainsi possible de combiner plusieurs critères de recherche avancés à l'aide des opérateurs booléens suivants :

- AND (obligatoirement en majuscules)
- OR (obligatoirement en majuscules)
- NOT (obligatoirement en majuscules ; ne peut pas être le seul critère de recherche)
- +
- -

Les caractères spéciaux doivent être échappés à l'aide du symbole \ :

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
```

Les critères de recherche avancée suivent le modèle des critères de recherche du paquetage Open Source Apache Lucene. Pour plus d'informations sur les critères de recherche, consultez le site Web Lucene Query Parser Syntax (http://lucene.apache.org/java/2_3_2/queryparsersyntax.html).

4.3 Affichage des résultats des recherches

Les recherches renvoient des séries d'événements. Les utilisateurs peuvent choisir d'afficher une vue de base ou détaillée des informations d'événements et peuvent configurer le nombre de résultats par page. Les résultats des recherches sont renvoyés par lots. La taille de lot par défaut est de 25 résultats, mais il est aisé de configurer une autre valeur.

- Section 4.3.1, « Vue de base des événements », page 28
- Section 4.3.2, « Vue détaillée des événements », page 29
- Section 4.3.3, « Affinement des résultats des recherches », page 29

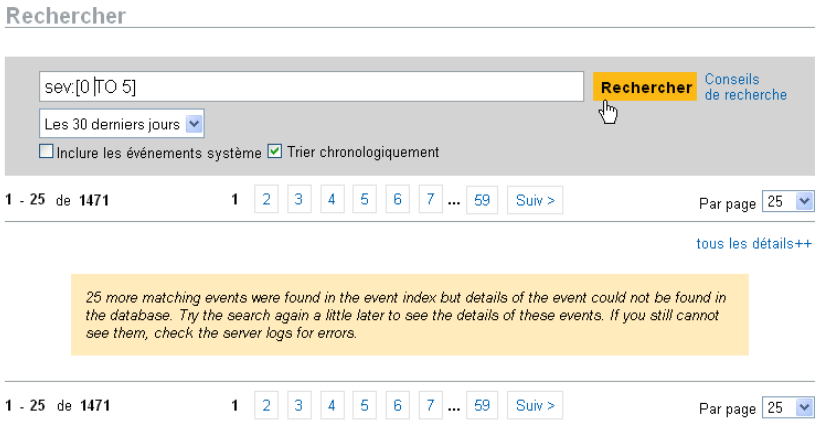
4.3.1 Vue de base des événements

Les informations pour chaque événement sont regroupées en données relatives à l'initiateur, d'une part, et à la cible, d'autre part. Si des informations ne sont pas disponibles pour un champ d'événement spécifique, celui-ci est marqué comme *Inconnu*.

Figure 4-2 *Vue de base des événements*

Il arrive parfois que le moteur de recherche indexe les événements plus vite que ce qu'ils ne sont insérés dans la base de données. Si un utilisateur exécute une recherche qui renvoie des événements qui n'ont pas été insérés dans la base de données, l'utilisateur reçoit un message indiquant qu'un certain nombre d'événements correspondent à la requête mais sont introuvables dans la base de données. Il suffit généralement de réexécuter la recherche plus tard pour que les événements figurent dans la base de données et que la recherche aboutisse.

Figure 4-3 *Événements indexés ne figurant pas encore dans la base de données*



4.3.2 Vue détaillée des événements

Les utilisateurs peuvent afficher davantage d'informations sur les événements en cliquant sur le lien *détails* à droite de la page. Les détails de tous les événements sur une page peuvent ainsi être développés ou réduits à l'aide du lien tous les détails++ ou *tous les détails*--. Cette préférence est conservée lorsque vous parcourez plusieurs pages ou résultats, de même que lorsque vous exécutez de nouvelles recherches.

Figure 4-4 *Vue détaillée des événements*

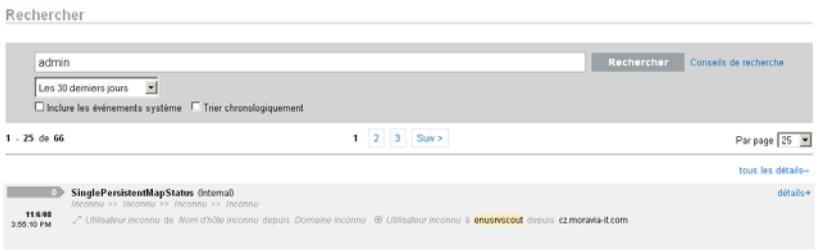
L'événement ci-dessus est identique à celui de la Figure 4-2 page 28 mais présente une vue détaillée qui affiche les champs de données supplémentaires qui ont peut-être été complétés.

4.3.3 Affinement des résultats des recherches

Une fois les résultats d'une recherche affichés, il peut être utile de les affiner en ajoutant des critères de recherche supplémentaires. Par exemple, vous pouvez voir le nom d'un même initiateur plusieurs fois dans les résultats et souhaiter consulter davantage d'événements initiés par cet utilisateur.

Pour filtrer les résultats selon une valeur spécifique reprise dans les résultats de la recherche :

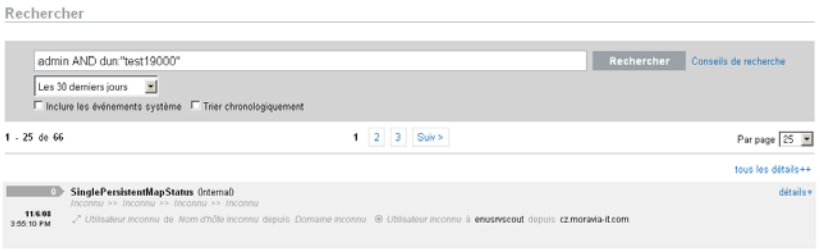
1. Identifiez dans les résultats de la recherche le critère souhaité pour le filtre.
2. Cliquez sur la valeur (par exemple, nom d'hôte cible test1900) selon laquelle vous souhaitez filtrer les résultats.



Suggestion : cette opération ajoute la valeur à votre filtre avec un opérateur AND. Pour ajouter la valeur à votre filtre avec un opérateur NOT, appuyez simultanément sur la touche Alt lorsque vous cliquez sur la valeur.

---

3. Cliquez sur *Rechercher*.



Toutefois, cette méthode d'affinement de la recherche ne fonctionne pas avec certains champs :

- EventTime
- Message
- Tous les champs liés au préparateur d'état
- Tous les champs liés à l'observateur
- Tous les champs ayant une valeur `Unknown`

4.4 Champs d'événement

Chaque événement comporte des champs qui peuvent être complétées le cas échéant, en fonction de l'événement spécifique. Les valeurs de ces champs d'événement peuvent être consultées en effectuant une recherche ou en exécutant un rapport. Chaque champ possède un nom abrégé utilisé dans les recherches avancées. Les valeurs de la plupart de ces champs sont visibles dans la vue détaillée des événements ; d'autres valeurs peuvent aussi être consultées dans la vue de base des événements.

Tableau 4-1 *Champs d'événement*

Champ	Nom abrégé	Description	Visible dans la vue de base	Visible dans la vue détaillée
Severity	sev	Gravité de l'événement sur une échelle allant de 0 (informatif) à 5 (critique).	X	X
EventTime	dt	Tampon horaire de l'événement. Il peut s'agir du tampon horaire du serveur Identity Audit ou de celui de la source d'événements d'origine (si l'option d'approbation de l'heure de l'événement est activée).	X	X
EventName	evt	Nom abrégé de l'événement.	X	X
Message	msg	Message détaillé de l'événement.		X
ProductName	pn	Produit ayant généré l'événement, autrement dit la source de l'événement. S'affiche derrière le nom de l'événement.	X	X
InitUserName	sun	Nom de l'utilisateur à l'origine de l'événement.	X	X

Champ	Nom abrégé	Description	Visible dans la vue de base	Visible dans la vue détaillée
InitUserID	iuid	ID de l'utilisateur à l'origine de l'événement.		X
InitUserDomain	rv35	Domaine de l'utilisateur à l'origine de l'événement. Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		
InitHostName	shn	Nom d'hôte de la machine à l'origine de l'événement.	X	X
InitHostDomain	rv42	Domaine de la machine à l'origine de l'événement.	X	X
InitIP	sip	Adresse IP de la machine à l'origine de l'événement.		X
InitServicePort	spint	Numéro du port à l'origine de l'événement (80, par exemple).		X
InitServicePortName	sp	Type du port à l'origine de l'événement (HTTP, par exemple).		X
TargetUserName	dun	Nom de l'utilisateur auquel était destiné l'événement.	X	X
TargetUserID	tuid	ID de l'utilisateur auquel était destiné l'événement.		X
TargetUserDomain	rv35	Domaine de l'utilisateur auquel était destiné l'événement. Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		X
TargetHostName	dhn	Nom d'hôte de la machine à laquelle était destiné l'événement.	X	X
TargetHostDomain	rv45	Domaine de la machine à laquelle était destiné l'événement.	X	X
TargetIP	dip	Adresse IP de la machine à laquelle était destiné l'événement.		X
TargetServicePort	dpint	Numéro du port auquel était destiné l'événement (80, par exemple).		X
TargetServicePortName	dp	Type du port auquel était destiné l'événement (HTTP, par exemple).		X
TargetTrustName	ttn	Rôle de l'utilisateur auquel était destiné l'événement (AdminFinance, par exemple). Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		

Champ	Nom abrégé	Description	Visible dans la vue de base	Visible dans la vue détaillée
TargetTrustID	ttid	ID numérique représentant le rôle de l'utilisateur auquel était destiné l'événement. Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		
TargetTrustDomain	ttd	Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		
EffectiveUserName	euname	Nom de l'utilisateur dont l'InitUser emprunte la personnalité (`root` utilisant `su`, par exemple) ; il vient après le *nom d'utilisateur de l'initiateur (ID utilisateur de l'initiateur*) *comme* dans la vue détaillée des événements.		X
EffectiveUserID	euid	ID numérique de l'utilisateur dont l'InitUser emprunte la personnalité (`root` utilisant `su`, par exemple).		X
ObserverHostName	sn	Nom d'hôte de la machine qui a transféré l'événement au système de gestion des événements d'information sur la sécurité (nom d'hôte d'un serveur syslog, par exemple). Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		
ObserverHostDomain	obsdom	Domaine de la machine qui a transféré l'événement au système de gestion des événements d'information sur la sécurité (domaine d'un serveur syslog, par exemple). Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		
ObserverIP	obsip	Adresse IP de la machine qui a transféré l'événement au système de gestion des événements d'information sur la sécurité (adresse IP d'un serveur syslog, par exemple). Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		

Champ	Nom abrégé	Description	Visible dans la vue de base	Visible dans la vue détaillée
ReporterHostName	rn	Nom d'hôte de la machine qui a signalé l'événement à un observateur. Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		
ReporterHostDomain	repdom	Domaine de la machine qui a signalé l'événement à un observateur. Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		
ReporterIP	repip	Adresse IP de la machine qui a signalé l'événement à un observateur. Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		
SensorType	st	Indicateur de caractère unique pour le type de capteur (N=réseau, H=hôte, O=système d'exploitation, A et I=événements d'audit Identity Audit, P=événements de performances Identity Audit). Peut faire l'objet d'une recherche bien qu'il n'apparaisse dans aucune des vues d'événement.		
