CA Enterprise Log Manager

Notes de parution

r12.1 SP1

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)
- CA Service Desk
- 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.

- Mise à niveau par abonnement : des informations spécifiques à CA Enterprise Log Manager r12.1 SP1 ont été ajoutées dans cette rubrique. Utilisez l'abonnement pour obtenir ce Service Pack et pour mettre à niveau CA Enterprise Log Manager pour la prise en charge de la norme FIPS.
- Nouvelles fonctionnalités et fonctionnalités modifiées dans la version r12.1 SP1 : ce chapitre décrit la compatibilité avec la norme FIPS pour CA Enterprise Log Manager, le chiffrement utilisé, les limitations et les modifications de la configuration requises pour accéder à l'interface utilisateur à partir de Microsoft Internet Explorer et de Mozilla Firefox. Il inclut également une rubrique relative à l'utilisation de l'image ISO pour effectuer de nouveaux déploiements et ajouter un nouveau serveur CA Enterprise Log Manager à un déploiement existant.
- Erreur de correspondance de certificat après modification de l'heure système du serveur CA EEM : cette rubrique indique désormais l'extension de nom de fichier de certificat .cer.
- Conditions préalables à la configuration avancée pour certains ordinateurs HP et IBM : cette nouvelle section décrit les modifications apportées aux paramètres par défaut d'alimentation sur des serveurs HP Proliant DL 380G5 Series et IBM X3650 Series.
- Les problèmes connus suivants ont été supprimés, étant donné qu'ils ont été réglés et ne s'appliquent plus à cette mise à jour :
  - Echec des agents utilisant des certificats personnalisés
  - Echec de l'exécuteur syslog secondaire lors de la charge
  - Des événements du même hôte de destination s'affichent parfois avec des noms d'hôtes différents
  - Restriction sur les spécifications de rapports PDF
  - Impossible de se connecter à CA Enterprise Log Manager après une mise à niveau
  - La mise à jour directe vers r12.1 M10 entraîne l'affichage de la mauvaise version du détecteur
  - Affichage incorrect d'une erreur indiquant que le gestionnaire de stratégies CA Audit n'a pas été installé
  - Mise à niveau vers CA Audit requise pour l'interopérabilité avec CA Enterprise Log Manager

Informations complémentaires :

Mise à niveau par abonnement (page 11)
Fonctionnalités r12.1 SP1 ajoutées et modifiées (page 35)
Conformité à la norme FIPS 140-2 (page 35)
Modes de fonctionnement (page 36)
Bibliothèques de chiffrement (page 36)
Algorithmes utilisés (page 37)
Certificats et fichiers clés (page 38)
Limitations de la prise en charge de la norme FIPS (page 39)
Configuration de Microsoft Internet Explorer pour l'accès à CA Enterprise Log Manager en mode FIPS (page 41)
Configuration de Mozilla Firefox pour l'accès à CA Enterprise Log Manager en mode FIPS (page 41)

Table des matières

Chapitre 1 : Bienvenue 11

Mise à niveau par abonnement 11

Chapitre 2 : Environnement d'exploitation 13

Environnements matériel et logiciel 13
Conditions préalables à la configuration avancée pour certains ordinateurs HP et IBM 15
Résolution de l'écran 15
Références du serveur CA EEM 16

Chapitre 3 : Fonctionnalités 17

Collecte de journaux 17
Stockage des journaux 20
Présentation normalisée des journaux 22
Génération de rapports de conformité 23
Alerte de violation de stratégie 25
Accès selon un rôle 26
Gestion de l'abonnement 27
Prise en charge des adresses IP IPv6 28

Chapitre 4 : Fonctionnalités r12.1 ajoutées et modifiées 31

Ouvrez API Access 31
Alertes donnant lieu à une action : Intégration de CA IT PAM 32
Alertes pouvant être déclenchées : Intégration de SNMP avec des produits NSM 32
Accès ODBC et JDBC 33
Pertinence d'identité et d'actif : Intégration de CA IT PAM 33
Collecte de journal directe étendue par l'agent par défaut 34
Planification automatique des mises à jour pour les clients d'abonnement 34

