CA User Activity Reporting Module

Manuel de présentation

Version 12.5.03

Produits CA référencés

Ce document fait référence aux produits CA suivants :

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- Poste de service CA
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Modifications de la documentation

Les actualisations suivantes ont été réalisées depuis la dernière version de la présente documentation.

- Présentation du démarrage rapide : cette rubrique existante a été mise à jour pour référencer des types d'événement, en plus des syslogs, pouvant être collectés par l'agent par défaut sur le serveur CA User Activity Reporting Module.
- Alerte de violation de stratégie : cette rubrique existante a été mise à jour de manière à référencer la possibilité d'envoyer des alertes sous forme d'interruptions SNMP à des systèmes de surveillance de la sécurité système et des alertes directes, pour exécuter un processus de sortie de l'événement/de l'alerte IT PAM, tel qu'un processus de création de tickets d'assistance.
- Explorer la bibliothèque de documentation : cette rubrique existante a été mise à jour pour référencer le nouveau Manuel de programmation de l'API, qui apparaît dorénavant sur la bibliothèque CA User Activity Reporting Module.

Informations complémentaires :

Présentation d'un déploiement rapide (page 13)
Alerte de violation de stratégie (page 60)
Exploration de la bibliothèque de documentation (page 72)

Table des matières

Chapitre 1 : Introduction

Ce chapitre traite des sujets suivants :

A propos de ce manuel

Ce *Manuel de présentation* traite de CA User Activity Reporting Module. Il débute par de rapides didacticiels qui vous permettent d'acquérir une première expérience du produit. Le premier didacticiel vous guide pour installer CA Enterprise Log Manager sur un seul serveur, l'exécuter et afficher des Syslogs collectés à partir d'unités UNIX à proximité sur le réseau. Le deuxième didacticiel vous guide pour installer un agent sur un système d'exploitation Windows, configurer la collecte de journaux et afficher les journaux d'événements qui en résultent. Il décrit ensuite les principales fonctions et indique les ressources permettant d'en savoir plus. Ce manuel a été conçu pour tous les publics.

Vous trouverez ci-dessous un récapitulatif du contenu.

Section	Description
A propos de CA Enterprise Log Manager	Intégrer CA User Activity Reporting Module dans votre environnement réseau actuel.
Déploiement rapide	Installer un système sur un seul serveur, configurer les sources d'événement Syslog, mettre à jour le connecteur Syslog pour l'agent par défaut et afficher les événements ajustés.
Déploiement de l'agent Windows	Préparer l'installation de l'agent, installer un agent pour le système d'exploitation Windows, configurer un connecteur pour la collecte avec agent, mettre à jour la source d'événement et afficher les événements générés.
Principales fonctionnalités	Profiter des principales fonctions, dont la collecte de journaux, le stockage des journaux, la génération de rapports de conformité et les alertes.
Informations complémentaires concernant CA User Activity Reporting Module	Obtenir les informations nécessaires par le biais des infobulles, de l'aide en ligne et de la bibliothèque documentaire.

Remarque : Pour plus de détails sur la prise en charge des systèmes d'exploitation ou la configuration système requise, consultez les *Notes de parution*. Pour disposer de procédures pas à pas sur l'installation de CA User Activity Reporting Module et la configuration initiale, consultez le *Manuel d'implémentation*. Pour plus de détails sur l'installation d'un agent, consultez le *Manuel d'installation des agents*. Pour plus de détails sur l'utilisation et la maintenance du produit, consultez le *Manuel d'administration*. Pour obtenir de l'aide quant à l'utilisation d'une page CA User Activity Reporting Module, consultez l'aide en ligne.

A propos de CA User Activity Reporting Module

CA User Activity Reporting Module est axé sur la conformité et l'assurance informatiques. Il vous permet de collecter, de normaliser, de cumuler et de générer des rapports concernant l'activité informatique, mais également de générer des alertes nécessitant une action en cas de violations de la conformité. Vous pouvez collecter des données provenant d'unités disparates, sécurisées et non sécurisées.

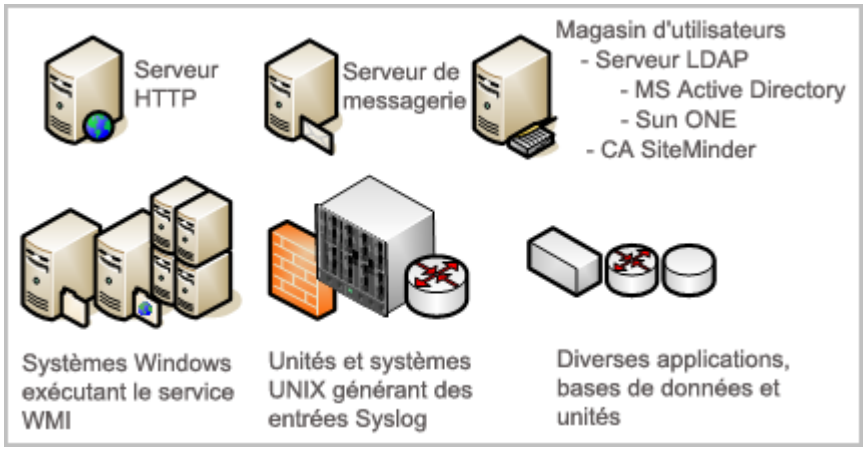
Votre réseau avant l'installation

Les réglementations et lois fédérales exigent la gestion des enregistrements de journaux. Par souci de conformité, vous devez.

- Autoriser l'accès aux journaux pour les audits.
- Stocker les journaux pendant plusieurs années.
- Restaurer les journaux à la demande.

Le grand nombre des enregistrements de journaux, leur emplacement et leur nature temporaire rendent difficile leur gestion. Les journaux sont continuellement générés par l'utilisateur et l'activité du processus sur le logiciel. Le taux de génération se mesure en événements par seconde (eps). Les événements bruts sont enregistrés sur chaque base de données, application et système actifs de votre réseau. La sauvegarde d'enregistrements de journaux doit se faire au niveau de chaque source d'événement avant qu'ils ne soient écrasés. La restauration des journaux d'événement est difficile quand des sources d'événement différentes sont stockées séparément.

Le format de la chaîne des événements bruts rend fastidieux leur interprétation car la sévérité de l'événement n'est pas évidente. Des données similaires peuvent également varier sur des systèmes différents.



L'efficacité opérationnelle exige une solution qui regroupe tous les journaux, facilite leur lecture, automatise l'archivage et le stockage et rationalise leur restauration. CA User Activity Reporting Module offre ces avantages, et vous permet d'envoyer des alertes aux personnes et systèmes quand des événements critiques se produisent.

Eléments installés

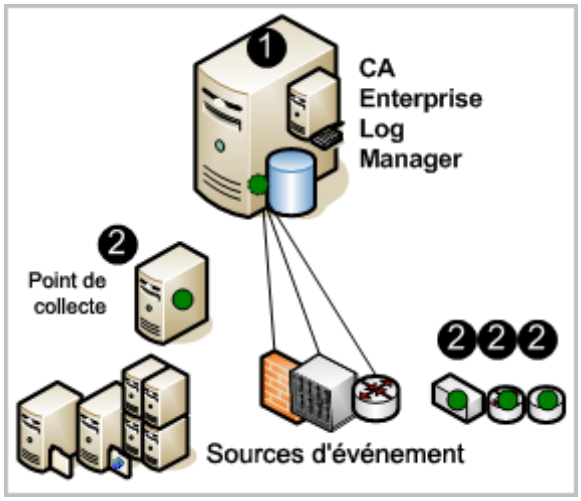
La configuration d'une solution avec un seul serveur et le lancement de la collecte d'événements prennent peu de temps.

Les disques d'installation incluent les composants ci-dessous.

- Système d'exploitation (Red Hat Enterprise Linux) pour le dispositif logiciel
- Serveur CA User Activity Reporting Module
- Agent CA User Activity Reporting Module (désigné ci-après par l'agent)

Dans l'illustration qui suit, CA User Activity Reporting Module est décrit comme un serveur comportant un petit serveur, un cercle sombre (vert) et une base de données. Le petit serveur représente le référentiel local de stockage de contenu au niveau des applications. Le cercle sombre représente l'agent par défaut et la base de données représente le magasin de journaux d'événements, où les journaux d'événements entrants sont traités et mis à disposition pour les requêtes et les rapports.

Les cercles sombres (verts) sur le point de collecte et les autres sources d'événement représentent des agents installés séparément. L'installation d'autres agents est facultative. Vous pouvez collecter des Syslogs provenant de sources d'événement compatibles avec UNIX grâce à l'agent par défaut, une fois la configuration requise terminée.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Vous installez le système d'exploitation pour le dispositif logiciel, puis vous installez l'application CA User Activity Reporting Module. Dès que vous configurez vos sources pour envoyer des Syslogs vers CA User Activity Reporting Module et que vous indiquez les cibles Syslog dans la configuration du connecteur pour l'agent par défaut, les Syslogs sont collectés et ajustés afin de simplifier leur interprétation.
2. (Facultatif) Vous pouvez installer un agent sur un hôte dédié comme point de collecte ou vous pouvez installer des agents directement sur les hôtes disposant des sources générant les événements que vous souhaitez collecter.

Remarque : Pour plus de détails sur l'installation du dispositif logiciel, consultez le *Manuel d'implémentation*. Pour plus de détails sur l'installation des agents, consultez le *Manuel d'installation des agents*.

Informations complémentaires :

Installation d'un agent (page 40)

Chapitre 2 : Déploiement rapide

Ce chapitre traite des sujets suivants :

Présentation d'un déploiement rapide

Vous pouvez obtenir un déploiement CA User Activity Reporting Module simple et en état de fonctionnement avec un seul dispositif logiciel. Le connecteur Syslog prédéfini permet à l'agent par défaut de recevoir les événements générés par Syslog. Il vous suffit de configurer vos sources Syslog pour envoyer les événements Syslog vers CA User Activity Reporting Module et de modifier la configuration du connecteur Syslog pour identifier les cibles Syslog. Les données reçues dépendent de la bande passante entre le serveur et les sources Syslog, ainsi que de la latence.

Les capteurs de journaux, y compris WinRM et ODBC, prennent en charge les collectes directes de l'ensemble des journaux parmi plus de vingt sources d'événement autres que Syslog. Le capteur de journaux WinRM vous permet de collecter des événements directement à partir de serveurs exécutant Windows, comme le serveur Forefront Security pour Exchange, Forefront Security pour SharePoint Server, Microsoft Office Communication Server et le serveur virtuel Hyper-V, ainsi que des services, tels que les services de certificats Active Directory. Le capteur de journaux ODBC vous permet de capturer des événements générés par des bases de données Oracle9i ou SQL Server 2005. Pour plus de détails, consultez la matrice d'intégration de produits CA Enterprise Log Manager.

Pour installer CA User Activity Reporting Module, vous devez disposer des informations d'identification d'EiamAdmin. En tant que superutilisateur EiamAdmin, vous configurez un compte d'administrateur que vous utilisez pour effectuer la configuration. Si vous vous connectez en utilisant les informations d'identification de l'administrateur, vous pouvez vérifier que l'installation est correcte en visualisant des événements d'autosurveillance.

Installation d'un système à un seul serveur

Un système à un seul serveur constitue le déploiement le plus simple vous permettant d'effectuer des requêtes sur des événements et d'en afficher les résultats. Veillez à sélectionner un ordinateur respectant la configuration matérielle minimale pour un dispositif logiciel CA User Activity Reporting Module.

Remarque : Pour obtenir la liste du matériel certifié, les systèmes d'exploitation pris en charge et la configuration requise en termes de logiciel système et de services, consultez les *Notes de parution*.

Pour installer CA User Activity Reporting Module sur un système à un seul serveur

1. Conservez à votre disposition les informations ci-dessous.
   - Mot de passe de l'utilisateur root
   - Nom d'hôte pour votre dispositif
   - Si vous n'utilisez pas DHCP, l'adresse IP statique, le masque de sous-réseau et la passerelle par défaut de votre dispositif
   - Domaine du dispositif

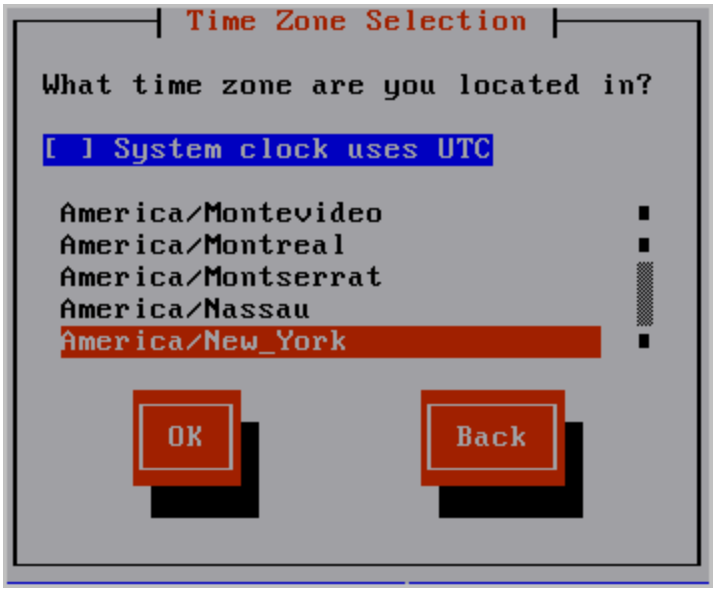
     Remarque : Le domaine doit être enregistré auprès des serveurs DNS de votre réseau pour que l'installation se termine correctement.
   - Adresse IP des serveurs DNS
   - Adresse IP de votre serveur de synchronisation NTP (facultatif)
   - Mot de passe du superutilisateur d'installation par défaut EiamAdmin
   - CAELM

     Il s'agit du nom d'application par défaut de l'application CA User Activity Reporting Module.

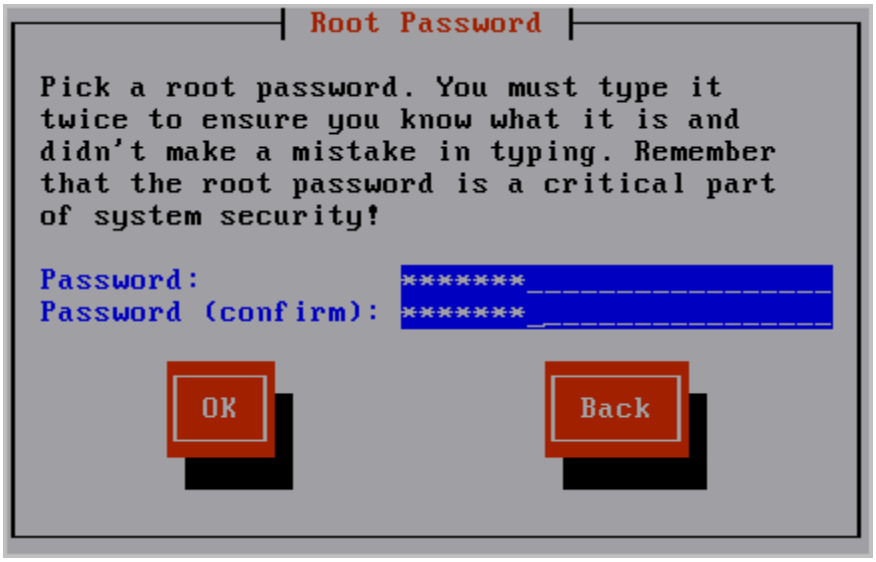
2. Installez le système d'exploitation préconfiguré à l'aide du média que vous avez créé à partir du package de téléchargement CA User Activity Reporting Module. Lors de l'installation du système d'exploitation, effectuez les opérations répertoriées ci-dessous.

   a. Choisissez un type de clavier. Par défaut, il s'agit d'un clavier Etats-Unis.

   b. Choisissez un fuseau horaire, par exemple America/New York, puis sélectionnez OK.



   c. Saisissez le mot de passe à utiliser comme mot de passe root, puis saisissez-le à nouveau pour le confirmer. Sélectionnez OK.