DataName	fr	Nom de l'objet de données signalé dans l'événement (nom de fichier ou de table de base de données, par exemple).		X
DataContext	rv36	Conteneur de l'objet de données FileName (par exemple, un répertoire pour un fichier ou une instance de base de données pour une table de base de données)		X
TaxonomyLevel1	rv50	Classification de l'événement selon la cible. Apparaît sous le nom de l'événement au format suivant : TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel2	rv51	Classification de l'événement selon la cible secondaire. Apparaît sous le nom de l'événement au format suivant : TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

Champ	Nom abrégé	Description	Visible dans la vue de base	Visible dans la vue détaillée
TaxonomyLevel3	rv52	Informations sur l'opération associée à l'événement. Apparaît sous le nom de l'événement au format suivant : TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel4	rv53	Informations sur les détails associés à l'événement. Apparaît sous le nom de l'événement au format suivant : TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

Certains champs sont indexés. L'indexation des champs permet de rechercher un mot isolé dans un champ sans caractère joker. Les champs sont indexés sur la base des espaces et autres caractères spéciaux. Pour ces champs, les articles tels que « un », « une », « le », etc. sont supprimés de l'index de recherche.

- EventName
- Message
- ProductName
- FileName
- DataContext
- TaxonomyLevel1
- TaxonomyLevel2
- TaxonomyLevel3
- TaxonomyLevel4

Création de rapports

5

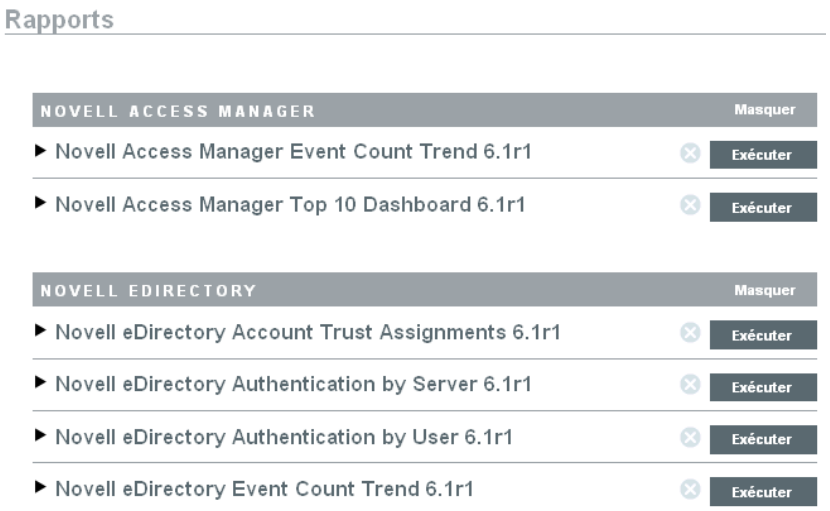
Ce chapitre explique comme exécuter, consulter et gérer des rapports dans Novell® Identity Audit.

5.1 Présentation

Identity Audit est installé avec un jeu de modèles de rapport liés aux applications Novell. Tous les utilisateurs Identity Audit peuvent exécuter un rapport en utilisant les paramètres qu'ils souhaitent (tels que les dates de début et de fin) et en enregistrer les résultats sous le nom de leur choix. Une fois le rapport exécuté, les résultats peuvent être récupérés par tout utilisateur Identity Audit et affichés sous la forme d'un fichier PDF.

Les rapports sont organisés par catégorie. L'installation de Identity Audit comporte des rapports pour chaque source d'événements prise en charge.

Figure 5-1 *Rapports organisés par catégorie*



5.2 Exécution de rapports

L'installation de Identity Audit comprend un ensemble de rapports organisés en plusieurs catégories de produits. Les utilisateurs peuvent poursuivre leurs activités dans l'application pendant l'exécution des rapports étant donné qu'elle s'effectue de manière asynchrone. Une fois les rapports terminés, leurs résultats peuvent être consultés au format PDF par n'importe quel utilisateur.

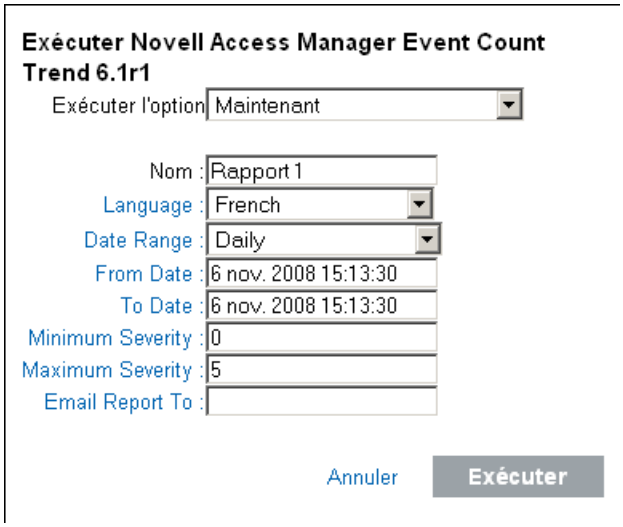
De nombreuses définitions de rapport incluent des paramètres que l'utilisateur est invité à définir avant d'exécuter les rapports. En fonction de la méthode utilisée par le développeur pour le concevoir, les paramètres du rapport peuvent être du texte, des nombres, des valeurs booléennes ou des dates. Un paramètre peut être une valeur par défaut ou une valeur à choisir parmi une liste dans la base de données Identity Audit.

Pour exécuter un rapport :

1 Dans Identity Audit, cliquez sur *Rapports* pour afficher les rapports disponibles.

Au besoin, cliquez sur une définition de rapport pour la développer. Si vous voyez *Exemple de rapport*, vous pouvez cliquer sur *Afficher* pour voir un rapport complété avec un ensemble de données fournies en guise de modèle.

2 Sélectionnez le rapport à exécuter, puis cliquez sur *Exécuter*.



3 Définissez le planning d'exécution du rapport. Si le rapport doit être exécuté plus tard, vous devez entrer l'heure de début.

- Maintenant : il s'agit de la valeur par défaut. Le rapport s'exécute immédiatement.

- Une fois : ce paramètre exécute le rapport une seule fois à l'heure et à la date spécifiées.
- Chaque jour : ce paramètre exécute le rapport une fois par jour à l'heure spécifiée.
- Chaque semaine : ce paramètre exécute le rapport chaque fois le même jour de la semaine à l'heure spécifiée.
- Chaque mois : ce paramètre exécute le rapport chaque mois le même jour, à la date et à l'heure spécifiées. Par exemple, si la date de début est le 28 octobre à 14h00, le rapport s'exécute le 28e jour de chaque mois à 14h00.

Remarque : tous les paramètres horaires sont basés sur l'heure locale du navigateur.

---

4. Entrez un nom qui permet d'identifier les résultats de rapport.

   Étant donné que le nom d'utilisateur et l'heure sont également utilisés pour identifier les résultats du rapport, le nom de ce dernier ne doit pas nécessairement être unique.

5. Sélectionnez la langue d'affichage du rapport (anglais, français, allemand, italien, japonais, chinois traditionnel, chinois simplifié, espagnol ou portugais).

6. Sélectionnez le type de rapport. Toutes les durées sont basées sur l'heure locale du navigateur.
   - Par jour : le rapport affiche les événements du jour (de minuit à 23h59). S'il est 8h00, le rapport affiche 8 heures de données.
   - Par semaine : le rapport affiche les événements de la semaine (de dimanche minuit jusqu'à la fi du jour en cours).