Chapitre 5 : Fonctionnalités r12.1 SP1 ajoutées et modifiées 35

Conformité à la norme FIPS 140-2 35
Modes de fonctionnement 36
Bibliothèques de chiffrement 36
    Algorithmes utilisés 37
Certificats et fichiers clés 38
Limitations de la prise en charge de la norme FIPS 39

Configuration de Microsoft Internet Explorer pour l'accès à CA Enterprise Log Manager en mode FIPS 41
Configuration de Mozilla Firefox pour l'accès à CA Enterprise Log Manager en mode FIPS 41
Image ISO pour de nouvelles installations 43

Chapitre 6 : Problèmes connus 45

Agents et adaptateurs CA 45
Dépendance d'installation d'un agent sous Red Hat Linux 4 45
Précision de l'heure de l'état de l'Agent selon la configuration du serveur NTP 46
Prévision d'un délai pour la mise à jour après le déploiement du connecteur en bloc 46
Le déploiement du connecteur en bloc avec une adresse IPv6 n'est pas correct 46
Le nom de montage du DVD ne peut pas contenir d'espaces 47
Echec de la configuration de la source d'événement au niveau du domaine 48
Retard d'ODBC et de JDBC suite à l'activation de la communication SSL 49
SuSE Linux non pris en charge dans les intégrations de la version 4.0.0.0 du détecteur de journaux 49
Restriction sur la configuration des ports 49
Risque de diminution des performances en cas de sélection d'un nombre trop important d'intégrations 50
La suppression d'un serveur dans une fédération ne supprime pas l'agent par défaut 50
Les rapports sur les données collectées par le collecteur SAPI de CA n'affichent pas les événements correctement 50
Remise de Syslogs via UDP non garantie 51
Conflit de services Syslog sous UNIX 52
Le détecteur de journaux WMI génère plusieurs événements de privilège d'utilisateur 52
Arrêt de la réception d'événements par le détecteur de journaux de fichier texte sur un système d'agent Solaris 53
Capacité de réponse nulle de l'agent lors de la présence d'un nombre très élevé d'événements dans le flux 54
Dispositif (hors interface utilisateur) 54
Connexion impossible au serveur CA Enterprise Log Manager sous le nom d'utilisateur EiamAdmin 55
Nombre excessif de fichiers journaux ELMAdapter 56
L'importation manuelle de fichiers d'analyse peut nécessiter la modification de la valeur d'expiration 57
Ajustement d'événement 58
Une chaîne de mappage de blocs et des valeurs numériques exigent des opérateurs différents 58
Impossibilité pour les fichiers DM personnalisés de mapper des événements epSIM (iTech) 59
Requêtes et rapports 59
Les résultats de la requête d'alertes d'action peuvent être incomplets 60
Restriction sur les requêtes avec plusieurs termes de recherche 60