Les informations relatives à la progression de l'installation apparaissent.

d. Retirez le disque d'installation du système d'exploitation, puis appuyez sur Entrée pour redémarrer le système.

Le système redémarre et entre en mode de démarrage non interactif. Il affiche les messages décrivant la progression de l'installation. Des informations détaillées sur cette installation sont enregistrées dans le fichier /tmp/pre-install_ca-elm.log.

L'invite ci-dessous s'affiche.

```
Please insert the CA Enterprise Log Manager r12 - Application Install disk
and press enter (Insérez le disque d'installation de l'application CA
Enterprise Log Manager r12 et appuyez sur Entrée)
```

3. Insérez le disque de l'application CA User Activity Reporting Module. Appuyez sur Entrée.

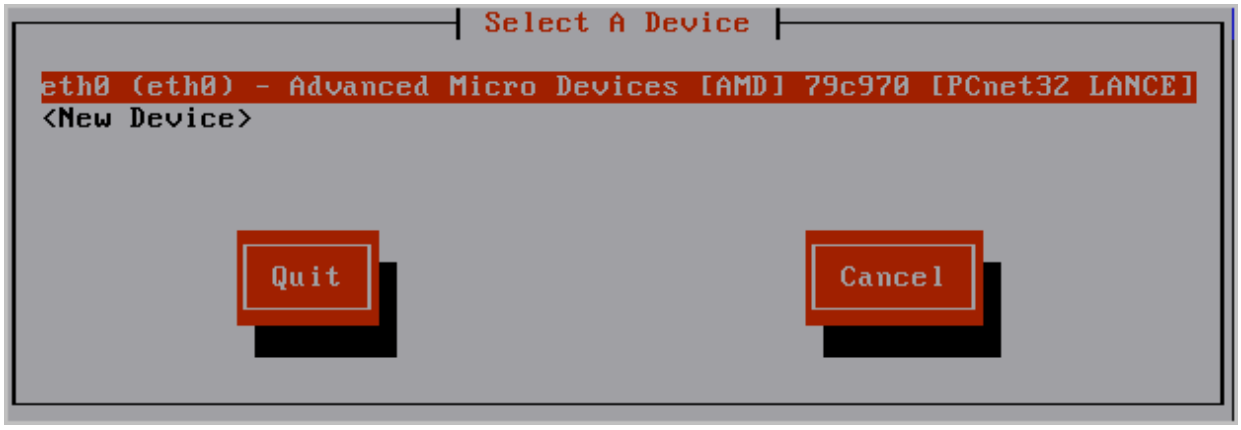
   Le processus d'installation vérifie si votre système respecte les spécifications minimales recommandées pour des performances optimales. Si tel n'est pas le cas, une invite s'affiche vous demandant si vous souhaitez arrêter ce processus d'installation.

   L'invite ci-dessous s'affiche.

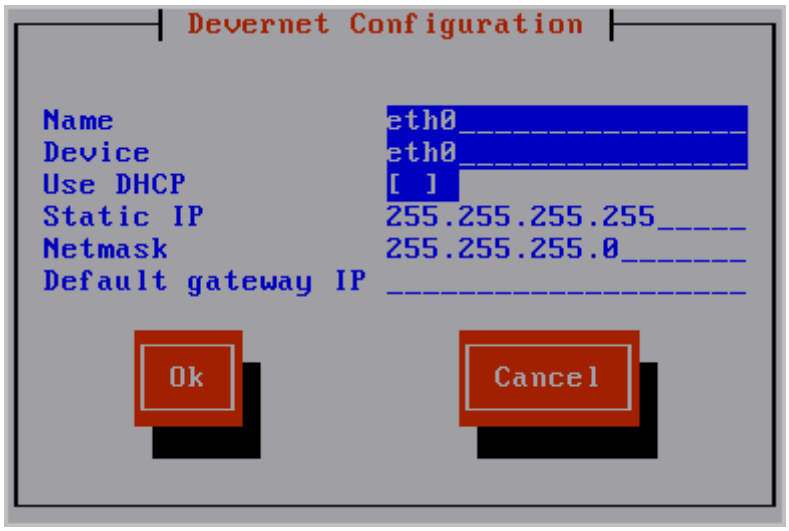
   ```
   Please enter a new hostname (Entrez un nouveau nom d'hôte)
   ```

4. Entrez le nom d'hôte de ce dispositif logiciel CA User Activity Reporting Module. Par exemple, entrez CALM1.

5. Acceptez l'unité par défaut, eth0. Appuyez sur Entrée pour passer à l'écran suivant.



6. Effectuez l'une des opérations suivantes, puis sélectionnez OK.
   - Sélectionnez Use DHCP, une option acceptable uniquement pour un système de test autonome.
   - Entrez l'adresse IP statique, le masque de sous-réseau et l'adresse IP de la passerelle par défaut à associer au nom d'hôte que vous avez entré.



Les services réseau sont redémarrés avec les nouveaux paramètres, qui sont affichés.

Le message suivant s'affiche :

```
Do you want to change the network configuration? (Voulez-vous modifier la
configuration du réseau ?)  (n) :
```

7. Vérifiez les paramètres du réseau. S'ils sont satisfaisants, saisissez "n" ou appuyez sur Entrée lorsqu'apparaît le message vous permettant de modifier les paramètres réseau.

   Le message suivant s'affiche :

   ```
   Please enter the domain name for this system (Entrez le nom du domaine pour
   ce système)
   ```

8. Entrez votre nom de domaine, par exemple <votre_société>.com.

   Le message suivant s'affiche :

   ```
   Please enter a comma separated list of DNS servers to use (Entrez une liste
   de serveurs DNS séparés par des virgules)
   ```

9. Entrez les adresses IP de vos serveurs DNS internes, séparées par des virgules et sans espace.

   La date et l'heure de votre système s'affichent avec le message ci-dessous.

   ```
   Do you want to change the system date and time? (Voulez-vous modifier l'heure
   et la date du système ?) (n)
   ```

10. Vérifiez la date et l'heure affichées du système. Si elles sont satisfaisantes, saisissez "n" ou appuyez sur Entrée.

    Le message suivant s'affiche :

    ```
    Do you want to configure the system to update the time through NTP? (Voulez-
    vous configurer le système pour mettre à jour l'heure via NTP ?)
    ```

11. Si vous souhaitez utiliser un serveur NTP (Network Time Protocol), continuez comme suit. Si tel n'est pas le cas, entrez "no" et passez à l'étape suivante.

    a. Répondez "yes" au message.

       Si vous spécifiez "yes", le message suivant apparaît.

       ```
       Please enter the NTP Server name or IP Address (Entrez le nom du serveur
       NTP ou l'adresse IP)
       ```

    b. Entrez le nom d'hôte ou l'adresse IP du serveur NTP.

       Un message de confirmation similaire au message suivant apparaît :"Your system has been configured to update the time at midnight using the NTP server located at <yourntpserver>."

12. Lisez les contrats de licence d'utilisateur final présentés et répondez comme suit.

    a. Lisez le contrat de licence d'utilisateur final du kit de développement Sun Java (JDK).

       A la fin du contrat, le message ci-dessous apparaît.

       ```
       Do you agree to the above license terms? (Acceptez-vous les conditions de licence ci-dessus ?) [yes or no]
       ```

    b. Saisissez "yes" si vous en acceptez les termes.

       Les informations d'enregistrement de produit sont affichées, suivies du message ci-dessous.

       ```
       Press Enter to continue.....
       ```

    c. Appuyez sur Entrée.

       Des messages indiquent qu'en préparation à l'installation CA User Activity Reporting Module, les paramètres système sont en cours de configuration. Le contrat de licence d'utilisateur final CA s'affiche.

    d. Lisez ce contrat de licence.

       A la fin du contrat, le message ci-dessous apparaît.

       ```
       Do you agree to the above license terms? (Acceptez-vous les conditions de licence ci-dessus ?) [Yes or no]:
       ```

    e. Saisissez "Yes" si vous en acceptez les termes.

       Les informations de serveur CA EEM apparaissent.

13. Répondez aux invites suivantes pour configurer CA EEM.

    ```
    Do you use a local or remote EEM server? (Utilisez-vous un serveur EEM local ou distant ?)
    Enter l (local) or r (remote) (Entrez l (local) ou r (distant))
    ```

    a. Pour créer un système de test autonome, entrez l pour local.

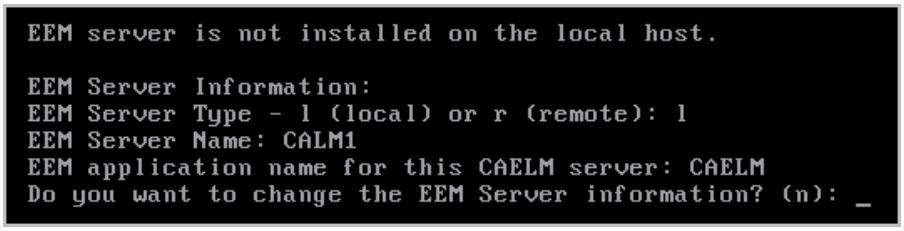
       ```
       Enter the password for the EEM server EiamAdmin user (Entrez le mot de passe pour l'utilisateur EiamAdmin du serveur EEM)
       Confirm the password for the EEM server EiamAdmin user (Confirmez le mot de passe pour l'utilisateur EiamAdmin du serveur EEM)
       ```

    b. Saisissez le mot de passe que vous souhaitez affecter au superutilisateur par défaut EiamAdmin ; saisissez-le à nouveau.

       ```
       Enter an application name for this CAELM server (CAELM) (Entrez un nom d'application pour ce serveur CA ELM)
       ```

c. Appuyez sur Entrée pour accepter CAELM, le nom d'application par défaut de CA User Activity Reporting Module.

   Les informations sur le serveur EEM que vous avez entrées jusqu'ici apparaissent avec un message vous demandant si vous souhaitez apporter des modifications.



d. Appuyez sur Entrée ou saisissez "n" pour accepter les informations de serveur CA EEM que vous avez entrées.

Le processus d'installation démarre. Des messages indiquent la progression, à mesure de l'installation réussie de chaque composant CA User Activity Reporting Module, des enregistrements effectués, des certificats acquis, des fichiers importés et des composants configurés. Le message d'installation réussie de CA ELM apparaît. Lorsque l'installation se termine, le système affiche l'adresse de connexion de la console.

14. Répondez à la question suivante :

```
Voulez-vous exécuter le serveur CA ELM en mode FIPS ?
Entrez Oui ou Non.
```

    Si vous entrez Oui, le serveur CA User Activity Reporting Module démarrera en mode FIPS. Si vous entrez Non, il démarrera en mode non-FIPS.

15. Notez cette adresse. Il s'agit de l'adresse que vous entrez dans un navigateur pour accéder à ce serveur CA User Activity Reporting Module, soit https://<nom_hôte>:5250/spin/calm.

    Une invite de connexion à <nom_hôte> apparaît. Vous pouvez l'ignorer.

    Remarque : Si, pour quelque raison que ce soit, vous souhaitez afficher l'invite du système d'exploitation à partir de cette invite de connexion, vous pouvez entrer caelmadmin et le mot de passe par défaut, qui est le mot de passe que vous avez affecté au compte de l'utilisateur EiamAdmin. Vous pouvez utiliser le compte caelmadmin pour vous connecter au dispositif, sur la console ou via SSH.

16. Continuez comme suit.
    - Si vous avez configuré une adresse IP statique, veillez à enregistrer cette adresse IP auprès des serveurs DNS spécifiés à l'étape 9.
    - Si vous avez configuré DHCP, mettez à jour votre fichier hosts sur l'ordinateur à partir duquel vous souhaitez naviguer pour atteindre ce serveur.
    - Accédez à l'adresse URL notée à l'étape 14, puis configurez le premier administrateur.

Mise à jour de votre fichier hosts Windows

Lors de l'installation CA User Activity Reporting Module, vous pouvez identifier un ou plusieurs serveurs DNS ou sélectionner l'utilisation de DHCP. Si vous avez sélectionné DHCP, vous devez mettre à jour le fichier hosts Windows, à l'aide de votre navigateur, sur l'ordinateur à partir duquel vous souhaitez accéder à CA User Activity Reporting Module.

Pour mettre à jour votre fichier hosts sur l'hôte avec votre navigateur

1. Ouvrez l'explorateur Windows et accédez à C:\WINDOWS\system32\drivers\etc.
2. Ouvrez le fichier hosts au moyen d'un éditeur, par exemple Bloc-notes.
3. Ajoutez une entrée contenant l'adresse IP du serveur CA User Activity Reporting Module et le nom d'hôte correspondant.
4. Dans le menu Fichier, sélectionnez Enregistrer, puis fermez le fichier.

Configuration du premier administrateur

Après avoir installé CA User Activity Reporting Module avec un seul serveur, pour préparer sa configuration, accédez à l'URL du CA User Activity Reporting Module à partir d'une station de travail distante, connectez-vous et créez un compte d'administrateur que vous pouvez utiliser pour effectuer la configuration.

Remarque : Dans le cadre de ce déploiement rapide, nous acceptons le magasin d'utilisateurs par défaut et les stratégies de mots de passe par défaut. En général, ces éléments sont configurés avant l'ajout du premier administrateur.

Pour configurer le premier administrateur

1. A partir de votre navigateur, connectez-vous à l'URL ci-dessous, où nom_hôte est le nom d'hôte ou l'adresse IP du serveur sur lequel vous avez installé CA User Activity Reporting Module.

   `https://<nom_hôte>:5250/spin/calm`

2. Si une alerte de sécurité survient, procédez comme suit.

   a. Cliquez sur Afficher le certificat.

   b. Cliquez sur Installer le certificat, acceptez les valeurs par défaut, puis terminez l'assistant d'importation.

      Un avertissement de sécurité s'affiche et indique que vous êtes sur le point d'installer un certificat qui déclare représenter le nom d'hôte du serveur CA User Activity Reporting Module.

   c. Cliquez sur Oui.

      Le certificat racine est installé et un message s'affiche indiquant que l'importation s'est correctement terminée.

   d. Cliquez sur OK.

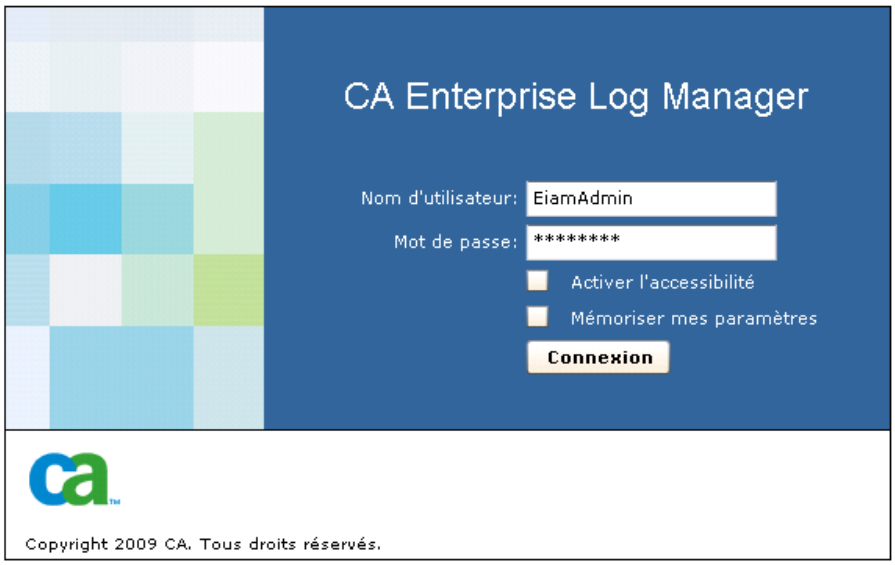
      La boîte de dialogue Certificat fiable s'affiche.

   e. Cliquez sur le chemin de certification et vérifiez que l'état du certificat indique que ce dernier est fiable (facultatif).

   f. Cliquez sur OK, puis sur Oui.