   - Par mois : le rapport affiche les événements du mois (à partir du premier jour du mois à minuit jusqu'à la fin du jour en cours).
   - Plage de dates personnalisée : pour ce paramètre uniquement, vous devez également définir une date de début et de fin ci-dessous.
   - Jour précédent : le rapport affiche les événements de la veille (de minuit à 23h59).

7. Si vous avez sélectionné Plage de dates personnalisée, définissez la date de début (De) et la date de fin (À) pour le rapport.

   Remarque : si le type de rapport sélectionné est Par jour, Par semaine, Par mois ou Jour précédent, ces paramètres horaires sont ignorés.

   ---

8. Définissez les événements de gravité minimale à inclure dans le rapport.

9. Définissez les événements de gravité maximale à inclure dans le rapport.

10. Si le rapport doit être envoyé par courrier électronique à un ou plusieurs utilisateurs, entrez leurs adresses en les séparant par des virgules.

    Remarque : pour activer les rapports d'expédition, l'administrateur doit configurer le relais de messagerie sous *Règles>Configuration*.

    ---

11. Cliquez sur *Exécuter*.

    Une entrée de résultats de rapport est créée et envoyée par courrier électronique aux destinataires désignés.

5.3 Affichage des rapports

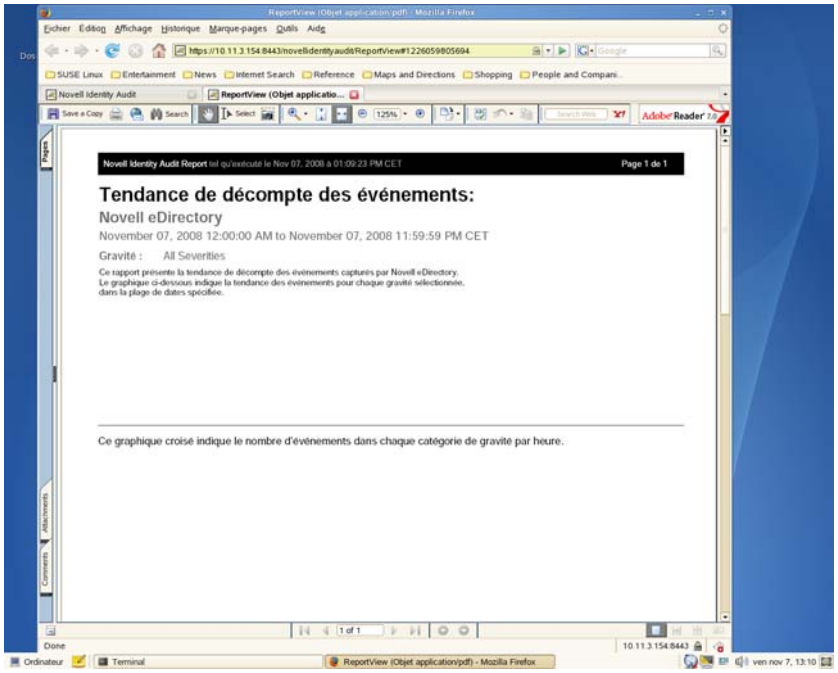
Les utilisateurs Identity Audit peuvent afficher des rapports dans l'application Identity Audit. Les autres utilisateurs peuvent recevoir les fichiers de rapportau format PDF par courrier électronique.

1 Pour afficher la liste des résultats de rapport, cliquez sur *Afficher*. Tous les rapports exécutés précédemment s'affichent avec le nom de rapport défini par l'utilisateur, le nom de l'utilisateur qui les a exécutés et l'heure de leur exécution.

2 Cliquez sur *afficher les paramètres* pour consulter les valeurs exactes utilisées pour l'exécution du rapport.

- Pour le type de rapport, D=Par jour, W=Par semaine, M=Par mois, DR=Plage de dates personnalisée et PD=Jour précédent.
- Pour la langue, en=anglais, fr=français, de=allemand, it=italien, ja=japonais, pt=portugais brésilien, es=espagnol, zh=chinois simplifié et zh_TW=chinois traditionnel.

3 Cliquez sur *Afficher* pour les résultats de rapport que vous souhaitez consulter. Les résultats de rapport s'affichent dans une nouvelle fenêtre auformat PDF.



Suggestion : les résultats de rapport sont présentés du plus récent au plus ancien.

5.4 Gestion des rapports

Les utilisateurs Identity Audit peuvent ajouter, supprimer, mettre à jour et planifier des rapports.

5.4.1 Ajout de rapports

Identity Audit contient des rapports préchargés, mais de nouveaux plug-ins de rapport (des fichiers`ZIP` spéciaux qui incluent la définition d'un rapport ainsi que des métadonnées) peuvent être téléchargés dans Identity Audit. Si le système ne contient aucun rapport, l'écran suivant s'affiche :

Figure 5-2 *Aucun rapport chargé*

Pour ajouter un rapport :

1 Cliquez sur le bouton *Rapports* à gauche de l'écran.

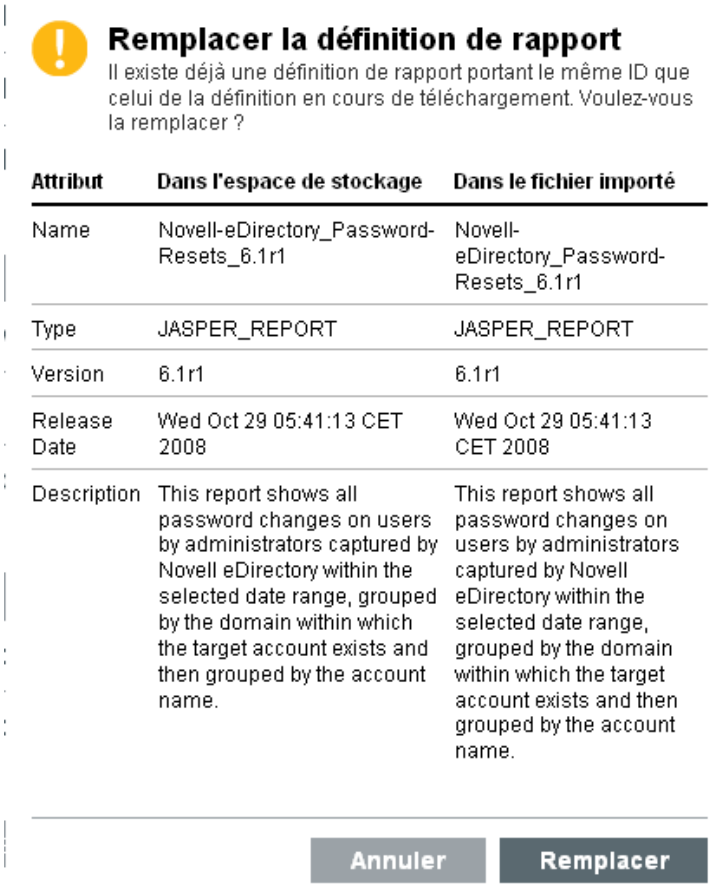
2 Cliquez sur le bouton *Télécharger le rapport*.

3 Recherchez l'emplacement du fichier `ZIP` de plug-in de rapport sur votre machine locale.

4 Cliquez sur *Ouvrir*.

5 Cliquez sur *Enregistrer*.

6 Si ce rapport existe déjà dans l'espace de stockage de rapports (d'après l'ID unique du rapport), Identity Audit affiche les détails des deux rapports, celui existant dans le système et celui importé. L'utilisateur peut décider s'il souhaite remplacer le rapport existant. Dans l'exemple suivant, la version du rapport importé est identique à celle du rapport existant.



7 La nouvelle définition de rapport est ajoutée à la liste dans l'ordre alphabétique et peut être exécutée immédiatement, le cas échéant.

Téléchargement de nouveaux rapports ou de mises à jour

Des rapports Novell, nouveaux ou mis à jour, peuvent être téléchargés à partir du site Web de Novell (http://support.novell.com/products/identityaudit/identityaudit10.html).

Création de rapports

Les utilisateurs peuvent rédiger ou modifier des rapports à l'aide de JasperForge* iReport, un concepteur de rapports graphiques pour JasperReports. iReport est un outil de développement de rapport libre qui peut être téléchargé sur le site JasperForge.org (http://jasperforge.org/plugins/project/project_home.php?group_id=83) (à compter de la publication du présent document).

Qu'ils soient nouveaux ou modifiés, les rapports peuvent inclure des champs de base de données supplémentaires qui ne figurent pas dans l'interface Web de Identity Audit. Ils doivent répondre aux exigences de fichiers et de format des plug-ins de rapport. Pour plus d'informations sur les champs de base de données et les exigences en matière de format et de fichier pour les plug-ins de rapport, reportez-vous au Sentinel SDK Web site (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) (site Web du SDK de Sentinel).

5.4.2 Assignation d'un nouveau nom à des résultats de rapport

Au contraire des définitions de rapport, les résultats de rapport peuvent être renommés dans l'interface Identity Audit.

1. Cliquez sur le bouton *Rapports* à gauche de l'écran.
2. Cliquez sur un nom de rapport pour le développer.
3. Cliquez sur le nom des résultats de rapport que vous souhaitez renommer.
4. Entrez le nouveau nom.
5. Cliquez sur *Renommer*.

5.4.3 Suppression de rapports

Les utilisateurs peuvent supprimer une définition ou un jeu de résultats de rapport. En cas de suppression d'une définition de rapport, tous les résultats associés à ce dernier sont également supprimés.