Le filtre simple de l'assistant des requêtes échoue lors de l'utilisation de caractères spéciaux 61
L'état d'un job planifié ne s'affiche pas après une mise à niveau 61
Echec de certains jobs d'alerte d'action planifiés trop fréquemment 62
Impossible de supprimer des balises qui contiennent des caractères spéciaux 63
Abonnement 63
Redémarrage automatique après mise à jour du SE lors d'une mise à niveau de SP 63
Erreur de manque de mémoire sur les ordinateurs disposant de peu de mémoire 63
La modification des informations d'identification de proxy verrouille le compte de domaine 64
Apparition unique d'un événement d'autosurveillance de redémarrage 65
Nouvelle sélection obligatoire des modules d'abonnement après la mise à niveau 66
Le bouton Tester le proxy renvoie une fausse alerte après un changement de configuration. 67
Deux règles de suppression ne s'appliquent pas correctement 67
La mise à jour vers r12.1 nécessite le redémarrage de iGateway 68
La mise à niveau vers la version r12.1 SP1 peut requérir le redémarrage d'iGateway 69
Mise à jour à des intégrations pour le détecteur de journaux syslog requise dans la version r12.1 SP1 pour les agents pour Windows 70
Gestion des utilisateurs et des accès 70
Restrictions d'accès à partir d'un navigateur sous Windows Vista 70
Restriction sur l'utilisation d'un calendrier avec stratégies d'accès 71
Divers 72
Occasionnellement, CA Enterprise Log Manager ne répond pas 72
Echec des appels de requête et de rapport d'API sur certains navigateurs 73
Fin de la prise en charge de CAELM4Audit 73
Impact du nom d'application personnalisé sur une requête d'archive 74
Paramètres de contraste élevé pour l'écran 74
iGateway s'arrête et redémarre continuellement 75
L'espace disque maximal pour CA Enterprise Log Manager virtuel est insuffisant 76
L'actualisation d'un navigateur déconnecte un utilisateur de CA Enterprise Log Manager 76
Erreur possible au niveau du service ou de l'interface de l'explorateur après le redémarrage d'iGateway 77
Echec des chargements et des exportations avec des navigateurs autres qu'Internet Explorer 77
L'affichage de l'interface utilisateur échoue de manière inattendue lors d'une installation avec un EEM distant 78

Chapitre 7 : Problèmes résolus 81

Problèmes fixés dans la version r12.1 SP1 81

Chapitre 8 : Documentation 83

Bibliothèque 83

Accès à la bibliothèque 84

Annexe A : Communiqués de tiers 85

Adaptive Communication Environment (ACE) 86
Logiciel régi par la licence Apache 88
boost 1.35.0 92
JDOM 1.0 93
PCRE 6.3 95
Zlib 1.2.3 97
ZThread 2.3.2 97

Chapitre 1 : Bienvenue

Bienvenue dans CA Enterprise Log Manager Ce document contient des informations relatives aux systèmes d'exploitation pris en charge, aux améliorations, aux problèmes connus et au support technique de CA.

Mise à niveau par abonnement

Vous pouvez mettre CA Enterprise Log Manager à niveau vers la version ou vers le Service Pack les plus récents en téléchargeant tous les modules livrés par abonnement.

Important : Vous devez mettre à niveau le serveur CA Enterprise Log Manager de gestion avant d'installer des nouveaux serveurs CA Enterprise Log Manager dans votre réseau. Cela garantit l'enregistrement des nouveaux serveurs.

Procédez comme suit.

1. Vérifiez la configuration de base de l'abonnement.
    a. Cliquez sur l'onglet Administration, sur le sous-onglet Services, puis sélectionnez Module d'abonnement.
    b. Sélectionnez non pour Redémarrage automatique après mise à jour du SE.
    c. Déplacez le module Gestionnaire de journaux vers la liste des éléments sélectionnés, si elle ne s'y trouve pas déjà.
    d. Vérifiez que toutes les valeurs requises sont configurées au niveau global.
    e. Vérifiez que toutes les valeurs requises sont configurées pour chaque serveur CA Enterprise Log Manager.

    Remarque : Dans des environnements fédérés, mettez à jour les parents avant les enfants.

    Un événement d'autosurveillance déclarant que les mises à jour d'abonnement ont été installées indique la fin.

2. Vérifiez la configuration de base de l'abonnement.
   a. Cliquez sur l'onglet Administration, sur le sous-onglet Services, puis sélectionnez Module d'abonnement.
   b. Sélectionnez non pour Redémarrage automatique après mise à jour du SE.
   c. Déplacez vers la liste des éléments sélectionnés tous les modules à télécharger.

   Remarque : Dans des environnements fédérés, mettez à jour les parents avant les enfants.
3. Lorsque le processus de mise à jour d'abonnement est terminé, redémarrez chaque serveur CA Enterprise Log Manager.