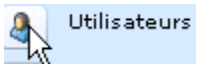
      La page de connexion apparaît.

3. Connectez-vous avec le nom d'utilisateur EiamAdmin et le mot de passe que vous avez créé lorsque vous avez installé le logiciel. Cliquez sur Connexion.

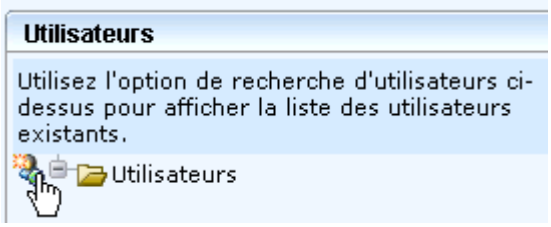


L'application s'ouvre ; seuls l'onglet Administrator et le sous-onglet Gestion des utilisateurs et des accès sont actifs.

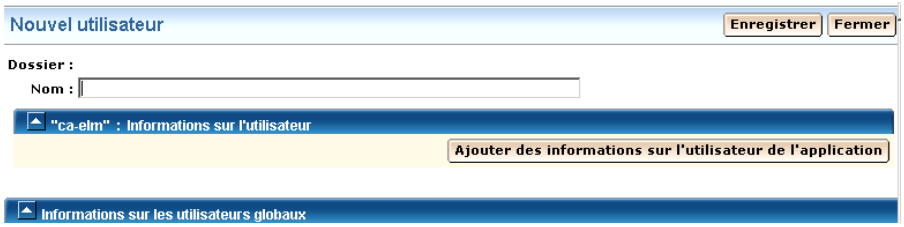
4. Cliquez sur Utilisateurs.



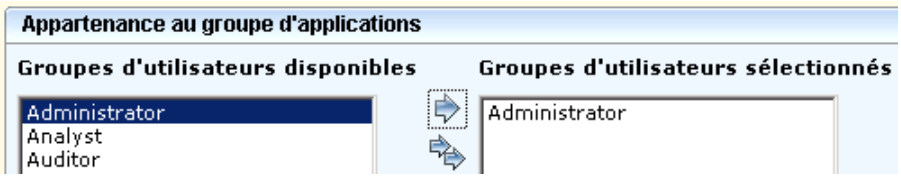
5. Cliquez sur Ajouter un nouvel utilisateur.



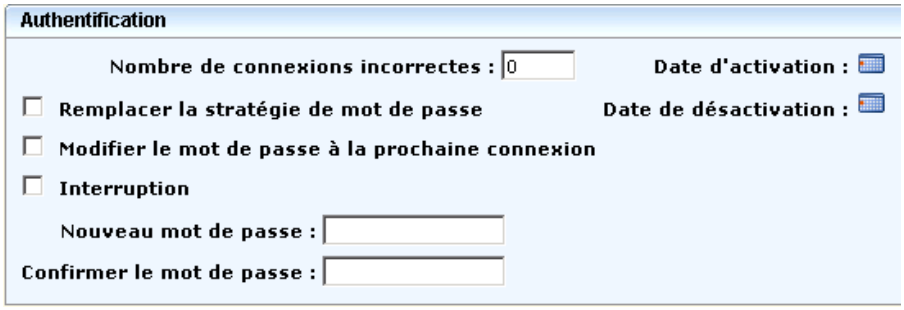
6. Entrez votre nom dans le champ Nom, puis cliquez sur Ajouter les détails de l'utilisateur de l'application.



7. Sélectionnez Administrator, puis placez-le dans la liste Groupes d'utilisateurs sélectionnés.



8. Sous Authentification, entrez un mot de passe pour ce nouveau compte dans le champ d'entrée, puis dans celui de confirmation.



9. Cliquez sur Enregistrer, puis sur Fermer. Cliquez sur Fermer.
10. Cliquez sur le lien Déconnexion de la barre d'outils.

    La page de connexion apparaît.

11. Connectez-vous à nouveau à CA User Activity Reporting Module avec les informations d'identification de l'administrateur que vous venez de définir.

    CA User Activity Reporting Module s'ouvre ; toutes les fonctionnalités sont activées. L'onglet Requêtes et rapports et le sous-onglet Requêtes sont affichés.

12. Affichez vos tentatives de connexion comme suit (facultatif).

    a. Dans la liste de balises de requête, sélectionnez Accès au système.

    b. Dans la liste de requêtes, sélectionnez Détail d'accès au système.

    Les résultats de la requête présentent vos deux tentatives de connexion, tout d'abord en tant qu'EiamAdmin, puis avec votre nom d'administrateur ; les tentatives de connexion sont marquées S pour successful (réussie).

Sévérité CA	Date	Compte	Exécutant	Hôte	Nom du jo...	Catégorie	Action	Résultat
Informations	Ven. 13 nov. 2009 5:33:26		-	SONMI02G2	NT-Security	System Access	Login Attempt	S
Informations	Ven. 13 nov. 2009 5:33:26	ANONYMOUS LOGON		SONMI02G2	NT-Security	System Access	Logoff	S
Informations	Ven. 13 nov. 2009 5:33:24	ANONYMOUS LOGON		SONMI02G2	NT-Security	System Access	Logoff	S
Informations	Ven. 13 nov. 2009 5:33:24		-	SONMI02G2	NT-Security	System Access	Login Attempt	S

Configuration des sources d'événement Syslog

Pour permettre à l'agent par défaut situé sur chaque serveur CA User Activity Reporting Module de collecter directement des événements Syslog, vous devez tout d'abord identifier les sources de ces événements, puis déterminer leur intégration associée. Vous pouvez ensuite effectuer les deux opérations suivantes dans l'ordre de votre choix.

- Configurez les sources d'événement Syslog. Connectez-vous à chaque hôte exécutant une source d'événement Syslog, puis configurez celle-ci conformément au manuel du connecteur de cette intégration Syslog.
- Configurez le connecteur Syslog sur l'agent par défaut afin d'ajouter les intégrations Syslog cibles associées aux sources d'événement configurées.

Dès que vous avez terminé ces deux étapes de configuration, la collecte et l'ajustement des événements commence. Vous pouvez ensuite utiliser CA User Activity Reporting Module pour afficher les événements qui vous intéressent ou générer des rapports à leur sujet, sous un format standardisé. Vous pouvez également générer des alertes lorsque des événements précis surviennent.

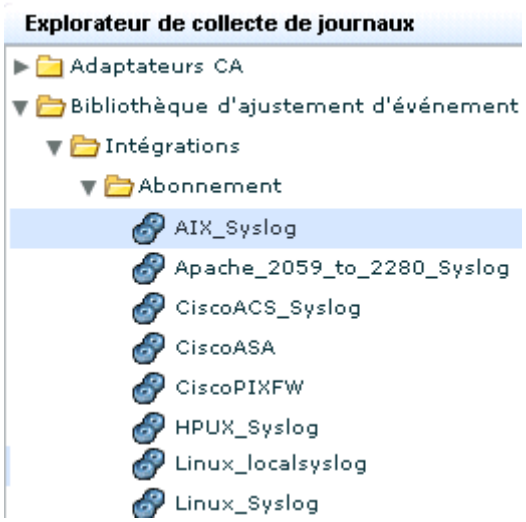
Pour configurer une source d'événement Syslog sélectionné

1. Connectez-vous à l'hôte sur lequel se trouve la source d'événement Syslog cible.
2. A partir d'un navigateur, lancez CA User Activity Reporting Module sur cet hôte.
3. Cliquez sur l'onglet Administration, puis sur le sous-onglet Collecte de journaux.

   L'explorateur de collecte de journaux s'affiche.

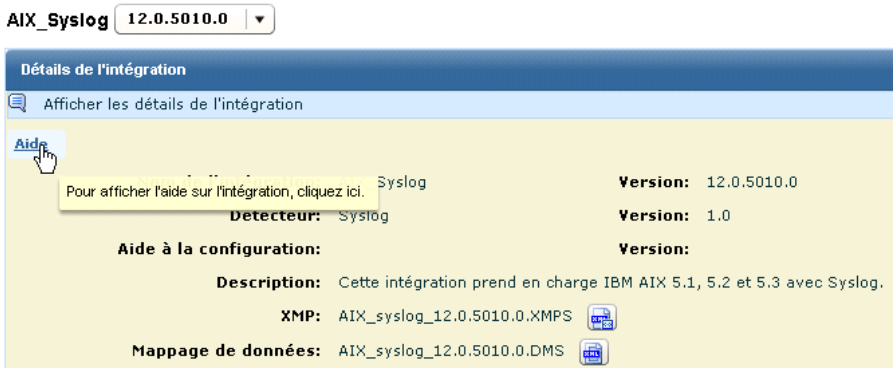
4. Développez Bibliothèque d'ajustement d'événement, Intégrations, Abonnement.

   La liste des intégrations prédéfinies s'affiche. Un exemple abrégé est présenté ci-dessous.



5. Sélectionnez l'intégration de la source d'événement que vous souhaitez configurer. Par exemple, si vous souhaitez collecter des Syslogs générés par un système d'exploitation AIX, vous devez sélectionner AIX_Syslog.

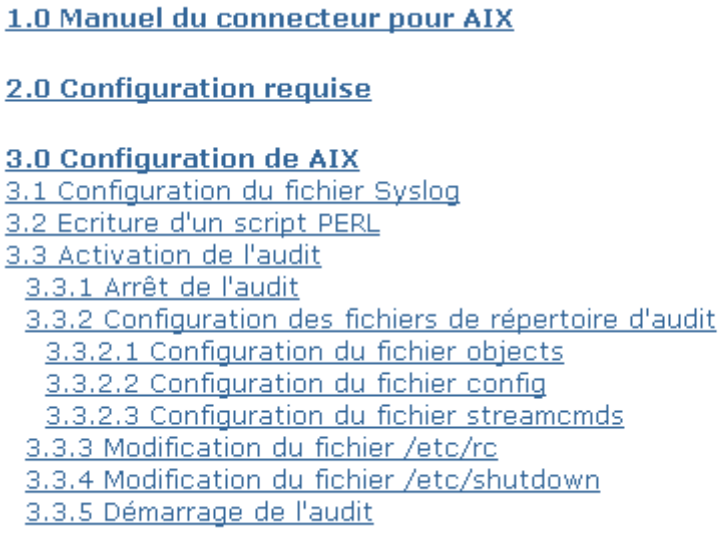
   Les détails de l'intégration apparaissent.



6. Cliquez sur le bouton Aide situé juste au-dessus du nom de l'intégration dans le volet droit.

   Le manuel du connecteur pour l'intégration sélectionnée apparaît.

7. Cliquez sur la section relative à la configuration requise par la source d'événement. Dans cet exemple, la documentation décrit la configuration de la source d'événement du système d'exploitation AIX pour envoyer ses Syslogs à CA User Activity Reporting Module.



Exemple d'une autre source de manuels de connecteurs : le support en ligne

Vous pouvez ouvrir un manuel de connecteur sélectionné à partir de l'interface utilisateur CA User Activity Reporting Module ou du support en ligne de CA. L'exemple ci-dessous présente l'ouverture d'un manuel de connecteur à partir de cette autre possibilité.

1. Connectez-vous au support en ligne de CA.
2. Sélectionnez CA Enterprise Log Manager dans la liste déroulante de sélection d'une page de produit.
3. Faites défilez jusqu'à l'état du produit et sélectionnez la matrice de certification de CA Enterprise Log Manager.
4. Sélectionnez la matrice d'intégration du produit.
5. Recherchez la catégorie de l'intégration associée à la source d'événement que vous configurez. Par exemple, si la source d'événement est le système d'exploitation AIX, faites défiler jusqu'à la catégorie des systèmes d'exploitation, puis cliquez sur le lien AIX.

Produit	Version	Journal Sensor
Systèmes d'exploitation		
AIX	5.1 5.2 5.3	syslog

Modification du connecteur Syslog

Chaque CA User Activity Reporting Module comporte un agent par défaut. Lorsque CA User Activity Reporting Module est installé, son agent par défaut comporte un connecteur partiellement configuré appelé Syslog_Connector, basé sur l'écouteur Syslog. Cet écouteur reçoit des événements Syslog bruts sur les ports par défaut, dès que vous configurez les sources d'événement pour envoyer des Syslogs à CA User Activity Reporting Module. Toutefois, si vous souhaitez que CA User Activity Reporting Module ajuste ces événements bruts, vous devez modifier ce Syslog_Connector. Certaines modifications sont obligatoires et d'autres facultatives.

- Vous devez identifier les cibles Syslog lorsque vous modifiez ce connecteur. Vous sélectionnez en tant que cibles Syslog chaque intégration correspondant à une ou plusieurs sources d'événement configurées ou prévues. Votre identification de cibles Syslog permet à CA User Activity Reporting Module d'ajuster ces événements correctement.
- Si vous le souhaitez, vous pouvez appliquer des règles de suppression, limiter l'acceptation de Syslogs à des hôtes de confiance, spécifier les ports à écouter autres que 514 (port UDP Syslog réservé) et 1468 (port TCP par défaut), et/ou ajouter un nouveau fuseau horaire pour un hôte fiable.

Pour modifier le connecteur Syslog d'un agent par défaut

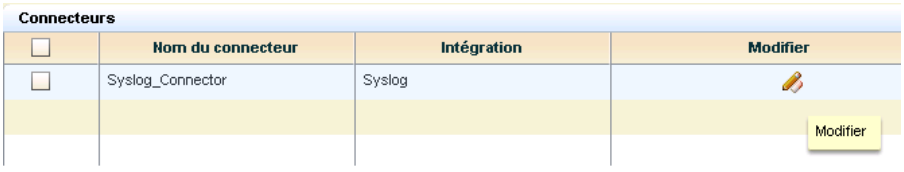
1. Cliquez sur l'onglet Administration.

   Le sous-onglet Collecte de journaux s'affiche.

2. Développez l'Explorateur d'agent, puis le groupe d'agents par défaut ou le groupe défini par l'utilisateur comportant CA User Activity Reporting Module à configurer.

3. Sélectionnez le nom d'un serveur CA User Activity Reporting Module.

   Le connecteur appelé Syslog_Connector s'affiche.



4. Cliquez sur Modifier.

   L'assistant de modification d'un connecteur apparaît ; l'étape Détails du connecteur est sélectionnée.