Si un rapport en cours est supprimé, la requête sur la base de données est annulée.

5.4.4 Mise à jour des définitions de rapport

Les utilisateurs peuvent télécharger des rapports mis à jour vers Identity Audit pour remplacer un rapport existant. Pour plus d'informations, reportez-vous à la Section 5.4.1, « Ajout de rapports », page 39.

Collecte des données

6

Les administrateurs peuvent configurer et surveiller la collecte des données pour Novell® Identity Audit. L'installation de Identity Audit permet de collecter des données provenant de diverses applications Novell à l'aide de l'agent de plate-forme Novell Audit. Pour plus d'informations sur les versions de l'agent de plate-forme qui sont prises en charge, reportez-vous à la Section 2.4, « Agent de plate-forme pris en charge », page 15.

6.1 Configuration des sources d'événements

Bien que Identity Audit soit préconfiguré pour accepter des données de plusieurs applications Novell, les serveurs d'applications proprement dits (sources d'événements) doivent être configurés pour envoyer des données au serveur Identity Audit. Cette opération fait partie de la configuration de base de Identity Audit. Pour plus d'informations, reportez-vous à la Section 3.2, « Configuration des sources d'événements », page 20.

6.2 État de la collecte des données

Les administrateurs peuvent activer ou désactiver la collecte de données globalement ou par application. Ils peuvent également afficher les informations d'état de santé de chaque application.

1. Loguez-vous à Identity Audit en tant qu'administrateur.
2. Cliquez sur .*Collecte* dans le coin supérieur droit de la page.

3 Activez ou désactivez la collecte de données globale par le biais du serveur d'audit.

4 Activez ou désactivez la collecte de données pour chaque application à partir des sources d'événements.

5 Cliquez sur *Afficher les détails* pour afficher plus d'informations sur les connexions actives pour chaque application.

Les modifications apportées à cette page prennent effet immédiatement.

- Section 6.2.1, « Serveur d'audit », page 44
- Section 6.2.2, « Sources d'événements », page 45

6.2.1 Serveur d'audit

Dans la section *Serveur d'audit*, les administrateurs peuvent activer ou désactiver la collecte de données globalement à l'aide des options Actif et Inactif. L'état de santé du serveur d'audit s'affiche également.

Bon état : un indicateur vert signifie que le serveur d'audit est en bon état (il est activé, écoute sur un port et ne comporte aucune erreur non résolue).

Erreur : un indicateur rouge signifie que le serveur d'audit a rencontré une erreur. Pour plus d'informations, reportez-vous aux fichiers `.server0.*.log`.

Hors ligne : un indicateur gris signifie que le serveur d'audit a été mis hors ligne par un administrateur.

6.2.2 Sources d'événements

Dans la section *Sources d'événements*, les administrateurs peuvent activer la collecte de données au niveau de l'application. Ces paramètres peuvent affecter la collecte de données pour plusieurs serveurs (par exemple, plusieurs instances eDirectory).

Remarque : ces paramètres activent (ou désactivent) la collecte de données Identity Audit des applications listées. Ils ne démarrent ou n'arrêtent pas pour autant les services sur les machines de source d'événements.

Pour chaque icône, l'état de santé est indiqué par une icône rouge, jaune, verte ou noire. Pour la plupart des états, vous pouvez afficher un complément d'informations en cliquant sur *afficher les détails*.

Bon état : un indicateur vert signifie que la source d'événements est en bonne santé et que Identity Audit a bien reçu les données qu'elle a envoyé.

Avertissement : un indicateur jaune signale un avertissement. Cela arrive souvent lorsque l'application est activée dans Identity Audit, mais n'a pas encore envoyé de données. Ce peut être le cas, par exemple, si l'agent de plate-forme sur la source d'événements n'est pas configuré correctement pour envoyer des données à Identity Audit ou si la consignation d'événements n'est pas activée pour l'application. Cliquez sur *Afficher les détails* pour plus d'informations.

Erreur : un indicateur rouge signifie que le serveur Identity Audit signale une erreur de connexion à cette application ou de réception des données provenant de cette dernière. Cliquez sur *Afficher les détails* pour plus d'informations.

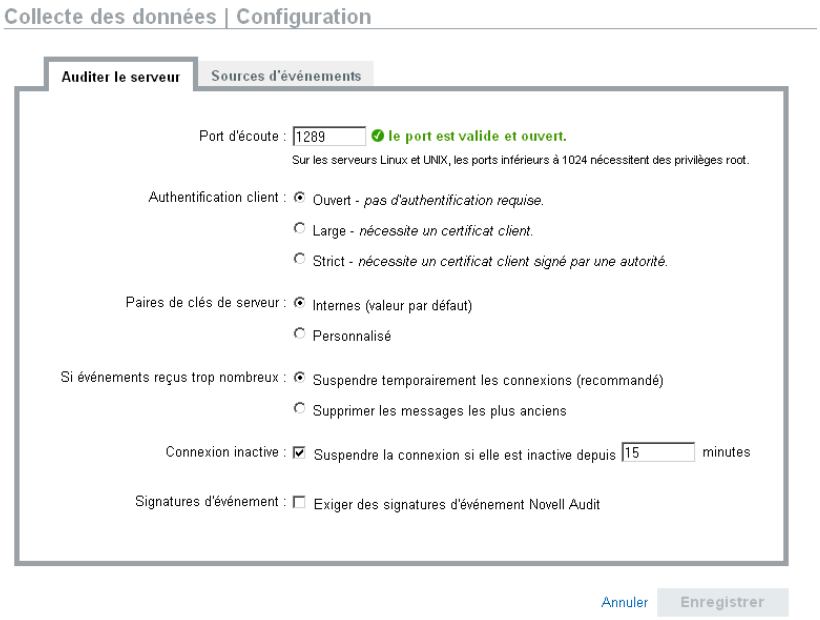
Hors ligne : un indicateur gris signifie que la source d'événements a été désactivée. Identity Audit ne traite aucune donnée en provenance de cette dernière.

Pour chaque source de données en ligne, Identity Audit affiche le taux d'événements calculé pour les événements entrants. Le taux d'événements est recalculé toutes les 60 secondes.

6.3 Options du serveur d'audit

Les administrateurs peuvent modifier certains paramètres relatifs à la manière dont Identity Audit écoute les données provenant des applications de source d'événements, y compris le port sur lequel Identity Audit écoute et le type d'authentification entre la source d'événements et Identity Audit.

1. Loguez-vous à Identity Audit en tant qu'administrateur.
2. Cliquez sur le lien *Collection* en haut de l'écran.
3. Cliquez sur le lien *Configuration* à droite de l'écran.
4. Assurez-vous que l'onglet *Serveur d'audit* est sélectionné.



5 Entrez le numéro de port sur lequel le serveur Identity Audit écoute les messages provenant des sources d'événement. Pour plus d'informations, reportez-vous à la Section 6.3.1, « Configuration et réacheminement de port », page 47.

6 Définissez les paramètres des paires de clés du serveur et d'authentification client appropriés . Pour plus d'informations, reportez-vous à la Section 6.3.2, « Authentification client », page 47.

7 Choisissez le comportement que le serveur Identity Audit doit adopter lorsque le tampon absorbe trop d'événéments.

Suspendre temporairement les connexions : ce paramètre coupe les connexions existantes et renonce à en accepter de nouvelles jusqu'à ce que le tampon dispose d'espace pour les nouveaux messages. En attendant, les messages sont mis en cache par les sources d'événements.

Supprimer les messages les plus anciens : ce paramètre supprime les messages plus anciens pour pouvoir en accepter de nouveaux.

Avertissement : aucune méthode ne permet de récupérer les messages supprimés si vous avez sélectionné *Supprimer les messagesles plus anciens*.

---

8 Sélectionnez *Connexion inactive* pour déconnecter les sources d'événements qui n'ont pas envoyé de données depuis un certain temps.

Les connexions des sources d'événements sont automatiquement restaurées lorsqu'elles recommencent à envoyer des données.

9 Entrez le nombre de minutes devant s'écouler avant de déconnecter une connexion inactive.

10 Sélectionnez *Signatures d'événement* pour recevoir une signature avec l'événement.

Remarque : pour recevoir une signature, l'agent de plate-forme sur la source d'événements doit être configuré correctement. Pour plus d'informations, reportez-vous au Section 6.1, « Configuration des sources d'événements », page 43. .

---

11 Cliquez sur *Enregistrer*.

6.3.1 Configuration et réacheminement de port

Le port par défaut sur lequel Identity Audit écoute les messages provenant des agents de plate-forme est le port 1289. Une fois le port défini, le système vérifie s'il est valide et ouvert.

Vous devez disposer de privilèges root pour effectuer des liaisons aux ports inférieurs à 1024. Novell vous recommande plutôt d'utiliser un port supérieur à 1024. Vous pouvez modifier les périphériques sources pour effectuer les envois vers un port supérieur ou utiliser le réacheminement de port sur le serveur Identity Audit.