   Un événement d'autosurveillance déclarant que les mises à jour d'abonnement ont été installées indique la fin.
4. Mettez à jour les agents et les connecteurs comme suit.
   a. Cliquez sur l'onglet Administration, sur le sous-onglet Collecte de journaux, puis sélectionnez Explorateur d'agent.
   b. Déterminez si les mises à jour d'abonnement doivent être appliquées au niveau de l'Explorateur d'agent, des groupes d'agents ou des agents.
   c. Sélectionnez le niveau souhaité, puis cliquez sur le bouton Abonnement.
   d. Appliquez les mises à jour aux agents si Agents faisait partie des modules téléchargés.
   e. Cliquez à nouveau sur le bouton Abonnement.
   f. Appliquez les mises à jour aux connecteurs, si disponibles.
5. Réenregistrez les produits tiers et les autres produits CA (CA Access Control par exemple) utilisant des appels d'API ouverte pour afficher des rapports CA Enterprise Log Manager dans leur interface native.

   Cette étape met à jour les certificats modifiés dans cette version. Pour de plus amples informations, consultez le *Manuel de programmation de l'API CA Enterprise Log Manager*.

Remarque : Pour connaître les problèmes connus liés à la mise à niveau d'un abonnement, reportez-vous aux notes de parution.

Informations complémentaires :

Redémarrage automatique après mise à jour du SE lors d'une mise à niveau de SP (page 63)
Mise à jour à des intégrations pour le détecteur de journaux syslog requise dans la version r12.1 SP1 pour les agents pour Windows (page 70)

Chapitre 2 : Environnement d'exploitation

Ce chapitre traite des sujets suivants :

Environnements matériel et logiciel (page 13)
Conditions préalables à la configuration avancée pour certains ordinateurs HP et IBM (page 15)
Résolution de l'écran (page 15)
Références du serveur CA EEM (page 16)

Environnements matériel et logiciel

Lors de son installation initiale, CA Enterprise Log Manager installe également le système d'exploitation Red Hat Enterprise Linux.

L'index de la matrice de certification CA Enterprise Log Manager inclut les liens vers les matrices de certification CA Enterprise Log Manager, dont les liens suivants :

- Matériel et logiciels de serveur

  Matrice de certification du matériel et des logiciels du serveur CA Enterprise Log Manager

- Matériel et logiciels d'agent

  Matrice de certification du matériel et des logiciels de l'agent CA Enterprise Log Manager

- Prise en charge des détecteurs de journal et des systèmes d'exploitation connexes

  Matrice de certification du détecteur de journal CA Enterprise Log Manager

- Intégrations du produit

  Matrice d'intégration du produit CA Enterprise Log Manager

- Certifications avec CA Audit iRecorder

  Matrice de certification CA Audit iRecorder de CA Enterprise Log Manager

Vous pouvez accéder à CA Enterprise Log Manager au moyen des navigateurs suivants, ainsi qu'avec Adobe Flash Player 9 ou 10.

- Internet Explorer 6 SP2 (uniquement en mode non FIPS)
- Internet Explorer 7 ou 8 (modes FIPS ou non FIPS)
- Mozilla Firefox 2.0.x et 3.0.x (uniquement en mode non FIPS)
- Mozilla Firefox 3.5.8 ou version ultérieure (modes FIPS et non FIPS)

Remarque : Les exportations de fichiers ne fonctionnent pas lorsque vous accédez à CA Enterprise Log Manager avec un navigateur Mozilla Firefox.

Conditions préalables à la configuration avancée pour certains ordinateurs HP et IBM

Lorsque CA Enterprise Log Manager est installé sur des serveurs HP Proliant DL 380G5 Series et IBM X3650 Series avec les paramètres par défaut d'utilisation de l'alimentation, des problèmes peuvent survenir au niveau d'iGateway et ralentir le fonctionnement, ou encore, au niveau de l'interface et requérir le redémarrage manuel du service.

Pour empêcher que cela ne soit le cas, modifiez les paramètres avant d'installer CA Enterprise Log Manager.

Remarque : Si vous avez déjà installé CA Enterprise Log Manager, vous pouvez éteindre l'ordinateur, modifier les paramètres comme indiqué et redémarrer l'ordinateur.