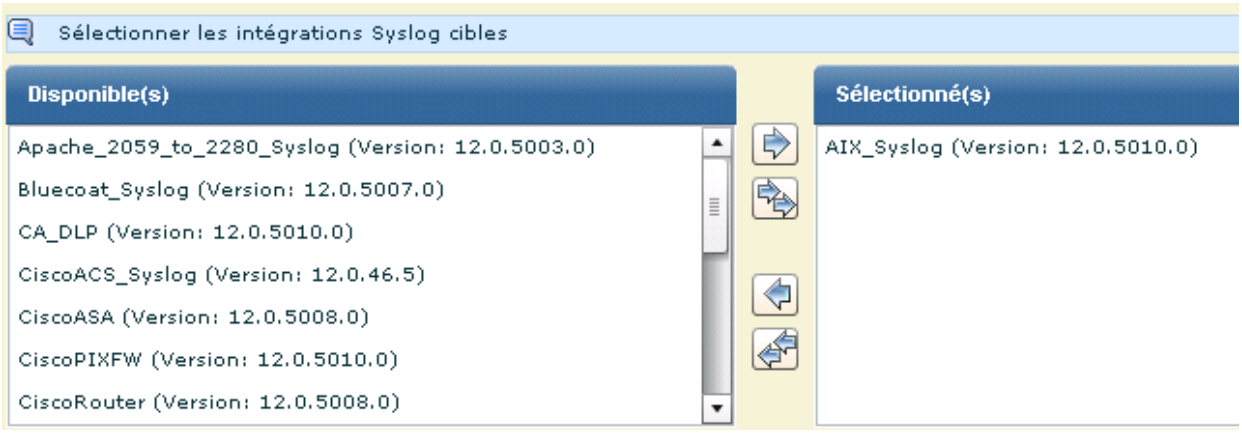
5. Cliquez sur Appliquer les règles de suppression (facultatif). Si vous souhaitez supprimer un type d'événement Syslog, c'est-à-dire si vous souhaitez qu'il ne soit *pas* collecté, faites-le passer de la liste Disponible(s) à la liste Sélectionné(s). Sélectionnez l'événement à déplacer, puis cliquez sur le bouton Déplacer.

6. Cliquez sur l'étape Configuration du connecteur.

   Toutes les intégrations disponibles sont sélectionnées par défaut.

7. Sélectionnez les cibles Syslog en faisant passer les intégrations Syslog à cibler de la liste Disponible(s) à la liste Sélectionné(s).

   Par exemple, si vous avez configuré le système d'exploitation AIX sur un hôte de votre réseau, vous faites passer la cible Syslog, AIX_Syslog, de la liste Disponible(s) à la liste Sélectionné(s).



8. Identifiez les hôtes fiables d'où proviennent les événements entrants acceptés par le connecteur Syslog (facultatif). Entrez l'adresse IP dans le champ d'entrée, puis cliquez sur Ajouter. Répétez cette procédure pour chaque hôte fiable. Tout événement reçu d'un hôte non configuré comme fiable est alors rejeté.

   Remarque : Il est recommandé de configurer des hôtes fiables. En général, vous configurez tous les hôtes sur lesquels vous avez établi des sources d'événement pour envoyer des Syslogs à CA User Activity Reporting Module. La spécification d'hôtes fiables assure que l'agent par défaut refuse les événements provenant de systèmes non autorisés qu'un attaquant a configurés pour envoyer des événements à l'écouteur Syslog.

9. Ajoutez des ports (facultatif).

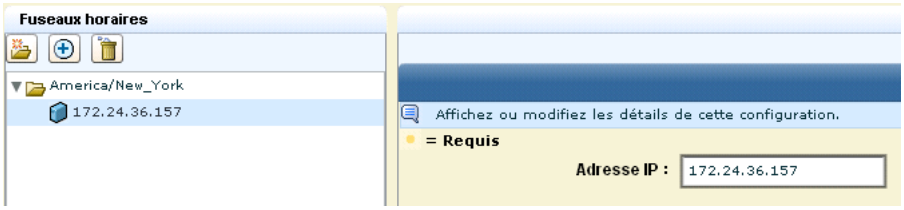
   En général, vous acceptez les ports UDP et TCP par défaut pour l'agent par défaut.

   Remarque : Vous pouvez améliorer les performances en définissant un connecteur Syslog pour différents types d'événements et en spécifiant un port différent pour chaque connecteur. Veillez à sélectionner des ports non utilisés lorsque vous affectez de nouveaux ports.

10. Ajoutez un fuseau horaire uniquement si vous collectez des Syslogs provenant d'ordinateurs situés dans un fuseau horaire différent de celui du dispositif logiciel (facultatif).

    a. Cliquez sur Créer un dossier, puis développez le dossier.

    b. Mettez en surbrillance l'entrée vide située sous le dossier. Entrez l'adresse IP d'un hôte fiable que vous avez configuré pour ce connecteur ou celle du serveur de synchronisation NTP que vous avez spécifié lors de l'installation de CA User Activity Reporting Module.



11. Cliquez sur Enregistrer et fermer.

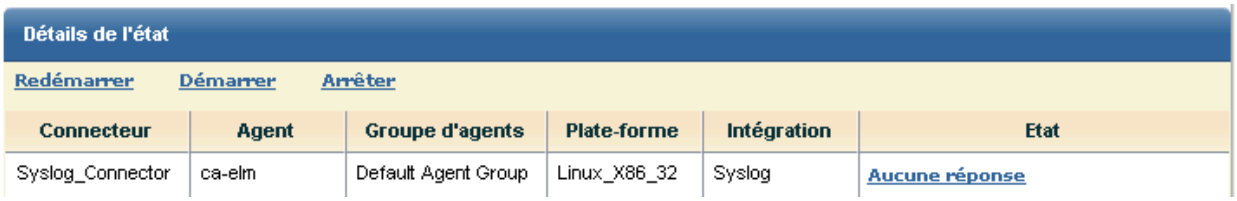
12. Affichez l'état.

    a. Cliquez sur Etat et commande.

Afficher l'état des agents est sélectionné. Comme l'agent par défaut se trouve sur ce serveur, le nom d'hôte du serveur que vous avez installé apparaît dans la colonne Agent. L'état affiché est Exécution en cours.

b. Cliquez sur le lien Exécution en cours pour afficher les détails.

c. Cliquez sur le bouton Connecteurs pour afficher l'état des connecteurs.



d. Cliquez sur le lien Exécution en cours.

Le pourcentage d'UC, l'utilisation de la mémoire, le nombre moyen d'événements par secondes et le nombre d'événements filtrés apparaissent.

Affichage d'événements Syslog

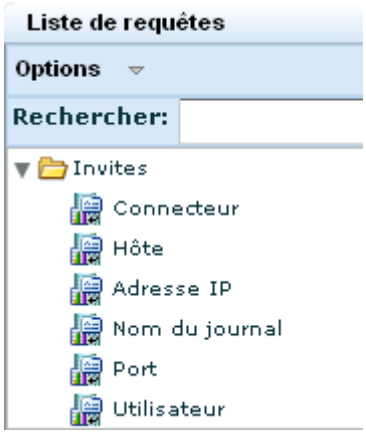
Pour afficher rapidement les résultats d'une requête sur des événements collectés par un écouteur Syslog, utilisez l'invite Hôte.

Pour afficher des événements Syslog

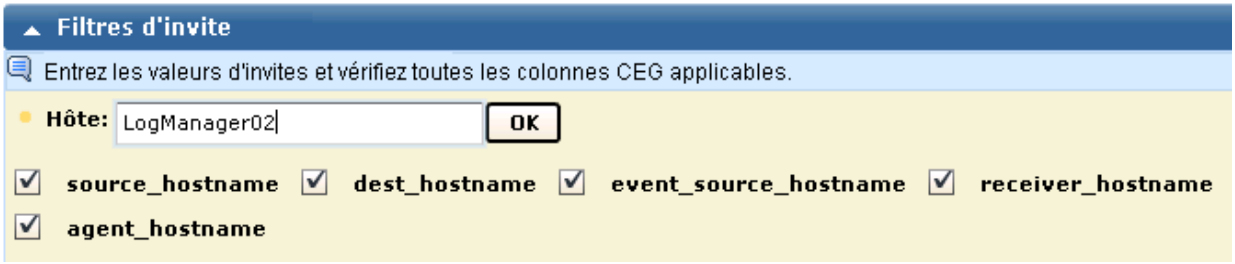
1. Sélectionnez l'onglet Requêtes et rapports.

   Le sous-onglet Requêtes s'affiche.

2. Développez Invites sous Liste de requêtes, puis sélectionnez Hôte.



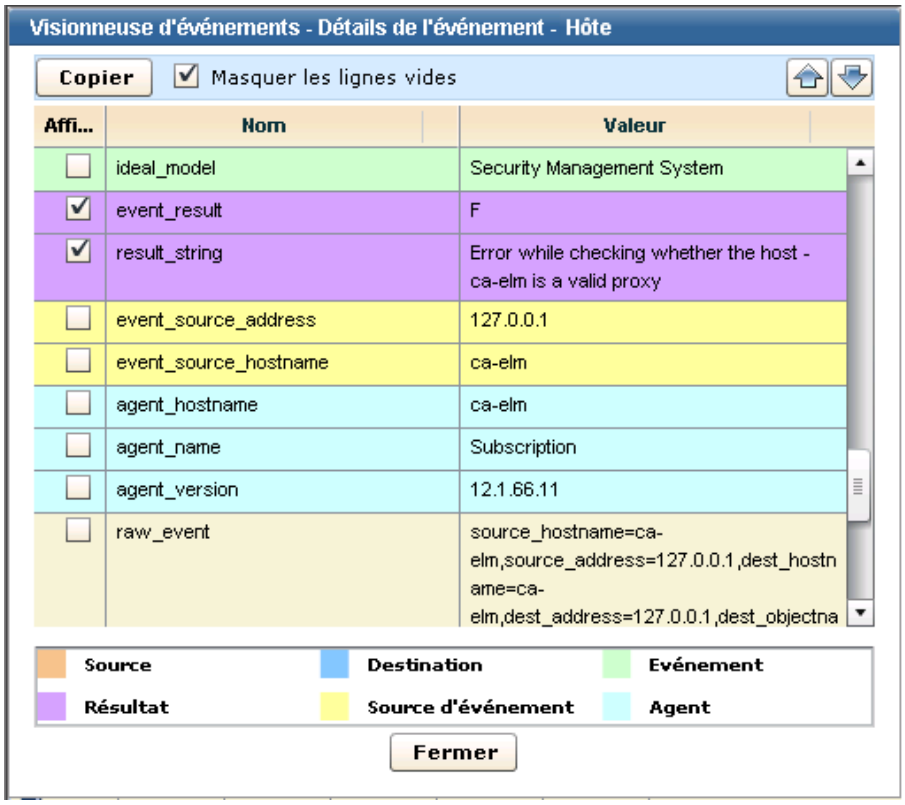
3. Soumettez une requête pour les événements collectés par l'agent par défaut.
   a. Dans le champ Hôte, entrez le nom d'hôte de l'agent par défaut ; il s'agit également du nom du CA User Activity Reporting Module sur lequel il réside.
   b. Sélectionnez agent_hostname.
   c. Cliquez sur OK.



4. Affichez les résultats à examiner.
   a. Pour trier par résultats, cliquez sur la colonne Résultats.
   b. Faites défiler jusqu'au premier résultat F pour failure (échec). Supposez qu'il s'agit d'un avertissement de configuration de la catégorie Gestion de la configuration.
   c. Double-cliquez pour sélectionner la ligne à afficher en détail.

   La visionneuse d'événements apparaît.

5. Faites défiler jusqu'à la zone d'affichage du résultat. Dans cet exemple, l'erreur est un avertissement vous indiquant que vous devez configurer le module d'abonnement. Il s'agit d'un avertissement que vous devez ignorer jusqu'à la fin de l'installation de tous les serveurs CA User Activity Reporting Module souhaités.



Chapitre 3 : Déploiement de l'agent Windows

Ce chapitre traite des sujets suivants :

Création d'un compte d'utilisateur pour l'agent

Avant d'installer un agent sous Windows, vous devez créer un nouveau compte pour l'agent dans le dossier Utilisateurs de Windows. Ce compte avec peu de droits permet à l'agent de s'exécuter avec le moins de droits possibles. Lorsque vous installez l'agent, vous devez fournir le nom d'utilisateur et le mot de passe que vous avez créés ici.

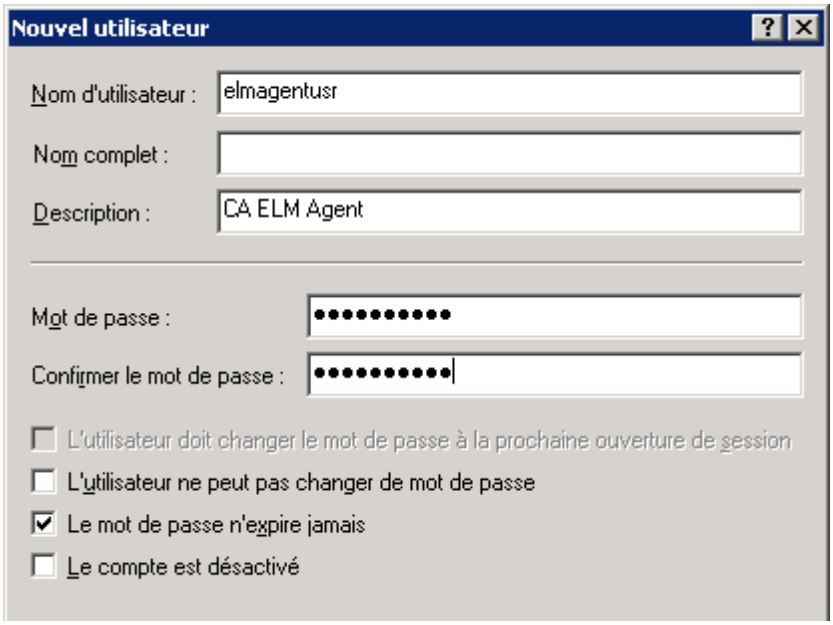
Remarque : Vous pouvez omettre cette étape et spécifier les informations d'identification du domaine d'un administrateur pour l'agent lorsque vous installez ce dernier, mais cela n'est pas recommandé.

Pour créer un compte d'utilisateur Windows pour l'agent

1. Connectez-vous à l'hôte sur lequel vous souhaitez installer l'agent. Utilisez les informations d'identification de l'administrateur.
2. Cliquez sur Démarrer, Programmes, Outils d'administration, Gestion de l'ordinateur.
3. Développez Utilisateurs et groupes locaux.
4. Cliquez avec le bouton droit sur Utilisateurs et sélectionnez Nouvel utilisateur.

   La boîte de dialogue Windows Nouvel utilisateur apparaît.
5. Entrez un nom d'utilisateur, puis entrez deux fois un mot de passe. Un mot de passe sûr comporte une combinaison de caractères alphabétiques, numériques et spéciaux. Par exemple agent_calmr12. Saisissez une description (facultatif).

   Important : N'oubliez pas ce nom et ce mot de passe, ou notez-les. Vous en aurez besoin lorsque vous installerez l'agent.



6. Cliquez sur Créer. Cliquez sur Fermer.

Informations complémentaires :

Installation d'un agent (page 40)

Définition de la clé d'authentification d'un agent

Avant d'installer le premier agent, vous devez connaître la clé d'authentification de celui-ci. Vous pouvez utiliser la valeur par défaut, si aucune clé n'a été définie, utiliser la clé en cours, si elle est définie, ou définir une nouvelle clé. La clé d'authentification de l'agent configurée ici doit être entrée lors de l'installation de chaque agent. Seul un administrateur peut effectuer cette tâche.

Pour définir la clé d'authentification d'un agent

1. Ouvrez le navigateur sur l'hôte où vous souhaitez installer l'agent, puis entrez l'URL du serveur CA User Activity Reporting Module pour cet agent. Voici un exemple.

   `https://<adresse_IP>:5250/spin/calm/`

2. Connectez-vous à CA User Activity Reporting Module. Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur Se connecter.
3. Cliquez sur l'onglet Administration.