Pour modifier la source d'événements afin qu'elle achemine les envois vers un autre port :

1. Loguez-vous à la machine de source d'événements.
2. Ouvrez le fichier `logevent` pour l'éditer. L'emplacement du fichier varie en fonction du système d'exploitation :
   - Linux : `/etc/logevent.conf`
   - Windows : `C:\WINDOWS\logevent.cfg`
   - NetWare : `SYS:\etc\logevent.cfg`
   - Solaris : `/etc/logevent.conf`
3. Définissez le paramètre LogEnginePort sur le port désiré.
4. Enregistrez le fichier.
5. Redémarrez l'agent de plate-forme. La méthode varie en fonction du système d'exploitation et de l'application. Redémarrez la machine ou reportez-vous à la documentation spécifique à l'application sur le site Web de documentation Novell (http://www.novell.com/documentation) pour obtenir des instructions.

Pour configurer le réacheminement de port sur le serveur Identity Audit :

1. Loguez-vous au système d'exploitation du serveur Identity Audit en tant qu'utilisateur `root` (ou en tant que `tel` en utilisant la commande `su`).
2. Ouvrez le fichier `/etc/init.d/boot.local` afin de l'éditer.
3. Ajoutez la commande suivante vers la fin du processus amorce :

   `iptables -A PREROUTING -t nat -p` *`protocol`* `--dport` *`incoming port`* `-j DNAT --to-destination` *`IP:rerouted port`*

   à l'endroit où *protocol* est tcp ou udp, *incoming port* est le port sur lequel les messages arrivent et *IP:rerouted port* est l'adresse IP de la machine locale accompagné d'un numéro de port disponible supérieur à 1024
4. Enregistrez les modifications apportées.
5. Redémarrer. Si vous ne parvenez pas redémarrer immédiatement, exécutez la commande `iptables` ci-dessus à partir d'une ligne de commande.

6.3.2 Authentification client

Les sources d'événement envoient leurs données via une connexion SSL et le paramètre *Authentification client* pour le serveur Identity Audit détermine quel type d'authentification est effectué pour les certificats provenant des agents de plate-forme sur les sources d'événement.

Ouvert : aucune authentification n'est requise. Identity Audit ne demande, n'exige ni ne valide aucun certificat de la source d'événements.

Large : la source d'événements doit fournir un certificat X.509 valide, mais celui-ci n'est pas validé. Il ne doit pas être signé par une autorité de certification.

Strict : la source d'événements doit fournir un certificat X.509 valide, lequel doit être signé par une autorité de certification approuvée. Si la source d'événements ne présente aucun certificat valide, Identity Audit n'accepte pas ses données d'événement.

- « Création d'un fichier Truststore » page 48
- « Importation d'un fichier Truststore » page 48
- « Paire de clés de serveur » page 49

Création d'un fichier Truststore

Dans le cadre d'une authentification stricte, vous devez disposer d'un fichier Truststore qui contient le certificat de la source d'événements ou celui de l'autorité de certification (CA) qui a signé le certificat de la source d'événements. Une fois en possession d'un certificat DER- ou PEM-, vous pouvez créer le fichier Truststore à l'aide de l'utilitaire CreateTruststore livré avec Identity Audit.

1. Loguez-vous au serveur Identity Audit avec l'identité novell.
2. Allez à l'emplacement `/opt/novell/identity_audit_1.0_x86/data/updates/done`.
3. Dézippez le fichier `audit_connector.zip`.

   ```
   unzip audit_connector.zip
   ```
4. Copiez le fichier `TruststoreCreator.sh` ou `TruststoreCreator.bat` sur la machine contenant les certificats ou copiez ces derniers sur la machine qui héberge l'utilitaire TruststoreCreator.
5. Exécutez l'utilitaire `TruststoreCreator.sh`.

   ```
   TruststoreCreator.sh -keystore /tmp/my.keystore -password password1 -certs /tmp/cert1.pem,/tmp/cert2.pem
   ```

   Dans cet exemple, l'utilitaire TruststoreCreator crée un fichier Keystore, `my.keystore`, qui contient deux certificats (`cert1.pem` et `cert2.pem`). Il est protégé par le mot de passe *password1*.

Importation d'un fichier Truststore

Dans le cadre d'une authentification stricte, l'administrateur peut importer un fichier Truststore à l'aide du bouton *Importer*. Cela permet de garantir que seules les sources d'événements autorisées envoient des données à Identity Audit. Le fichier Truststore doit inclure le certificat de la source d'événements ou celui de l'autorité de certification qui l'a signé.

La procédure suivante doit être exécutée sur la machine qui contient le fichier Truststore. Vous pouvez ouvrir un navigateur Web sur la machine qui contient le fichier Truststore ou le déplacer sur une machine équipée d'un navigateur Web.

Pour importer un fichier Truststore :

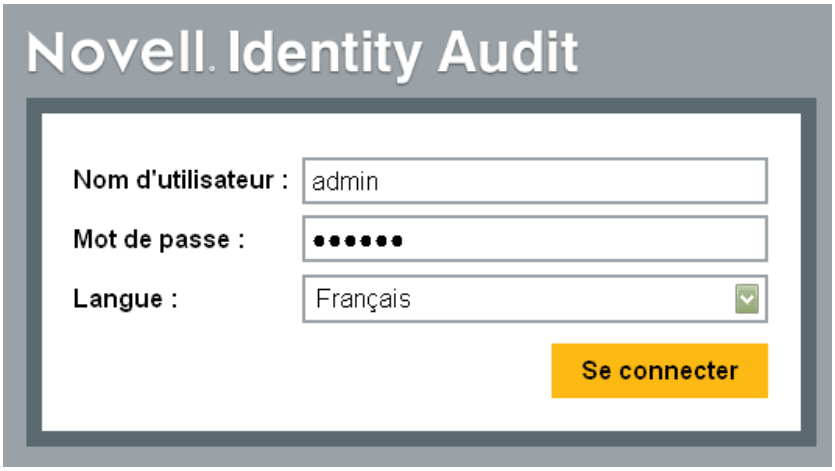
1. Loguez-vous à Identity Audit en tant qu'administrateur.

2 Cliquez sur le lien *Collection* en haut de l'écran.

3 Cliquez sur le lien *Configuration* à droite de l'écran.

4 Assurez-vous que l'onglet *Serveur d'audit* est sélectionné.

5 Cliquez sur l'option *Strict* sous *Authentification client*.

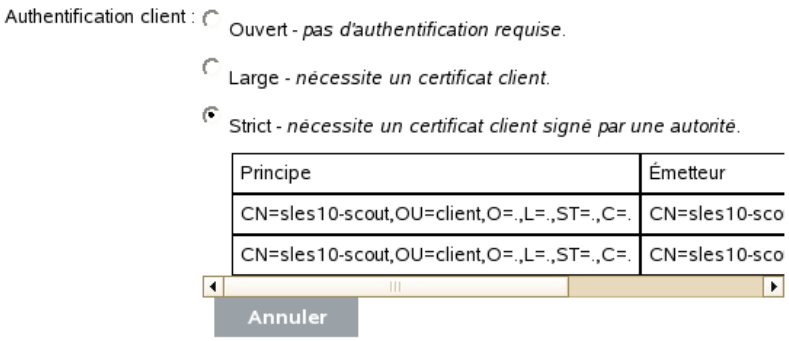


6 Cliquez sur *Parcourir* et recherchez le fichier Truststore (par exemple, `my.keystore`)

7 Entrez le mot de passe du fichier Truststore.

8 Cliquez sur *Importer*.

9 Cliquez sur *Détails* pour afficher un complément d'informations sur le fichier Truststore.



10 Cliquez sur *Enregistrer*.

Une fois le fichier Truststore importé, vous pouvez cliquer sur *Détails* pour afficher les certificats inclus dans le fichier Truststore.

Paire de clés de serveur

Identity Audit est installé avec un certificat intégré qui authentifie le serveur Identity Audit auprès des sources d'événements. Ce certificat peut être remplacé par un certificat signé par une autorité de certification (CA) publique.

Pour remplacer le certificat intégré :

1 Loguez-vous à Identity Audit en tant qu'administrateur.

2 Cliquez sur le lien *Collection* en haut de l'écran.

3 Cliquez sur le lien *Configuration* à droite de l'écran.

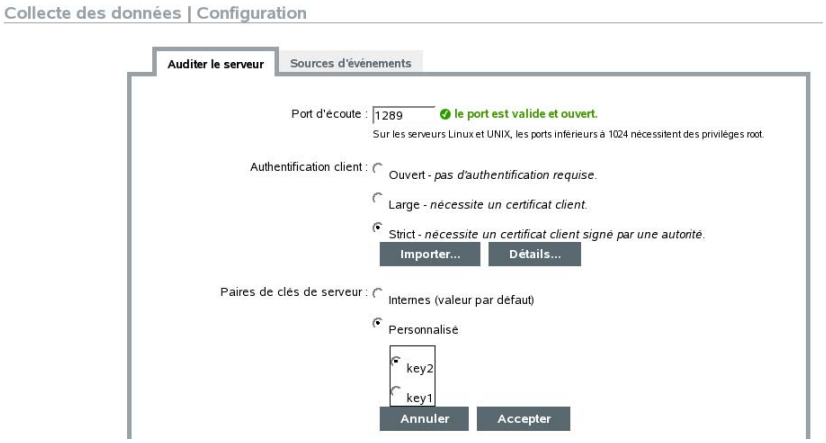
4 Assurez-vous que l'onglet *Serveur d'audit* est sélectionné.

5 Sous *Paires de clés de serveur*, sélectionnez *Personnalisé*.

6 Cliquez sur *Parcourir* et recherchez le fichier Truststore.

7 Entrez le mot de passe du fichier Truststore.

8 Cliquez sur *Importer*.



Si le fichier contient plusieurs paires de clés publiques/privées, sélectionnez la paire de clés souhaitée et cliquez sur *OK*.