   L'explorateur de collecte de journaux s'affiche dans le volet gauche.
4. Sélectionnez le dossier de l'Explorateur d'agent.

   Une barre d'outil apparaît dans le volet principal.
5. Cliquez sur Clé d'authentification d'agent.

6. Entrez la clé d'authentification à utiliser pour l'installation de l'agent ou prenez note de l'entrée actuelle.

   Important : N'oubliez pas cette clé ou notez sa valeur. Vous en aurez besoin pour installer l'agent.

7. Cliquez sur Enregistrer.
8. Passez à l'étape suivante, Téléchargement du programme d'installation de l'agent.

Téléchargement du programme d'installation de l'agent

Si vous venez de définir la clé d'authentification de l'agent, vous êtes prêt à télécharger le programme d'installation de l'agent sur le bureau.

Pour télécharger le programme d'installation de l'agent

1. Dans la barre d'outils affichée pour l'Explorateur d'agent, cliquez sur Télécharger des fichiers binaires d'agent.

Des liens vers les fichiers binaires d'agents disponibles apparaissent dans le volet principal.

2. Cliquez sur le lien Windows pour installer l'agent sur un serveur exécutant le système d'exploitation Windows Server 2003.

La boîte de dialogue Sélection de l'emplacement de téléchargement par <adresse IP> apparaît.

3. Sélectionnez le bureau, puis cliquez sur Enregistrer.

Un message indiquant la progression du téléchargement du fichier binaire d'agent sélectionné apparaît, suivi d'un message de confirmation.

4. Cliquez sur OK.
5. Réduisez le navigateur mais laissez la connexion ouverte, afin de pouvoir vérifier rapidement l'installation une fois celle-ci terminée.

   Le lanceur du programme d'installation de l'agent apparaît sur le bureau.

Installation d'un agent

Avant de commencer, gardez à disposition les informations ci-dessous.

- Adresse IP du serveur CA User Activity Reporting Module à partir duquel vous avez téléchargé le programme de l'agent
- Nom et mot de passe du compte d'utilisateur que vous avez créé pour l'agent
- Clé d'authentification de l'agent que vous avez définie

Pour installer un agent destiné à un hôte Windows

1. Double-cliquez sur le lanceur de l'installation de l'agent.

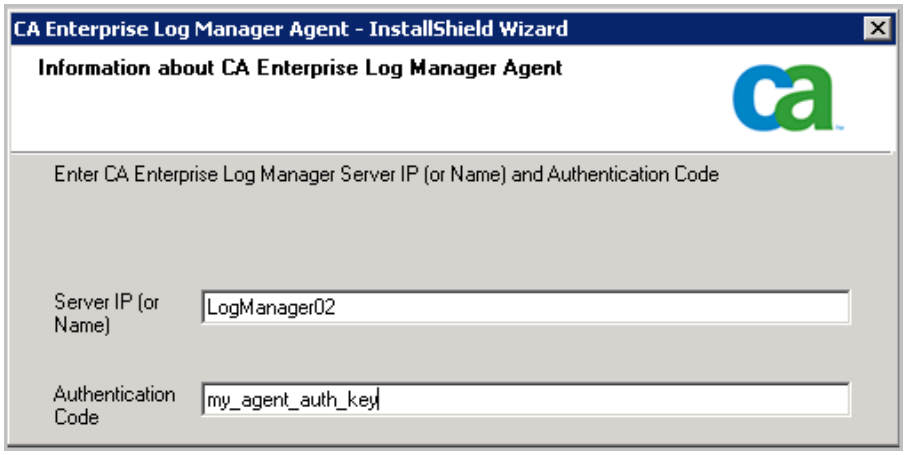
L'assistant d'installation démarre.

2. Cliquez sur Suivant, lisez la licence, cliquez sur J'accepte les termes des contrats de licence pour continuer, puis cliquez sur Suivant.
3. Acceptez le chemin d'installation ou modifiez-le, puis cliquez sur Suivant.
4. Entrez les informations requises, comme suit.
   a. Entrez le nom d'hôte du CA User Activity Reporting Module auquel cet agent doit transférer les journaux qu'il collecte.

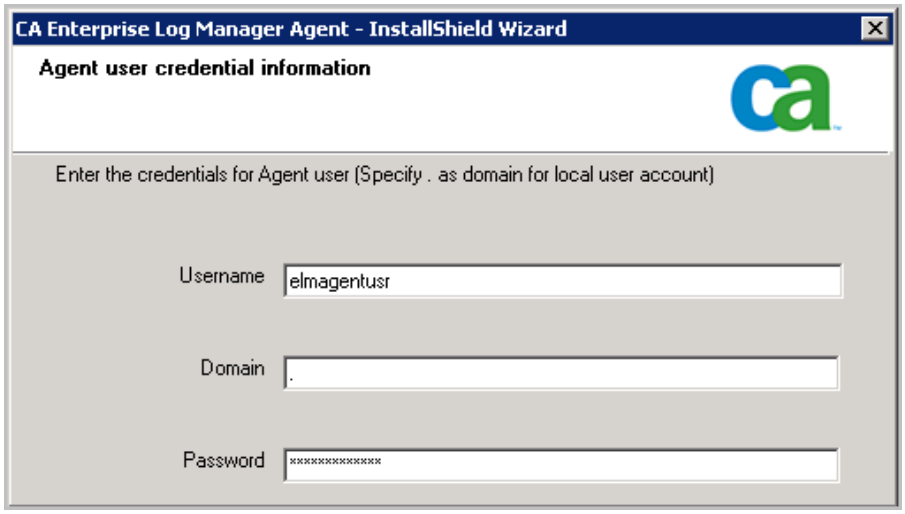
      Remarque : Comme CA User Activity Reporting Module de cet exemple de scénario utilise DHCP pour l'affectation des adresses IP, vous ne devez pas entrer d'adresse IP ici ; en effet, en cas de changement ultérieur de l'adresse IP du serveur, vous risqueriez de devoir réinstaller l'agent.

   b. Entrez la clé d'authentification de l'agent.

   Voici un exemple.



5. Entrez le nom et mot de passe du compte d'utilisateur que vous avez configuré pour l'agent, puis cliquez sur Suivant.



6. Cliquez sur Suivant. La spécification d'un fichier de connecteur exporté est facultative.

   La page Lancer la copie des fichiers apparaît.

7. Cliquez sur Suivant.

   Le processus d'installation de l'agent prend fin.

8. Cliquez sur Terminer.

9. Vous devez ensuite configurer des connecteurs pour cet agent.

   Une fois les connecteurs configurés, les événements collectés sont envoyés au magasin de journaux d'événements CA User Activity Reporting Module via le port 17001.

   Important : Si vous n'autorisez pas de trafic sortant à partir de l'hôte sur lequel vous avez installé l'agent et si vous utilisez le pare-feu Windows, vous devez ouvrir ce port sur ce pare-feu.

Informations complémentaires :

Téléchargement du programme d'installation de l'agent (page 39)
Création d'un compte d'utilisateur pour l'agent (page 36)
Définition de la clé d'authentification d'un agent (page 38)

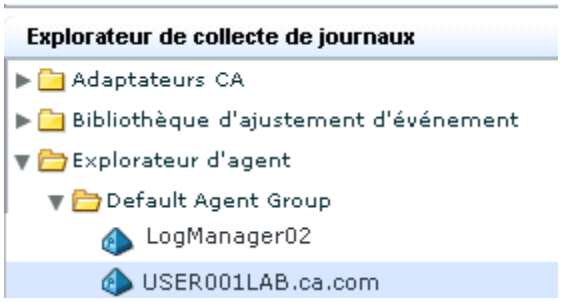
Création d'un connecteur basé sur NTEventLog

Après avoir installé un agent, vous créez un connecteur pour spécifier les sources des événements que vous souhaitez collecter. Votre agent étant installé sur un serveur Windows, vous devez créer un connecteur basé sur l'intégration NTEventLog et spécifier les paramètres du WMILogSensor, comme décrit dans le manuel du connecteur que vous ouvrez à partir de l'assistant de création d'un connecteur. Spécifiez le nom de l'hôte sur lequel l'agent est installé pour la collecte de journaux avec agent. Si vous le souhaitez, vous pouvez ajouter un autre détecteur de journaux WMI pour ce connecteur et spécifier un autre hôte que celui sur lequel l'agent est installé. Cela permet la collecte de journaux sans agent. Le ou les hôtes supplémentaires doivent se trouver dans le même domaine et disposer du même administrateur Windows que le premier hôte que vous avez ajouté.

Pour configurer un connecteur basé sur NTEventLog

1. Agrandissez votre navigateur affichant l'Explorateur d'agent CA User Activity Reporting Module.
2. Développez l'Explorateur d'agent, puis le groupe d'agents par défaut.

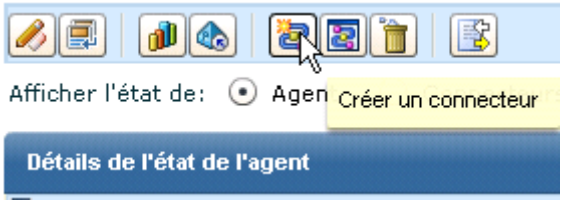
   Le nom de l'ordinateur sur lequel vous avez installé l'agent apparaît.



3. Sélectionnez cet agent.

   Le volet Connecteurs de l'agent apparaît.

4. Cliquez sur Créer un connecteur.

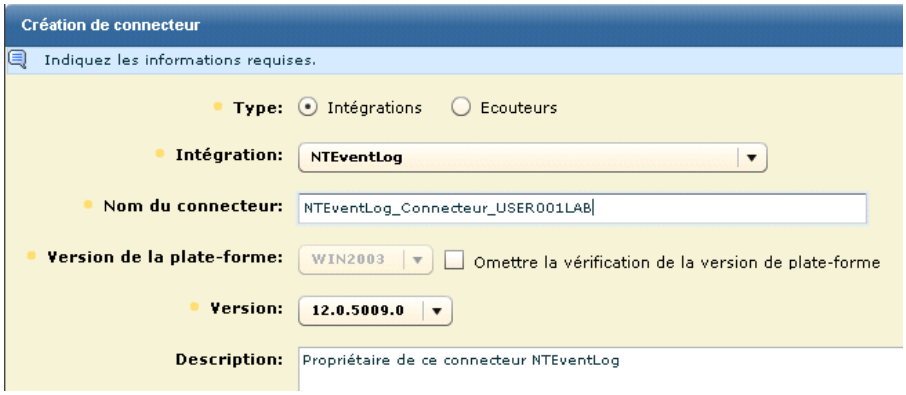


   L'assistant de création d'un connecteur apparaît ; l'étape Détails du connecteur est sélectionnée.

5. Laissez Intégrations sélectionné, puis sélectionnez NTEventLog dans la liste déroulante Intégration.

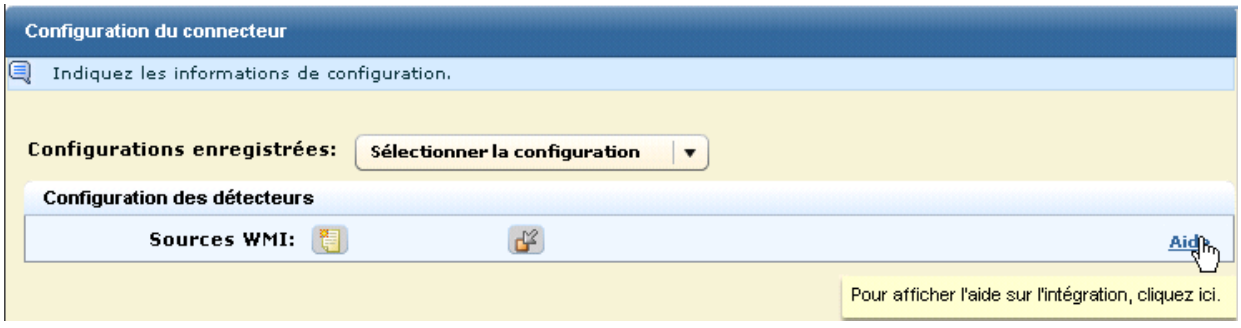
   Les champs Nom du connecteur et Description sont remplis selon la sélection effectuée dans Intégration.

6. Modifiez le nom du connecteur afin d'obtenir un nom unique. Vous pouvez envisager de compléter ce nom par le nom du serveur cible, par exemple NTEventLog_Connector_USER001LAB.

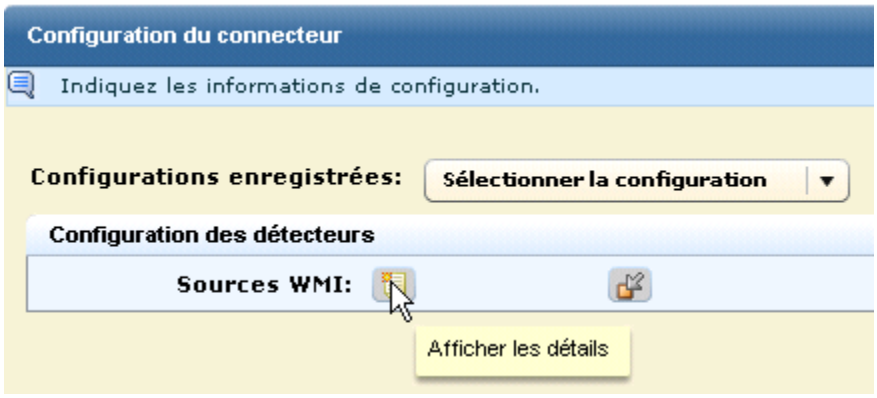


7. Sélectionnez l'étape Configuration du connecteur.

Le volet Configuration des détecteurs apparaît ; un bouton Aide permet d'accéder au manuel du connecteur NTEventLog qui décrit les champs de configuration du détecteur.



8. Cliquez sur le bouton Afficher les détails pour les sources WMI.



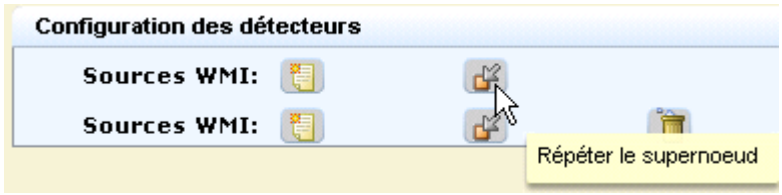
9. Configurez les paramètres WMILogSensor pour l'ordinateur local de collecte de journaux avec agent. Pour plus de détails, cliquez sur le lien Aide.

   Les exemples ci-après présentent une configuration où l'utilisateur est un administrateur Windows sur le serveur WMI spécifié. Le domaine est défini pour le serveur WMI.

10. Configurez un détecteur WMI pour un autre ordinateur, pour une collecte de journaux sans agent utilisant ce même connecteur (facultatif).

    a. Cliquez sur le bouton Répéter le supernoeud.

       L'illustration suivante présente une configuration comportant deux sources WMI.



b. Configurez les paramètres WMILogSensor pour un autre ordinateur.

L'exemple ci-après présente une configuration pour un deuxième détecteur de journaux WMI dans le même domaine et avec les mêmes informations d'identification d'administrateur.

11. Cliquez sur Enregistrer et fermer.
12. Pour afficher l'état du connecteur que vous avez configuré, procédez comme suit.
    a. Sélectionnez l'agent dans le volet gauche.
    b. Cliquez sur Etat et commande.
    c. Sélectionnez Afficher l'état des connecteurs.

    Le volet Détails de l'état apparaît.