9 Cliquez sur *Détails* pour afficher un complément d'informations sur la paire de clés de serveur.

10 Cliquez sur *Enregistrer*.

6.4 Sources d'événements

La page *Sources d'événements* permet aux administrateurs de configurer les paramètres horaires pour les événements de chaque source. Les paramètres horaires des événements peuvent être basés sur le tampon horaire de la source d'événements (« approuver l'heure de l'événement ») ou sur celui du serveur Identity Audit. Le tampon horaire influence l'ordre d'affichage des événements dans une recherche si vous triez sur les paramètres horaires. Le tampon horaire influence également l'heure affichée dans les rapports. Le paramètre par défaut consiste à utiliser l'heure du serveur Identity Audit.

Remarque : il est recommandé de disposer d'un serveur NTP afin de garantir la synchronisation horaire de toutes les machines du système Identity Audit. Si un serveur NTP est disponible, Novell recommande d'approuver l'heure de l'événement pour les applications. Si aucun serveur NTP n'est disponible, Novell recommande d'utiliser l'heure du serveur Identity Audit pour toutes les applications (paramètre par défaut) pour corriger les différences horaires entre les machines.

Pour modifier les options d'heure de l'événement :

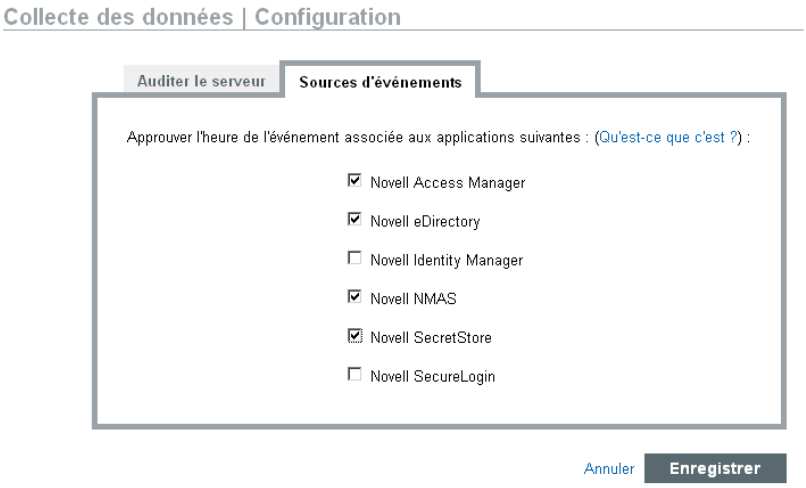
1 Loguez-vous à Identity Audit en tant qu'administrateur.

2 Cliquez sur le lien *Collection* en haut de l'écran.

3 Cliquez sur le lien *Configuration* à droite de l'écran.

4 Cliquez sur *Sources d'événements*.

5 Sélectionnez toutes les applications pour lesquelles Identity Audit doit utiliser le tampon horaire de l'événement provenant de l'application d'origine.



Pour toutes les autres, le tampon horaire du serveur Identity Audit remplace celui de l'application d'origine.

Les changements prennent effet immédiatement pour tous les nouveaux événements entrants. Le traitement des événements déjà en file d'attente peut toutefois prendre un certain temps.

Stockage des données

7

Le programme d'installation de Novell® Identity Audit installe une base de données PostgreSQL contenant toutes les tables et les utilisateurs nécessaires pour exécuter Identity Audit. Cette base de données comprend également des procédures stockées destinées à la gestion des partitions de la base de données et à l'archivage des données anciennes. Les administrateurs peuvent gérer les paramètres de stockage et d'archivage de la base de données via l'interface Web.

7.1 État de santé de la base de données

La page relative à l'état de santé du stockage des données, qui est uniquement accessible pour les administrateurs, affiche l'état de santé de la base de données selon le nombre de partitions disponibles dans la base et l'efficacité des procédures stockées pour la création de nouvelles partitions et l'archivage des données (si configuré).

Pour afficher l'état de santé de la base de données :

1. Loguez-vous à Identity Audit en tant qu'administrateur.
2. Cliquez sur le lien Stockage dans le coin supérieur droit de la page.

   La page relative à l'état de santé s'affiche.

Cette page indique si diverses fonctions de la base de données présentent un bon état (vert), un avertissement (jaune) ou une erreur (rouge).

Base de données en ligne : cet indicateur permet de savoir s'il existe bien dans la base de données le nombre prévu de partitions pour chaque table partitionnée. Le nombre prévu de partitions se base sur le nombre de jours configuré pour être en ligne (ou le nombre de jours depuis l'installation, en cas d'installation récente).

Si le nombre de partitions ne correspond pas aux prévisions, la page affiche le nom de la table concernée ainsi que le nombre prévu et le nombre réel de partitions dans la base de données.

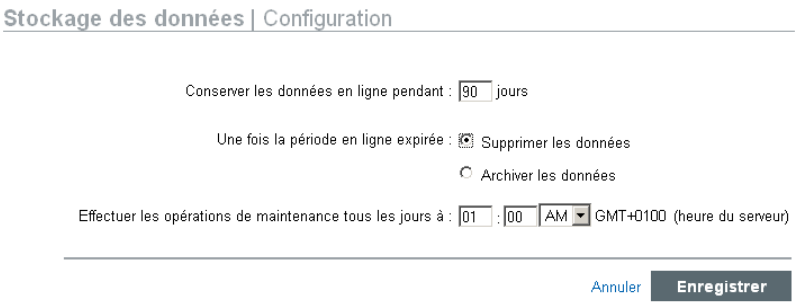
Tâches de base de données en ligne : Cet indicateur devient rouge en cas d'erreurs survenues lors de la dernière exécution des procédures stockées d'ajout de partitions et de suppression de données. Si l'archivage est activé, cet indicateur ne s'affiche que si des erreurs sont survenues lors de la dernière exécution du travail d'ajout de partitions. En cas d'erreurs, la page affiche le nom, le tampon horaire et les détails associés au travail ayant échoué.

Base de données d'archivage : cet indicateur ne s'affiche que si l'archivage est activé. Il devient rouge en cas d'erreurs survenues lors de la dernière exécution de la procédure stockée d'archivage de données. En cas d'erreurs, la page affiche le nom, le tampon horaire et les détails associés au travail ayant échoué.

7.2 Configuration du stockage des données

La base de données constitue l'espace de stockage des événements entrants, des informations de configuration et des résultats des rapports. Identity Audit fournit des procédures de gestion de la base de données afin d'éviter sa saturation. La page Stockage des données, accessible uniquement aux administrateurs, permet de configurer divers aspects du stockage des données.

Figure 7-1 *Configuration du stockage des données*



Conserver les données en ligne pendant : Les administrateurs peuvent spécifier le nombre de jours de conservation des données dans la base à des fins de création de rapports. Le minimum est un jour ; ce doit être un nombre entier (pas de décimale).

Une fois la période en ligne expirée : Une fois la période de conservation des données en ligne écoulée, toutes les données d'événement plus anciennes sont soit supprimées, soit déplacées de la base de données vers un répertoire d'archivage.

Avertissement : Novell ne prend pas en charge la récupération de données supprimées. L'option Supprimer doit dès lors être utilisée avec prudence.

Archiver dans ce répertoire de la base de données : Si vous sélectionnez l'option *Archiver les données*, spécifiez l'emplacement d'un répertoire existant dans lequel les données archivées seront inscrites. Ce répertoire doit déjà exister et l'utilisateur novell doit disposer d'un accès en écriture à ce dernier. Par défaut, cet emplacement est /data/db_archive dans le répertoire privé de Identity Audit. Le répertoire par défaut est créé avec les autorisations adéquates lors de l'installation de Identity Audit.

Important : Novell recommande de déplacer régulièrement les fichiers d'archivage vers un emplacement de stockage à long terme pour éviter une saturation du disque dur.

Tester: Si l'option *Archiver les données* est sélectionnée, le bouton Tester permet de vérifier si le répertoire d'archivage existe et s'il est accessible en écriture par l'utilisateur novell.

Effectuer les opérations de maintenance tous les jours à : Spécifiez l'heure à laquelle les routines de maintenance doivent être effectuées. Elle se base sur l'heure locale du serveur Identity Audit. À l'heure planifiée pour la maintenance, une procédure stockée s'exécute afin d'ajouter des partitions à la base de données. Deux heures plus tard, une autre procédure stockée intervient pour archiver ou supprimer les données plus anciennes que le nombre de jours configuré.

Il convient de planifier l'archivage des données à un moment de la journée où la base de données est relativement peu utilisée.

Règles

8

Ce chapitre décrit les canaux d'événements qui peuvent être utilisés pour envoyer des événements depuis Identity Audit vers un autre système.

8.1 Présentation des règles

L'interface Règles permet de définir des règles afin d'évaluer tous les événements entrants et d'acheminer les événements sélectionnés vers les canaux de sortie désignés. Par exemple, chaque événement d'un niveau de gravité de 5 peut être envoyer par courrier électronique à une liste de distribution d'analystes de sécurité ou à un administrateur.

Remarque : tous les événements sont également acheminés vers la base de données.

Un événement entrant est évalué par rapport à chaque règle de filtre pour que, en cas de correspondance, les opérations d'acheminement associées à cette règle soient déclenchées :

Envoyer un message électronique : envoie l'événement à un ou plusieurs utilisateurs à l'aide d'un relais SMTP configuré.