13. Cliquez sur le lien Exécution en cours.

    L'état affiché de la cible configurée dans le connecteur inclut le pourcentage d'UC, l'utilisation de la mémoire et le nombre moyen d'événements par seconde.

Configuration d'une source d'événement Windows

Après avoir configuré un connecteur à l'aide de l'intégration NTEventLog sur l'agent, vous devez pouvoir consulter des événements au moyen de la visionneuse d'événements. Si des événements ne sont pas transférés à votre visionneuse, vous devez modifier les paramètres Windows de vos stratégies locales sur la source d'événement.

Pour configurer des stratégies locales sur la source d'événement d'un connecteur NTEventLog

1. Si l'explorateur de collecte de journaux n'est pas déjà affiché, cliquez sur l'onglet Administration.
2. Développez Bibliothèque d'ajustement d'événement, Intégrations, Abonnement, puis sélectionnez NTEventLog et cliquez sur le lien Aide situé au-dessus du nom de l'intégration dans le volet Afficher les détails de l'intégration.

   Le manuel du connecteur pour le journal d'événements NT (sécurité, application, système) apparaît.
3. Réduisez l'interface utilisateur CA User Activity Reporting Module, puis suivez les indications du manuel du connecteur pour modifier les stratégies locales sur une source d'événement s'exécutant sous Windows.

   Remarque : Si vous utilisez Windows Server 2003, sélectionnez Panneau de configuration, Outils d'administration, Stratégie de sécurité locale, puis développez Stratégies locales.
4. Si vous avez configuré un détecteur WMI pour un second serveur WMI, modifiez également les stratégies locales de ce serveur (facultatif).
5. Agrandissez CA User Activity Reporting Module.

Affichage de journaux à partir de sources d'événement Windows

Pour afficher rapidement les résultats d'une requête sur des événements collectés par un écouteur Syslog, utilisez l'invite Hôte. Vous pouvez également sélectionner des requêtes ou des rapports.

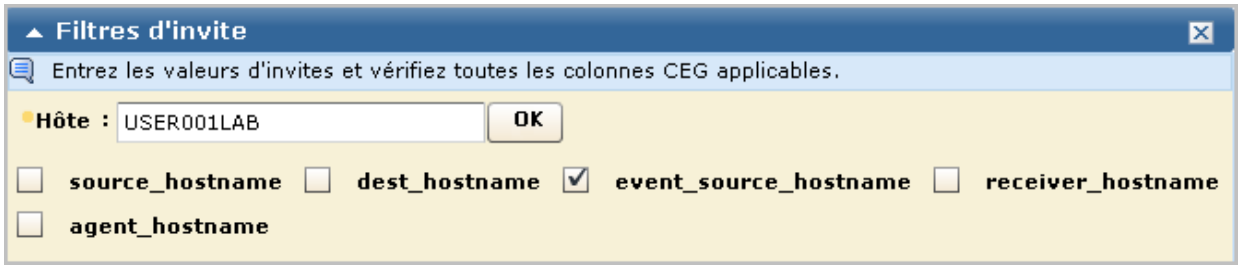
Pour afficher les journaux d'événements entrants

1. Sélectionnez l'onglet Requêtes et rapports.

   Le sous-onglet Requêtes s'affiche.

2. Développez Invites sous Liste de requêtes, puis sélectionnez Hôte.

3. Dans le champ Hôte, entrez le nom du serveur WMI configuré pour le détecteur. Désélectionnez les autres cases, puis cliquez sur OK.



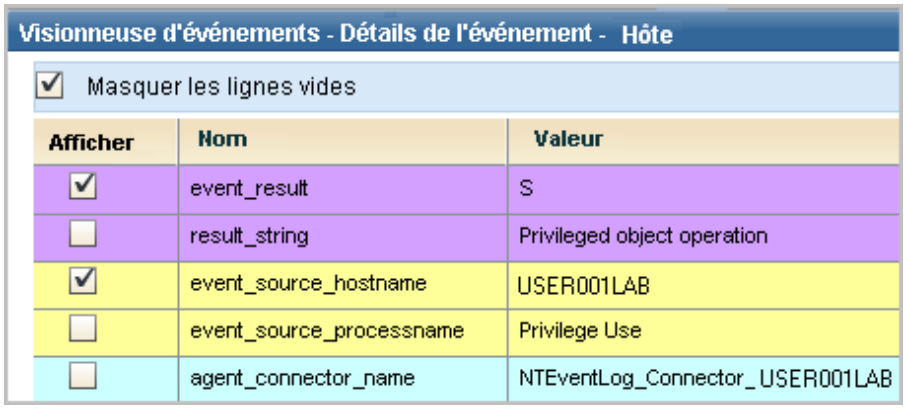
   Les événements provenant des sources d'événement du serveur WMI apparaissent.

4. Cliquez sur Sévérité CA, puis faites défiler pour rechercher un avertissement. L'exemple ci-dessous est compressé, sans les colonnes Date et Source d'événement.

Sévérité CA ▼	Utilisateur de	Résultat	Catégorie	Action	Nom du journal
Warning	calm_agent	S	System Access	Privilege Use	NT-Security

5. Cliquez sur Afficher les événements bruts pour afficher les événements bruts de l'avertissement.

6. Double-cliquez sur l'avertissement pour afficher la visionneuse d'événements avec beaucoup plus de données. Quelques lignes d'exemples de données sont affichées ci-dessous.

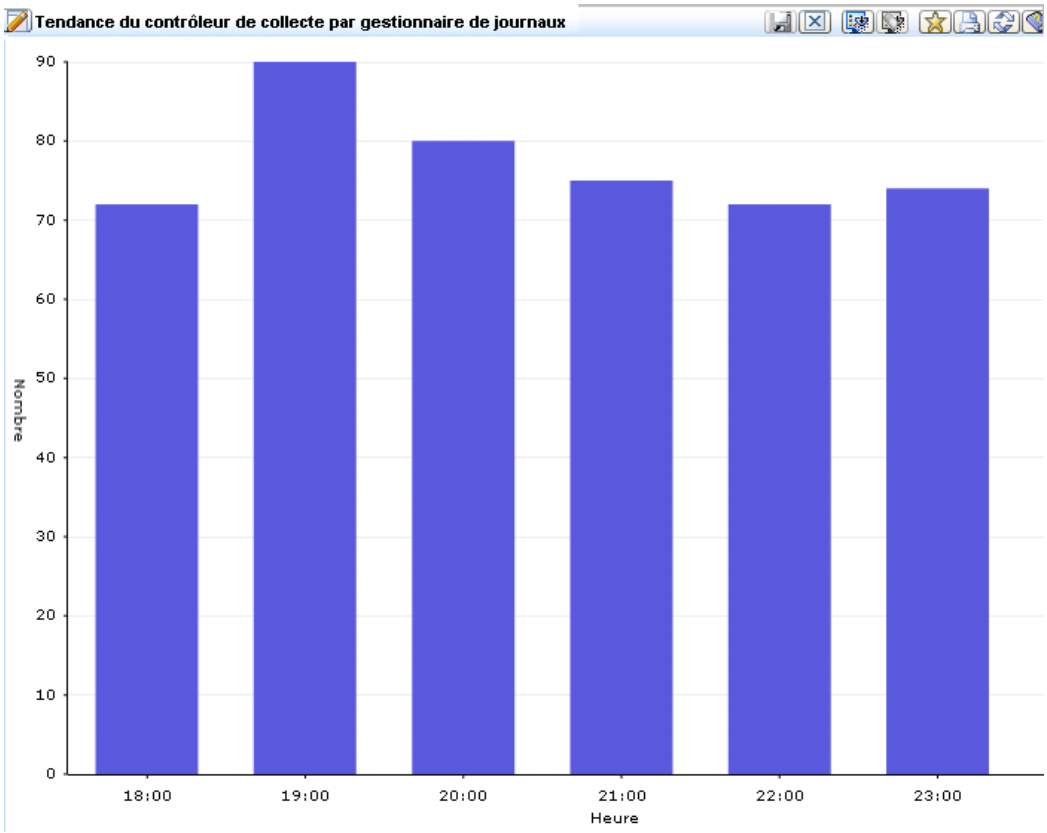


Visionneuse d'événements - Détails de l'événement - Hôte

Masquer les lignes vides

Afficher	Nom	Valeur
☑	event_result	S
☐	result_string	Privileged object operation
☑	event_source_hostname	USER001LAB
☐	event_source_processname	Privilege Use
☐	agent_connector_name	NTEventLog_Connector_USER001LAB

7. Cliquez sur l'onglet Requêtes et rapports, cliquez sur une requête de la liste de requêtes, par exemple Tendance du contrôleur de collecte par gestionnaire de journaux. Affichez le graphique à barres des résultats.



8. Cliquez sur Rapports. Sous Liste de rapports, entrez auto dans le champ Rechercher, afin d'afficher le nom du rapport Evénements d'autosurveillance du système. Sélectionnez ce rapport pour afficher une liste des événements générés par le serveur CA User Activity Reporting Module.

Remarque : Pour obtenir des détails concernant la planification de rapports sur les informations que vous souhaitez analyser, consultez l'aide en ligne ou le *Manuel d'administration*.

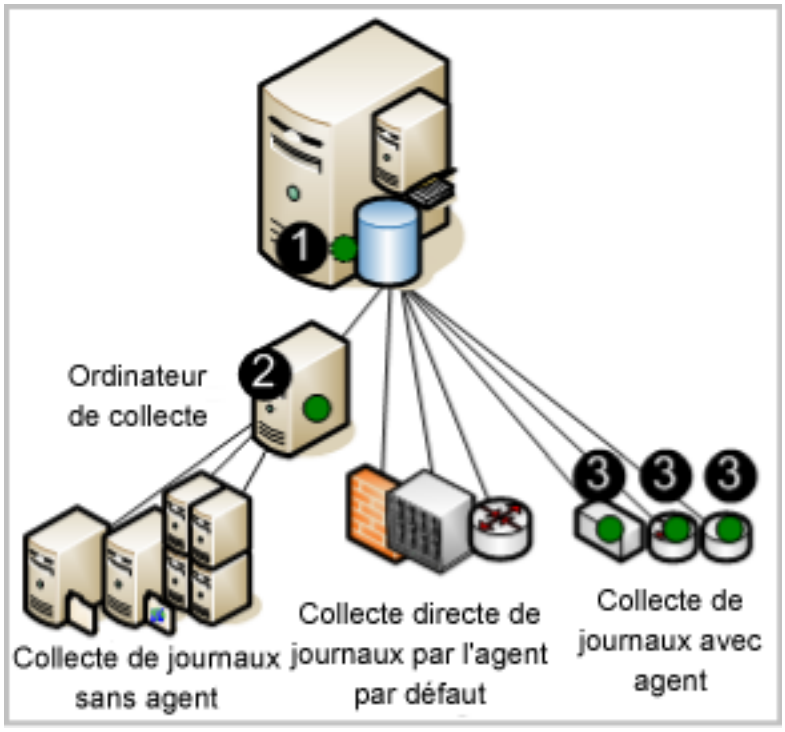
Chapitre 4 : Principales fonctionnalités

Ce chapitre traite des sujets suivants :

Collecte de journaux

Le serveur CA User Activity Reporting Module peut être configuré pour collecter des journaux à l'aide d'une ou de plusieurs techniques prises en charge. Les techniques diffèrent quant au type et à l'emplacement du composant qui écoute et collecte les journaux. Ces composants sont configurés sur les agents.

L'illustration ci-dessous décrit un système avec un seul serveur, où l'emplacement des agents est indiqué par un cercle sombre (vert).



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Configurez l'agent par défaut sur CA User Activity Reporting Module pour récupérer directement des événements auprès des sources Syslog spécifiées.
2. Configurez l'agent installé sur un point de collecte Windows pour collecter des événements provenant des serveurs Windows spécifiés et les transmettre à CA User Activity Reporting Module.
3. Configurez les agents installés sur des hôtes où sont exécutées les sources d'événement, pour collecter le type d'événement configuré et effectuer la suppression.

Remarque : Le trafic entre l'agent et le serveur CA User Activity Reporting Module de destination est toujours chiffré.

Etudiez les avantages de chaque technique de collecte de journaux ci-dessous.

- Collecte directe de journaux

  Avec la collecte directe de journaux, vous configurez l'écouteur Syslog sur l'agent par défaut pour recevoir les événements des sources fiables spécifiées. Vous pouvez également configurer d'autres connecteurs pour collecter des événements provenant de n'importe quelle source d'événement compatible avec l'environnement de fonctionnement du dispositif logiciel.

  Avantage : vous n'avez pas besoin d'installer un agent pour collecter les journaux des sources d'événement à proximité du serveur CA User Activity Reporting Module sur le réseau.

- Collecte sans agent

  Avec la collecte sans agent, il n'existe aucun agent local sur les sources d'événement. Au lieu de cela, un agent est installé sur un point de collecte dédié. Des connecteurs sont configurés pour chaque source d'événement cible sur cet agent.

Avantage : vous pouvez collecter des journaux provenant de sources d'événement s'exécutant sur des serveurs où vous ne pouvez pas installer d'agents, comme des serveurs où la stratégie d'entreprise interdit les agents. La remise est garantie, par exemple, lorsque la collecte de journaux ODBC est correctement configurée.

- Collecte avec agent

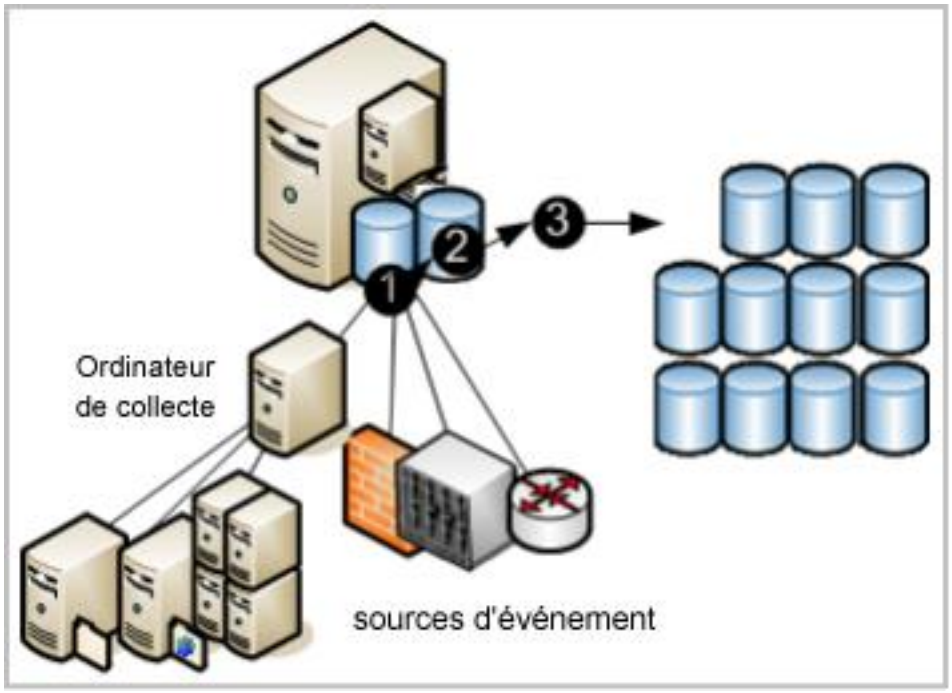
  Pour la collecte avec agent, un agent est installé lorsqu'une ou plusieurs sources d'événement sont exécutées et qu'un connecteur est configuré pour chaque source d'événement.

  Avantage : vous pouvez collecter des journaux provenant d'une source pour laquelle la bande passante du réseau vers CA User Activity Reporting Module n'est pas suffisamment efficace pour prendre en charge la collecte directe de journaux. Vous pouvez utiliser l'agent pour filtrer les événements et réduire le trafic émis sur le réseau. La remise d'événement est garantie.

Remarque : Pour plus de détails sur la configuration des agents, consultez le *Manuel d'administration*.

Stockage des journaux

CA User Activity Reporting Module dispose du stockage intégré et géré des journaux des bases de données récemment archivées. Les événements collectés par les agents provenant de sources d'événement suivent un cycle de stockage tel qu'illustré par le schéma ci-dessous.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Les nouveaux événements collectés par n'importe quelle technique sont envoyés à CA User Activity Reporting Module. L'état des événements entrants dépend de la technique utilisée pour les collecter. Les événements entrants doivent être ajustés avant d'être insérés dans la base de données.
2. Lorsque la base de données des enregistrements ajustés atteint la taille configurée, tous les enregistrements sont compressés en une base de données et enregistrés sous un seul nom. La compression des données des journaux réduit les coûts induits par leur déplacement et leur stockage. La base de données compressée peut être déplacée automatiquement en fonction de la configuration de l'archivage automatique ; vous pouvez également la sauvegarder et la déplacer manuellement avant qu'elle n'atteigne la durée configurée avant suppression (les bases de données archivées automatiquement sont supprimées de la source dès qu'elles sont déplacées).
3. Si vous configurez l'archivage automatique pour qu'il déplace chaque jour les bases de données compressées vers un serveur distant, vous pouvez déplacer ces sauvegardes vers un stockage de journaux hors site à long terme si vous le souhaitez. En conservant les sauvegardes des journaux, vous respectez les réglementations stipulant que les journaux doivent être collectés de manière sécurisée, stockés de manière centralisée pendant un certain nombre d'années et disponibles pour être examinés (vous pouvez restaurer la base de données à tout moment depuis le stockage à long terme).

Remarque : Pour plus de détails sur la configuration du magasin de journaux d'événements, y compris la configuration de l'archivage automatique, consultez le *Manuel d'implémentation*. Pour plus de détails sur la restauration des sauvegardes à des fins d'examen et de génération de rapports, consultez le *Manuel d'administration*.

Présentation normalisée des journaux

Les journaux générés par les applications, les systèmes d'exploitation et les unités utilisent tous leur propre format. CA User Activity Reporting Module ajuste les journaux collectés afin de normaliser la consignation des données. Le format standard facilite la comparaison des données collectées auprès de différentes sources pour les auditeurs et les cadres supérieurs. Techniquement, le CEG (Common Event Grammar) CA facilite l'implémentation de la normalisation et de la classification des événements.

La CEG propose plusieurs champs utilisés pour normaliser différents aspects de l'événement, notamment ceux répertoriés ci-dessous.

- Modèle idéal (classe de technologies comme les antivirus, les SGBD et les pare-feu)
- Catégorie (par exemple Gestion des identités et Sécurité du réseau)
- Classe (par exemple Gestion des comptes et Gestion de groupes)
- Action (par exemple Création d'un compte et Création d'un groupe)
- Résultats (par exemple Opération réussie et Echec)

Remarque : Pour plus de détails sur les règles et fichiers utilisés lors de l'ajustement des événements, consultez le *Manuel d'administration CA User Activity Reporting Module*. Consultez la section relative à la Grammaire commune aux événements dans l'aide en ligne pour de plus amples détails sur la normalisation et la classification des événements.

Génération de rapports de conformité

CA User Activity Reporting Module vous permet de collecter et de traiter des données relatives à la sécurité, puis de les transformer en rapports appropriés pour les auditeurs internes ou externes. Vous pouvez interagir par le biais de requêtes et de rapports à des fins d'examen. Vous pouvez automatiser le processus de génération de rapports en planifiant les jobs de rapport.

Le système offre les avantages ci-dessous.

- Simplicité de formulation de requêtes, grâce aux balises
- Génération de rapports en temps quasi-réel
- Centralisation de la recherche dans les archives distribuées des journaux critiques

Il se concentre sur la génération de rapports de conformité plutôt que sur la corrélation en temps réel des événements et alertes. La réglementation exige la génération de rapports prouvant la conformité avec les contrôles relatifs au secteur. CA User Activity Reporting Module fournit des rapports contenant les balises ci-dessous pour faciliter l'identification.

- Basel II
- COBIT
- COSO
- Directive UE - Protection des données
- FISMA
- GLBA
- HIPAA
- ISO\IEC 27001\2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS 70
- SOX

Vous pouvez examiner des rapports de journaux prédéfinis ou effectuer des recherches en fonction de critères spécifiés par vos soins. De nouveaux rapports sont fournis avec les mises à jour d'abonnement.

Les fonctionnalités d'affichage des journaux reposent sur les éléments suivants :

- Requêtes à la demande, prédéfinies ou définies par l'utilisateur, dont les résultats peuvent atteindre jusqu'à 5 000 enregistrements
- Recherche rapide, au moyen d'invites, pour un nom d'hôte, une adresse IP, un numéro de port ou un nom d'utilisateur spécifié
- Génération de rapports planifiée et à la demande, avec contenu de génération de rapports prêt à l'emploi
- Requêtes et alertes planifiées
- Rapports de base avec informations de tendances
- Visionneuses d'événements interactives et graphiques
- Génération automatisée de rapport avec pièce jointe de courriel
- Stratégies de conservation automatisée de rapport

Remarque : Pour plus de détails sur l'utilisation de requêtes et de rapports prédéfinis ou sur la création de requêtes et de rapports personnalisés, consultez le *Manuel d'administration CA User Activity Reporting Module*.

Alerte de violation de stratégie

CA User Activity Reporting Module vous permet d'automatiser l'envoi d'un courriel d'alerte lorsque survient un événement qui nécessite une attention à court terme. Vous pouvez également surveiller à tout instant les alertes d'action à partir de CA User Activity Reporting Module, en spécifiant un intervalle de temps, depuis les cinq dernières minutes jusqu'aux 30 derniers jours écoulés. Des alertes sont envoyées automatiquement à un flux RSS auquel il est possible d'accéder à partir d'un navigateur Web. Si vous le souhaitez, vous pouvez spécifier d'autres destinations, y compris des adresses électroniques, un processus CA IT PAM, qui génère des tickets de bureau d'assistance, et une ou plusieurs adresses IP de destination d'interruption SNMP.

Pour vous aider à commencer, de nombreuses requêtes prédéfinies sont disponibles pour être planifiées, sans modification, en alertes d'action. Quelques exemples sont présentés ci-dessous.

- Activité excessive de l'utilisateur
- Utilisation élevée de l'UC
- Peu d'espace disque disponible
- Journal des événements de sécurité effacé au cours des dernières 24 heures
- Stratégie d'audit Windows modifiée au cours des dernières 24 heures

Certaines requêtes comportent des listes à clés, où vous fournissez les valeurs utilisées par la requête. Certaines listes à clés contiennent des valeurs prédéfinies que vous pouvez compléter, par exemple les comptes par défaut et les groupes avec droits. D'autres listes à clés, comme celle des ressources stratégiques, ne comportent pas de valeurs par défaut. Une fois configurées, des alertes peuvent être planifiées pour des requêtes prédéfinies comme celles répertoriées ci-dessous.

- Ajout ou retrait d'une appartenance à un groupe par des groupes avec droits.
- Connexion établie par le compte par défaut
- Aucun événement reçu par les sources stratégiques.

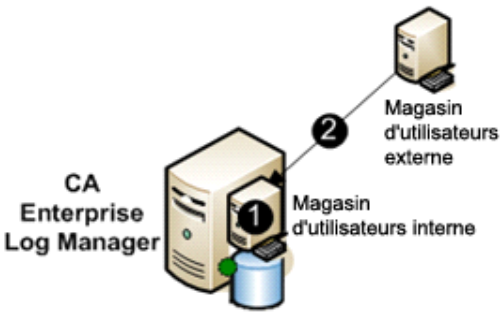
Les listes à clés peuvent être mises à jour manuellement, en important un fichier, ou en exécutant un traitement des valeurs dynamiques de CA IT PAM.

Remarque : Pour plus de détails sur les alertes d'action, consultez le *Manuel d'administration CA User Activity Reporting Module*.

Gestion des droits

Lorsque vous configurez le magasin d'utilisateurs, vous pouvez utiliser le magasin d'utilisateurs par défaut sur CA User Activity Reporting Module pour configurer des comptes d'utilisateur ou référencer un magasin d'utilisateurs externe contenant des comptes d'utilisateur déjà définis. La base de données sous-jacente est exclusive à CA User Activity Reporting Module et n'utilise pas un SGBD du commerce.

Les magasins d'utilisateurs externes pris en charge incluent CA SiteMinder et les répertoires LDAP comme Microsoft Active Directory, Sun One et Novell eDirectory. Si vous faites référence à un magasin d'utilisateurs externe, les informations des comptes d'utilisateur sont automatiquement chargées en lecture seule, tel qu'illustré par la flèche dans le schéma ci-dessous. Vous définissez uniquement les détails propres à l'application pour les comptes sélectionnés. Aucune donnée n'est déplacée du magasin d'utilisateurs interne vers le magasin d'utilisateurs externe référencé.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Le magasin d'utilisateurs interne procède à la gestion des droits en authentifiant les informations d'identification fournies par les utilisateurs lors de la connexion et en autorisant l'accès des utilisateurs aux différentes fonctions de l'interface utilisateur, en fonction des stratégies associées aux rôles affectés à leurs comptes d'utilisateur. Si le nom d'utilisateur et le mot de passe d'un utilisateur tentant de se connecter ont été chargés par un magasin d'utilisateurs externe, les informations d'identification entrées doivent correspondre aux informations d'identification chargées.
2. La seule fonction du magasin d'utilisateurs externe consiste à charger ses comptes d'utilisateur dans le magasin d'utilisateurs interne. Ces comptes sont chargés automatiquement lorsque la référence au magasin d'utilisateurs est enregistrée.

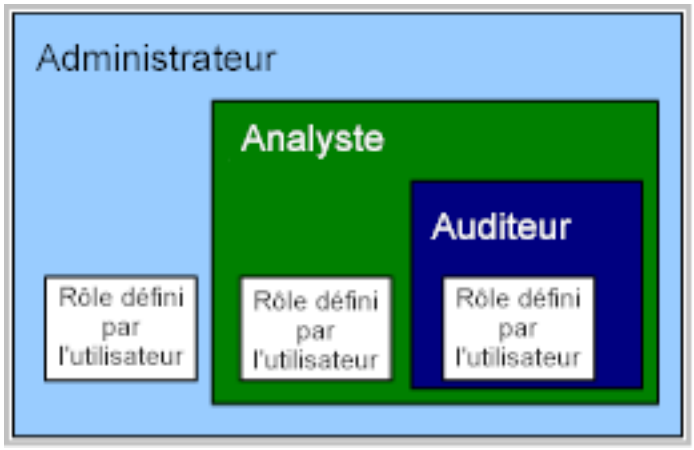
Remarque : Pour plus de détails sur la configuration de l'accès de l'utilisateur de base, consultez le *Manuel d'implémentation CA User Activity Reporting Module*. Pour plus de détails sur les stratégies de prise en charge de rôles prédéfinis, de création de comptes d'utilisateur et d'affectation de rôles, consultez le *Manuel d'administration CA User Activity Reporting Module*.

Accès selon un rôle

CA User Activity Reporting Module propose trois groupes d'applications ou rôles prédéfinis. Les administrateurs affectent les rôles ci-dessous aux utilisateurs, pour spécifier leurs droits d'accès aux fonctions CA User Activity Reporting Module.

- Administrator
- Analyst
- Auditor

L'auditeur peut accéder à quelques fonctions. L'analyste peut accéder à toutes les fonctions Auditor, auxquelles s'ajoutent quelques autres fonctions. L'administrateur peut accéder à toutes les fonctions. Vous pouvez définir un rôle personnalisé avec des stratégies associées qui limitent l'accès de l'utilisateur aux ressources, de façon à répondre à vos besoins commerciaux.



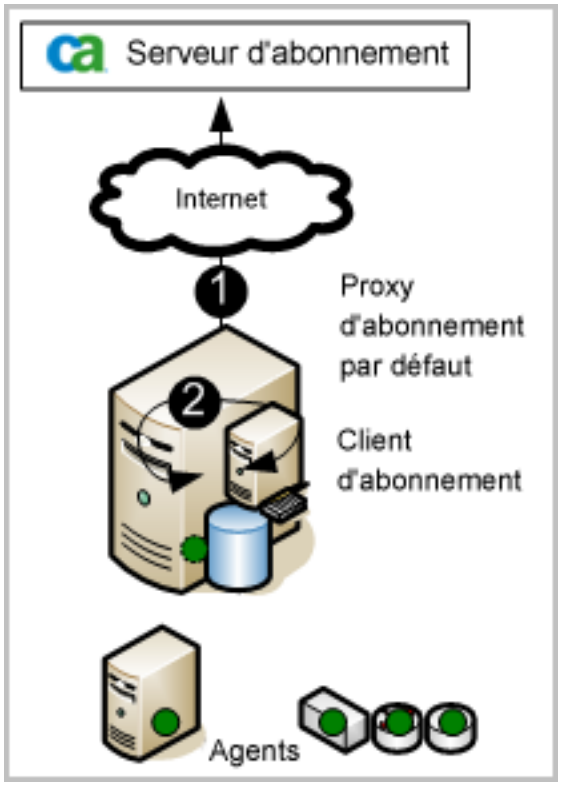
Les administrateurs peuvent personnaliser l'accès à n'importe quelle ressource en créant un groupe d'applications personnalisé avec des stratégies associées, puis en affectant ce groupe d'applications, ou rôle, aux comptes d'utilisateur.

Remarque : Pour plus de détails sur la planification et la création de rôles personnalisés, de stratégies personnalisées et de filtres d'accès, consultez le *Manuel d'administration CA User Activity Reporting Module*.

Gestion de l'abonnement

Le module d'abonnement est le service qui permet de télécharger automatiquement, de manière planifiée, les mises à jour d'abonnement provenant du serveur d'abonnement CA et de les distribuer aux serveurs CA User Activity Reporting Module. Lorsqu'une mise à jour d'abonnement inclut le module pour les agents, les utilisateurs lancent le déploiement de ces mises à jour vers les agents. *Les mises à jour d'abonnement* sont des mises à jour de composants CA User Activity Reporting Module, ainsi que des mises à jour de système d'exploitation, des correctifs et des mises à jour de contenu, comme les rapports.

L'illustration ci-dessous décrit le scénario le plus simple de connexion directe à Internet.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Le serveur CA User Activity Reporting Module, en tant que serveur d'abonnements par défaut, contacte le serveur d'abonnements CA concernant les mises à jour et télécharge toute mise à jour nouvellement disponible. Le serveur CA User Activity Reporting Module crée une sauvegarde, puis envoie les mises à jour de contenu vers le composant incorporé du serveur de mises à jour qui stocke les mises à jour de contenu pour tous les autres serveurs CA User Activity Reporting Module.
2. En tant que client d'abonnement, le serveur CA User Activity Reporting Module installe lui-même les mises à jour des produits et du système d'exploitation dont il a besoin.

Remarque : Pour plus de détails sur la planification et la configuration de l'abonnement, consultez le *Manuel d'implémentation*. Pour plus de détails sur l'ajustement et la modification de la configuration d'abonnement et sur l'application des mises à jour aux agents, consultez le *Manuel d'administration*.