Consigner dans le fichier : permet d'inscrire l'événement dans un fichier spécifié sur le serveur Identity Audit.

Consigner dans Syslog : permet de transférer l'événement à un serveur syslog configuré.

Suggestion : les événements sont traités individuellement par les opérations associées. De ce fait, ne négligez pas les implications en termes de performances lors de la sélection du canal de sortie pour l'envoi des événements. Par exemple, l'opération Consigner dans le fichier est celle utilisant le moins de ressources ; elle peut donc être utilisée pour tester des critères de règle afin de déterminer le volume de données avant l'envoi d'un flux d'événements par courrier électronique ou via syslog.

De même, lorsque vous configurez l'opération Envoyer un message électronique, vous devez tenir compte du nombre d'événements que le destinataire peut effectivement gérer et régler le filtrage sur la règle de façon appropriée.

La sortie d'événements utilise le format JSON (JavaScript Object Notation), un format d'échange de données léger. Les événements correspondent à des noms de champ (par exemple, "evt" pour le nom de l'événement) suivis de deux-points et d'une valeur (par exemple, "Start") et séparés par des virgules.


```
{"st":"I","evt":"Start","sev":"1","sres":"Collector","res":"Collec
torManager","rv99":"0","rv1":"0","repassetid":"0","rv77":"0","agen
t":"Novell SecureLogin","obsassetid":"0","vul":"0","port":"Novell
SecureLogin","msg":"Processing started for Collector Novell
```

SecureLogin (ID D892E9F0-3CA7-102B-B5A1-005056C00005).","dt":"1224204655689","id":"751D97B0-7E13-112B-B933-000C29E8CEDE","src":"D892E9F0-3CA7-102B-B5A2-005056C00004"}

8.2 Configuration de règles

Il est possible de configurer des règles Identity Audit afin de filtrer les événements selon un ou plusieurs champs pouvant faire l'objet de recherches. Pour obtenir une liste des champs d'événement de Identity Audit qui peuvent faire l'objet de recherches, reportez-vous au Tableau 4-1 page 30. Chaque règle peut être associée à une ou plusieurs opérations configurées.

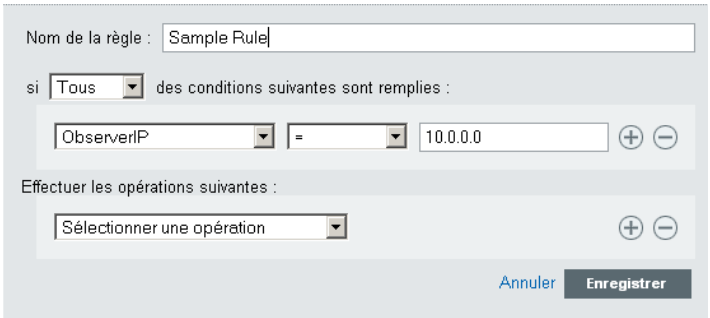
8.2.1 Critères de filtre

Les règles peuvent être basées sur n'importe quel champ pouvant faire l'objet de recherches. Pour obtenir la liste de ces champs, reportez-vous au Tableau 4-1 page 30. Les opérateurs disponibles dépendent du type de données du champ d'événement. Par exemple, `correspond au sous-réseau` est disponible pour les adresses IP et `correspond à regex` est disponible pour les champs de texte.

8.2.2 Ajout d'une règle

Les administrateurs peuvent ajouter une règle basée sur le filtre, puis définir un ou plusieurs canaux vers lesquels envoyer les événements qui correspondent aux critères définis pour la règle.

1. Loguez-vous à Identity Audit en tant qu'administrateur.
2. Cliquez sur .*Règles* dans le coin supérieur droit de la page.
3. Cliquez sur *Ajouter une règle*.
4. Entrez un nom de règle.
5. Si vous souhaitez créer plusieurs conditions, sélectionnez *Tous* pour lier les conditions avec un opérateur AND. Sélectionnez *une des* pour lier les conditions avec un opérateur OR.
6. Sélectionnez le champ d'événement, l'opérateur et la valeur du filtre.



7 Sélectionnez une opération à effectuer sur chaque événement qui correspond aux critères de filtre.

   Les détails des opérations sont basés sur les informations de configuration qui s'affichent lorsque vous cliquez sur le lien *Configuration*.

8 Configurez autant d'opérations que vous le souhaitez.

9 Cliquez sur *Enregistrer*.

8.2.3 Classement des règles

Étant donné que les événements sont évalués par les règles dans l'ordre jusqu'à l'obtention d'une correspondance, Novell vous recommande de classer les règles de façon appropriée. Les règles les plus importantes et celles définies avec le plus de précision doivent être placées en tête de liste. Si plusieurs règles existent, elles peuvent être réorganisées à l'aide de la fonction glisser-déplacer.

Pour reclasser les règles :

1 Loguez-vous à Identity Audit en tant qu'administrateur.

2 Cliquez sur .*Règles* dans le coin supérieur droit de la page.

3 Placez le curseur de la souris sur l'icône à gauche des numéros de règle pour activer la fonction glisser-déplacer. La forme du curseur change.

4 Effectuez un glisser-déplacer de la règle vers l'emplacement adéquat dans la liste triée.

8.2.4 Suppression d'une règle

Si des événements sont déjà en file d'attente pour une ou plusieurs opérations lorsque vous supprimez une règle, le vidage de la file d'attente après la désactivation de la règle peut prendre un certain temps.

8.2.5 Activation ou désactivation d'une règle

Sous la colonne Actif, une case à cocher à gauche de chaque règle permet d'activer cette dernière. Les nouvelles règles sont activées par défaut. Si vous désactivez une règle, les événements entrants ne sont plus évalués par celle-ci. Si des événements sont déjà en file d'attente pour une ou plusieurs opérations, le vidage de la file d'attente après la désactivation de la règle peut prendre un certain temps.

8.3 Configuration d'opérations

Un événement est acheminé vers un ou plusieurs canaux lorsqu'il satisfait aux critères spécifiés par une des règles. Avant que les événements ne puissent être envoyés vers un canal, il faut configurer l'opération d'envoi vers ce canal avec les informations de connexion appropriées (ainsi que les références d'authentification, si elles sont nécessaires pour le relais SMTP). Le système Identity Audit ne peut avoir qu'une seule connexion configurée par type d'opération (par exemple, tous les événements qui doivent être inscrits dans un fichier doivent l'être dans le même fichier).

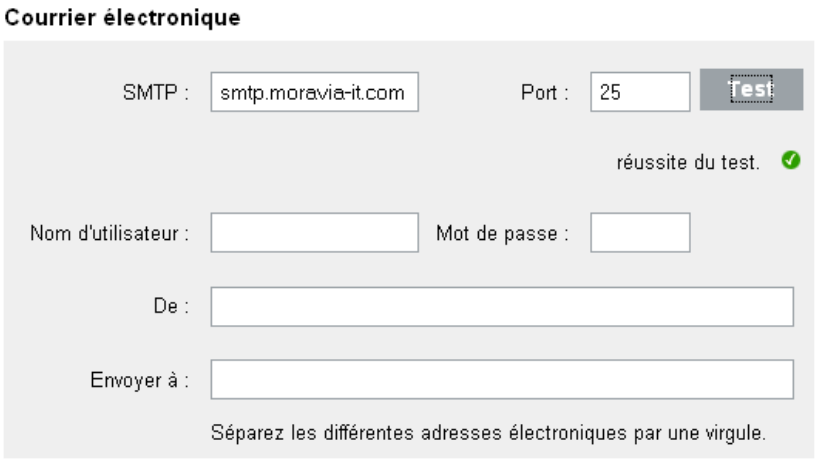
8.3.1 Envoyer un message électronique

Pour configurer une opération Envoyer un message électronique, vous avez besoin des informations de connexion d'un relais SMTP (adresse IP et numéro de port), ainsi que des adresses d'émission et de réception. Vous pouvez envoyer le message à plusieurs adresses électroniques. Pour ce faire, spécifiez-les sous forme d'une liste séparée par des virgules.

Remarque : pour éviter des surcharges de votre relais SMTP ou des destinataires des messages électroniques, cette opération ne doit être utilisée qu'avec des règles qui génèrent de faibles volumes d'événements.

La configuration du relais SMTP permet également d'envoyer des rapports aux utilisateurs.

1. Loguez-vous à Identity Audit en tant qu'administrateur.
2. Cliquez sur .*Règles* dans le coin supérieur droit de la page.
3. Cliquez sur *Configuration*.
4. Sous *Courrier électronique*, entrez le nom et le port d'un relais SMTP disponible. Si vous le souhaitez, cliquez sur *Test* pour contrôler la connexion.



5. Si le relais SMTP requiert une authentification, entrez un nom d'utilisateur et un mot de passe.
6. Entrez l'adresse de l'expéditeur des messages électroniques.

7 Entrez une ou plusieurs adresses électroniques en les séparant par une virgule.

8 Cliquez sur *Enregistrer*.

Tous les événements Identity Audit qui répondent aux critères de filtre pour lesquels l'opération Envoyer un message électronique est définie, sont transmis aux mêmes relais et liste d'adresses.

8.3.2 Consigner dans Syslog

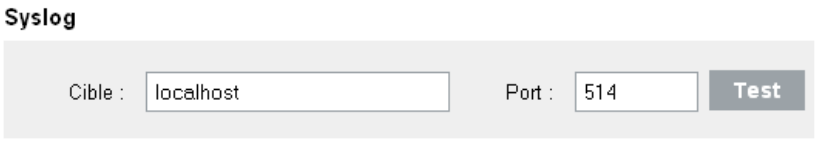
Pour configurer une opération Consigner dans Syslog, vous avez besoin des informations de connexion du serveur Syslog (adresse IP et numéro de port).

1 Loguez-vous à Identity Audit en tant qu'administrateur.

2 Cliquez sur .*Règles* dans le coin supérieur droit de la page.

3 Cliquez sur *Configuration*.

4 Sous *Syslog*, entrez un nom ou une adresse IP et un port ouvert d'un serveur Syslog. Si vous le souhaitez, cliquez sur *Test* pour tester si le serveur cible et le port existent.



5 Cliquez sur *Enregistrer*.

Tous les événements Identity Audit qui répondent aux critères de filtre pour lesquels l'opération Consigner dans Syslog est définie, sont envoyés au même serveur syslog.

8.3.3 Consigner dans le fichier

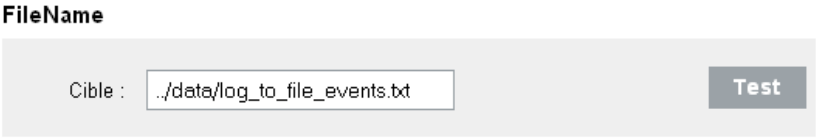
Pour configurer l'opération Consigner dans le fichier, vous avez besoin du nom et du chemin du fichier dans lequel les événements seront inscrits. Le répertoire doit déjà exister et l'utilisateur novell doit disposer d'autorisations d'écriture sur ce dernier. Si le fichier n'existe pas encore, Identity Audit le crée.

1 Loguez-vous à Identity Audit en tant qu'administrateur.

2 Cliquez sur .*Règles* dans le coin supérieur droit de la page.

3 Cliquez sur *Configuration*.

4 Sous *FileName*, entrez le chemin du fichier dans lequel vous souhaitez consigner les événements. Si vous le souhaitez, cliquez sur *Test* pour contrôler la connexion.



5 Cliquez sur *Enregistrer*.

Tous les événements Identity Audit qui répondent aux critères de filtre pour lesquels l'opération Consigner dans le fichier est définie, sont inscrits dans le même fichier.

Administration des utilisateurs

9

Les administrateurs peuvent ajouter, éditer et supprimer des utilisateurs dans Novell® Identity Audit et accorder des droits d'administration. Les utilisateurs, quant à eux, peuvent modifier les détails de leur propre profil utilisateur.

9.1 Ajout d'un utilisateur

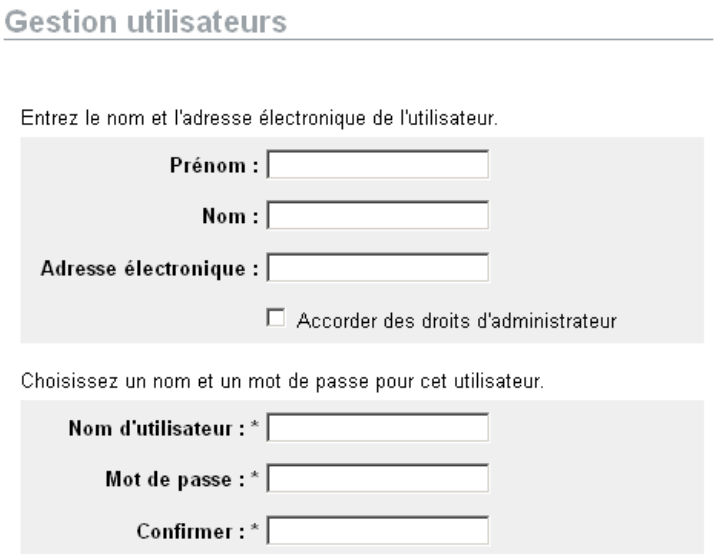
L'ajout d'un utilisateur dans le système Identity Audit crée un utilisateur qui peut alors se loguer à l'application Identity Audit.

Si l'option *Accorder des droits d'administrateur* est sélectionnée, l'utilisateur se voit attribuer des droits d'administration dans le système Identity Audit. Ces droits permettent notamment de gérer les fonctions suivantes :

- Administration des utilisateurs
- Collecte des données
- Stockage des données

Pour ajouter un utilisateur :

1. Loguez-vous à Identity Audit en tant qu'administrateur.
2. Cliquez sur .*Gestion utilisateurs* dans le coin supérieur droit de la page.
3. Cliquez sur *Ajouter un utilisateur*.
4. Entrez les informations relatives à l'utilisateur.



Les champs marqués d'un astérisque (*) sont obligatoires et le nom d'utilisateur doit être unique.

Remarque : le format d'adresse électronique est validé, mais les champs réservés au numéro de téléphone autorisent tous les formats. Veillez à entrer un numéro de téléphone valide.

---

5 Sélectionnez *Accorder des droits d'administrateur*, si vous le souhaitez.

6 Cliquez sur *Enregistrer*.

9.2 Édition des détails des utilisateurs

Les administrateurs peuvent éditer les informations de n'importe quel utilisateur dans le système. Les utilisateurs peuvent également éditer tous les champs de leur profil à l'exception de leur nom d'utilisateur et leur statut d'administrateur. Les utilisateurs peuvent également modifier les mots de passe.

- Section 9.2.1, « Éditer votre profil », page 64
- Section 9.2.2, « Modifier votre mot de passe », page 65
- Section 9.2.3, « Éditer le profil d'un autre utilisateur (fonctionnalité exclusivement réservée aux administrateurs) », page 65
- Section 9.2.4, « Réinitialiser le mot de passe d'un autre utilisateur (fonctionnalité exclusivement réservée aux administrateurs) », page 66

9.2.1 Éditer votre profil

1 Cliquez sur *profil* dans le coin supérieur droit.

2 Éditez les champs disponibles.

3 Cliquez sur *Enregistrer*.

9.2.2 Modifier votre mot de passe

S'ils connaissent leur mot de passe actuel, les utilisateurs peuvent le modifier. Dans le cas contraire, un administrateur doit réinitialiser le mot de passe.

1 Cliquez sur *profil* dans le coin supérieur droit.

2 Entrez votre mot de passe actuel.

3 Entrez votre nouveau mot de passe.

4 Confirmez votre nouveau mot de passe.

5 Cliquez sur *Enregistrer*.

9.2.3 Éditer le profil d'un autre utilisateur (fonctionnalité exclusivement réservée aux administrateurs)

1 Loguez-vous à Identity Audit en tant qu'administrateur.

2 Cliquez sur .*Gestion utilisateurs* dans le coin supérieur droit de la page.

3 Cliquez sur *Éditer* sous l'utilisateur dont vous souhaitez éditer le profil.

4 Éditez les champs (à l'exception du nom d'utilisateur).

5 Cliquez sur *Enregistrer*.

Les modifications apportées à la page *Accorder des droits d'administrateur* prennent effet au prochain login de l'utilisateur.

9.2.4 Réinitialiser le mot de passe d'un autre utilisateur (fonctionnalité exclusivement réservée aux administrateurs)

Pour réinitialiser le mot de passe d'un utilisateur, reportez-vous à la Section 9.2.3, « Éditer le profil d'un autre utilisateur (fonctionnalité exclusivement réservée aux administrateurs) », page 65.

9.3 Suppression d'un utilisateur

Les administrateurs peuvent supprimer des utilisateurs du système.

1 Loguez-vous à Identity Audit en tant qu'administrateur.

2 Cliquez sur .*Gestion utilisateurs* dans le coin supérieur droit de la page.

3 Cliquez sur *Éditer* sous l'utilisateur que vous souhaitez supprimer.

4 Cliquez sur *Supprimer cet utilisateur* dans le coin supérieur droit de la page.

5 Cliquez sur *Supprimer* pour confirmer la suppression.

Fichier Truststore

A

L'utilisation d'une authentification stricte pour la connexion entre Identity Audit et les applications Novell dont elle collecte les données peut améliorer la sécurité des données.

A.1 Créer un fichier Keystore

Un fichier Keystore peut être créé à l'aide du programme exécutable « keytool » de Java fourni avec toutes les installations JRE. Ce fichier Keystore contient une paire de clés publique/privée permettant de remplacer le certificat par défaut fourni avec Identity Audit. Vous trouverez des instructions de base ci-dessous, mais pour plus d'informations sur keytool, consultez le site Web de Sun (http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html).

1. Allez dans le répertoire /bin pour Java (par exemple, `$JAVA_HOME/bin`).
2. Exécutez la commande suivante :

   ```
   keytool -genkey -alias alias -keystore .keystore
   ```

3. Entrez un mot de passe pour le fichier Keystore. Il est utilisé lors de l'importation du fichier Truststore.
4. Entrez les informations suivantes : votre prénom et votre nom.
   - Prénom et nom
   - Unité organisationnelle
   - Organisation
   - Ville ou localité
   - Département ou province
   - Code du pays à deux chiffres
5. Vérifiez les informations.
6. Appuyez sur Entrée pour utiliser le même mot de passe que celui de Keystore.

   Un fichier .keystore est créé avec une clé privée et une clé publique correspondante (certificat).