Contenu prêt à l'emploi

CA User Activity Reporting Module contient un contenu prédéfini que vous commencez à utiliser dès l'installation et la configuration du produit. Le processus d'abonnement ajoute régulièrement du contenu nouveau et met à jour celui existant.

Les catégories de contenu prédéfini incluent :

- Rapports avec balises
- Requêtes avec balises
- Intégrations avec des capteurs associés, fichiers d'analyse (XMP), fichiers de mappage (DM) et, dans certains cas, règles de suppression
- Règles de suppression et de récapitulation

Chapitre 5 : Informations complémentaires concernant CA User Activity Reporting Module

Ce chapitre traite des sujets suivants :

Affichage des infobulles

Vous pouvez identifier la finalité des boutons, des cases à cocher et des rapports de la page CA User Activity Reporting Module dans votre affichage actuel.

Pour afficher les infobulles et autres aides

1. Déplacez votre curseur au-dessus des boutons pour afficher la description de leur fonction. Vous pouvez ainsi visualiser la fonction de n'importe quel bouton.

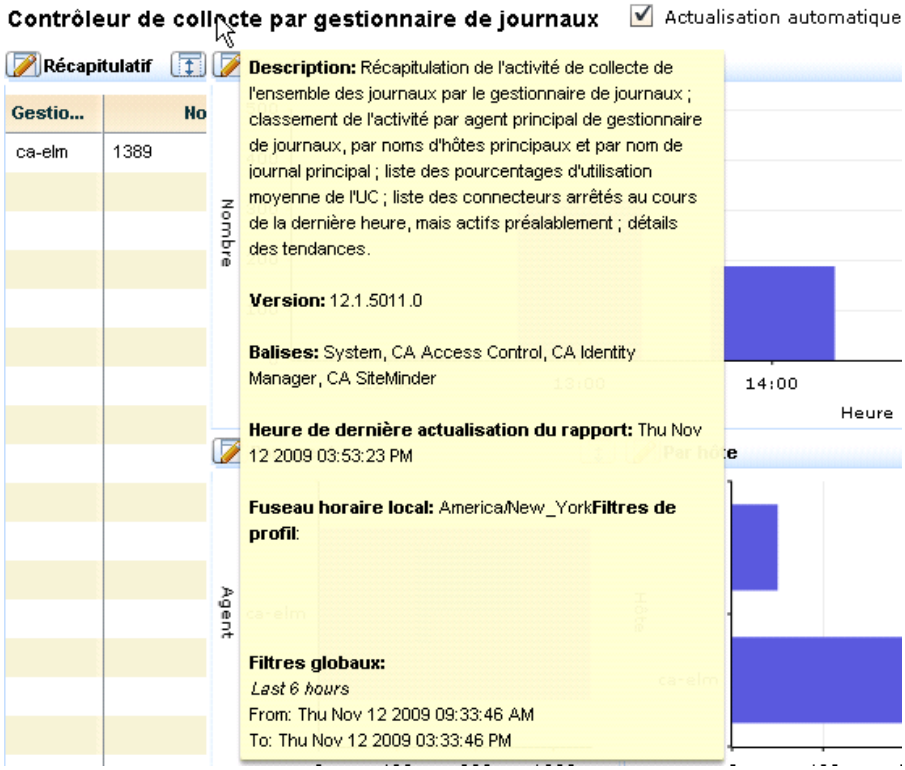
2. Notez la différence entre les boutons actifs et inactifs.

   Lorsqu'ils sont activés, les boutons s'affichent en couleur. Par exemple, le bouton Liste des filtres d'accès s'affiche en couleur pour les administrateurs de la gestion des utilisateurs et des accès.

Lorsqu'ils sont désactivés, les boutons s'affichent en noir et blanc. Par exemple, les boutons Liste des filtres d'accès s'affichent en noir et blanc pour les auditeurs.

3. Affichez les descriptions des champs de saisie ou des cases à cocher en déplaçant votre curseur au-dessus du nom du champ.

4. Affichez les descriptions des rapports en déplaçant votre curseur au-dessus du nom du rapport.



5. Vous remarquerez un point orange à gauche de certains champs. Ce point signifie que le champ est obligatoire. Pour les configurations pouvant être enregistrées, vous ne pouvez pas effectuer d'enregistrement tant que tous les champs obligatoires ne sont pas renseignés.

Affichage de l'aide en ligne

Vous pouvez afficher de l'aide sur la page que vous consultez ou pour toute tâche que vous souhaitez effectuer.

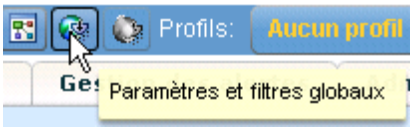
Pour afficher l'aide en ligne

1. Cliquez sur le lien Aide dans la barre d'outils pour afficher le système d'aide en ligne de CA User Activity Reporting Module.

Le système d'aide de CA User Activity Reporting Module apparaît, son contenu étant affiché dans le volet gauche.

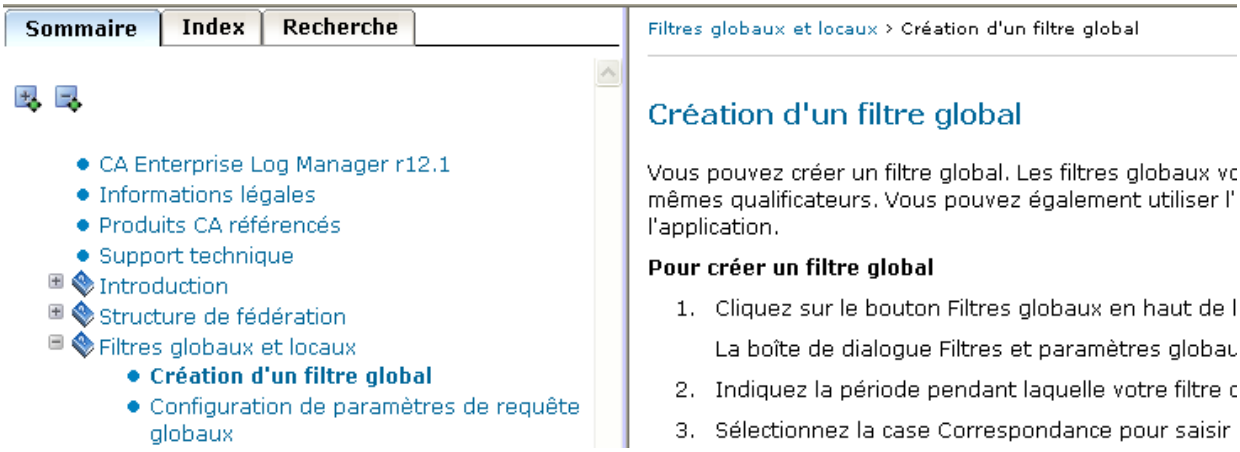
2. L'exemple ci-dessous présente l'accès à l'aide contextuelle à partir d'un bouton Aide.

   a. Cliquez sur le bouton Afficher/Modifier les filtres globaux.



   La fenêtre Filtres et paramètres globaux apparaît et affiche un bouton Aide.

b. Cliquez sur le bouton Aide. L'aide en ligne pour la procédure que vous pouvez effectuer sur la page, le volet ou la boîte de dialogue en cours apparaît dans une fenêtre secondaire.



c. Si vous savez quelle tâche effectuer sans connaître la méthode d'accès à la page correspondante dans CA User Activity Reporting Module, vous pouvez rechercher cette page dans la table des matières. Cliquez sur le titre de la tâche pour afficher la page correspondante.

Remarque : Si vous ne trouvez pas la tâche dont vous avez besoin dans la table des matières, consultez la bibliothèque de documentation.

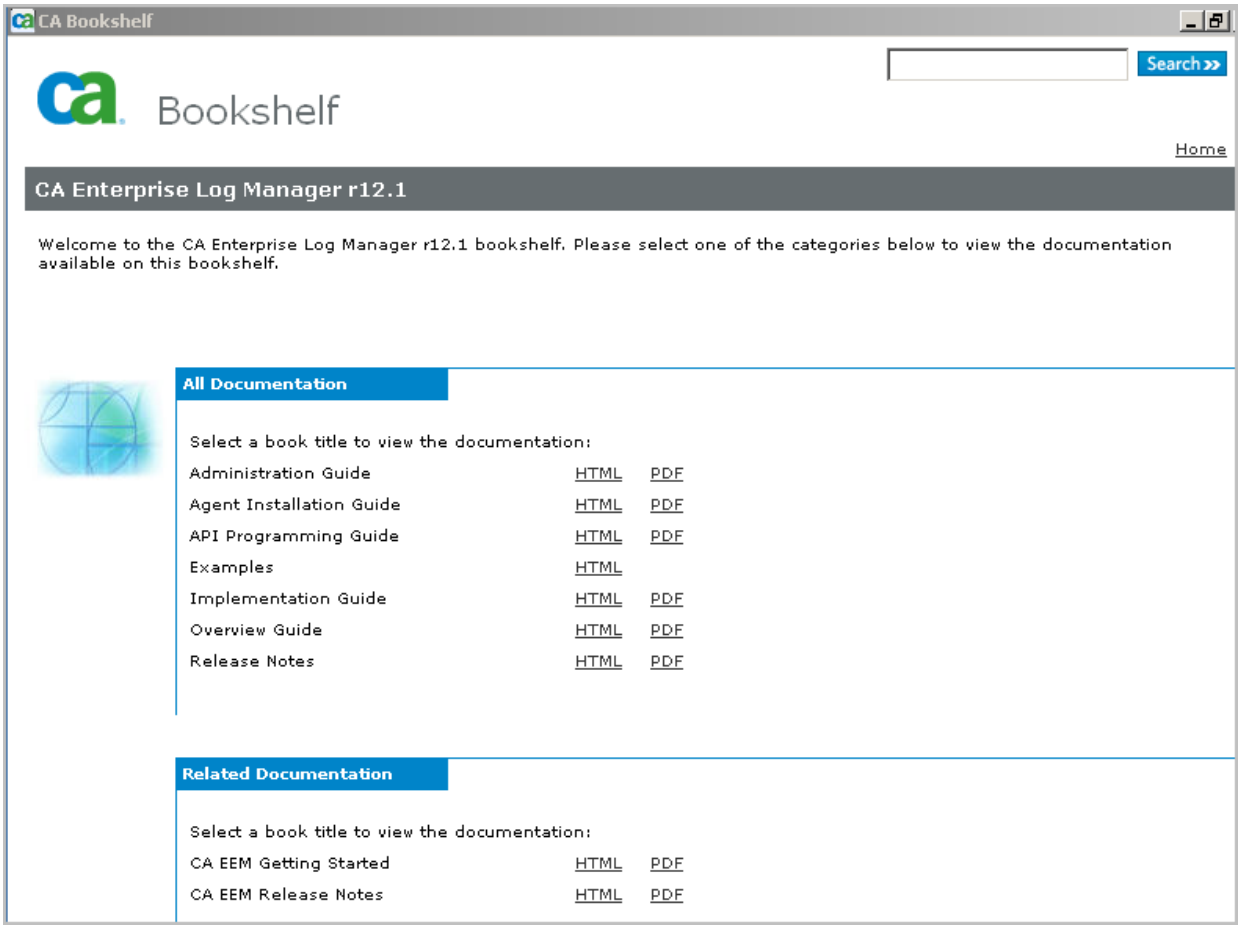
Exploration de la bibliothèque de documentation

Vous pouvez copier la bibliothèque sur votre lecteur local et ouvrir le livre souhaité au format HTML ou PDF. Les livres au format HTML contiennent des références croisées d'un livre à l'autre.

Pour explorer la bibliothèque

1. Copiez sur votre lecteur local la bibliothèque présente sur le DVD d'installation de l'application ou téléchargez-la à partir du site de support clientèle de CA. Pour ouvrir la bibliothèque, double-cliquez sur Bookshelf.hta ou sur Bookshelf.html.

   Une page similaire à la page suivante apparaît.

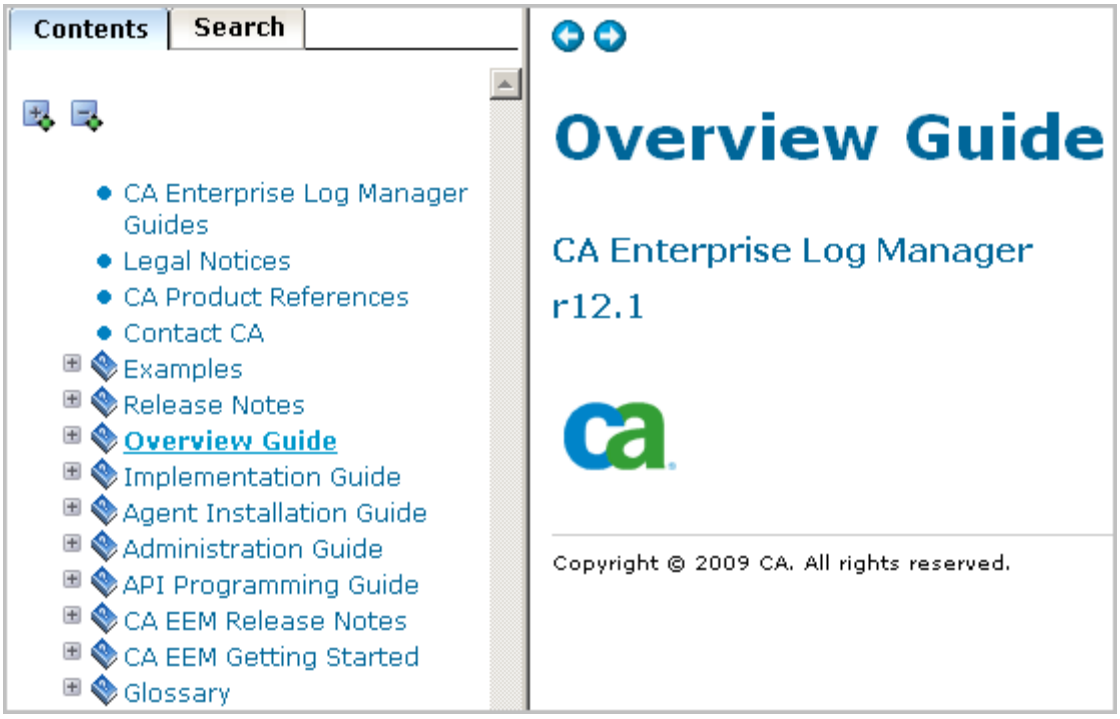


Le contenu des principaux manuels et des exemples est répertorié ci-dessous.

Produit livrable	Description
Manuel d'installation des agents	Installer des agents.
Manuel d'implémentation	Installer et configurer un système CA User Activity Reporting Module.
Manuel d'administration	Personnalisez la configuration, effectuez des tâches d'administration de routine et utilisez les requêtes, les rapports et les alertes.
Manuel de programmation de l'API	Utilisez l'API pour afficher des données d'événement dans un navigateur Web ou incorporer des rapports dans un autre produit CA ou tiers.
Exemples	Résoudre des problèmes professionnels courants, avec des liens vers des rubriques de la documentation.

2. Saisissez une valeur dans le champ d'entrée Rechercher, puis cliquez sur le bouton Rechercher pour afficher toutes les occurrences documentées qui comprennent votre entrée.
3. Cliquez sur un lien Imprimer pour ouvrir le PDF du manuel sélectionné.

4. Cliquez sur un lien HTML pour ouvrir l'ensemble de documentation intégré. Cet ensemble intégré comprend tous les manuels au format HTML. Si vous sélectionnez le lien HTML du Manuel de présentation, ce manuel est affiché.



Index