Pour modifier les paramètres d'utilisation de l'alimentation sur un serveur HP Proliant DL 380G5 :

1. Accédez au menu BIOS Settings (paramètres du BIOS).
2. Naviguez jusqu'aux paramètres d'utilisation de l'alimentation.
3. Sélectionnez OS Control Mode.

   Remarque : Le paramètre par défaut est HP Dynamic Power Settings Mode.

Pour modifier les paramètres d'utilisation de l'alimentation sur un serveur IBM X3650 :

1. Accédez au menu BIOS Settings (paramètres du BIOS).
2. Naviguez jusqu'aux paramètres d'utilisation de l'alimentation.
3. Désactivez les paramètres suivants.
   - Active Energy Manager
   - Enhanced C1 Power State

Résolution de l'écran

La résolution d'écran minimale requise est de 1024 x 768 pixels. Pour un affichage plus confortable, la résolution de 1280 x 1024 est recommandée.

Références du serveur CA EEM

Pour obtenir des informations sur la prise en charge des systèmes d'exploitation par un serveur CA EEM existant, consultez le manuel de *mise en oeuvre de CA Embedded Entitlements Manager*. Ce manuel fait partie de la bibliothèque CA Enterprise Log Manager.

Vous pouvez également télécharger cette bibliothèque à partir du support technique. En cas de problème, n'hésitez pas à contacter notre service d'assistance technique à l'adresse http://www.ca.com/worldwide.

Chapitre 3 : Fonctionnalités

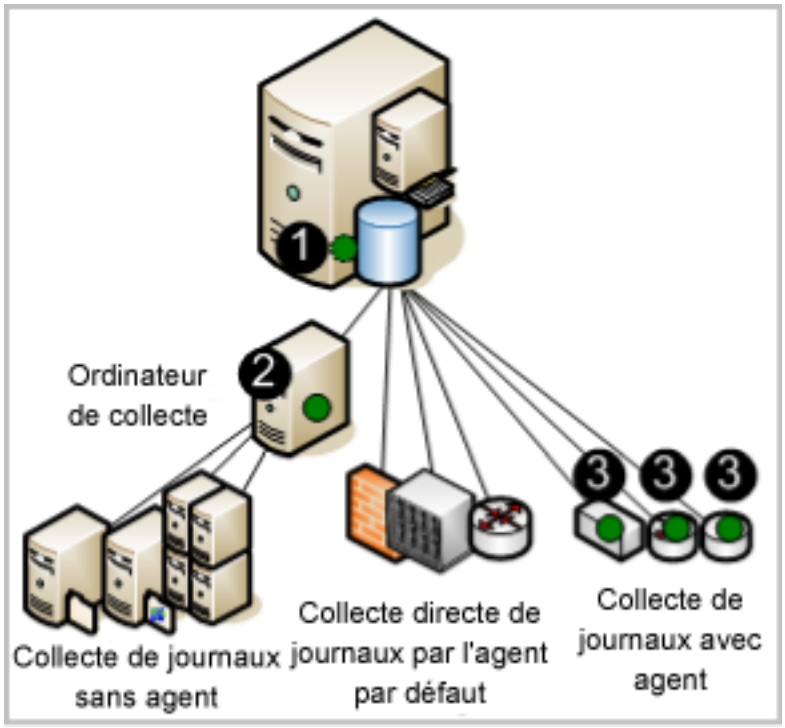
Ce chapitre traite des sujets suivants :

Collecte de journaux (page 17)
Stockage des journaux (page 20)
Présentation normalisée des journaux (page 22)
Génération de rapports de conformité (page 23)
Alerte de violation de stratégie (page 25)
Accès selon un rôle (page 26)
Gestion de l'abonnement (page 27)
Prise en charge des adresses IP IPv6 (page 28)

Collecte de journaux

Le serveur CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager.
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 Enterprise Log Manager 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 Enterprise Log Manager 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

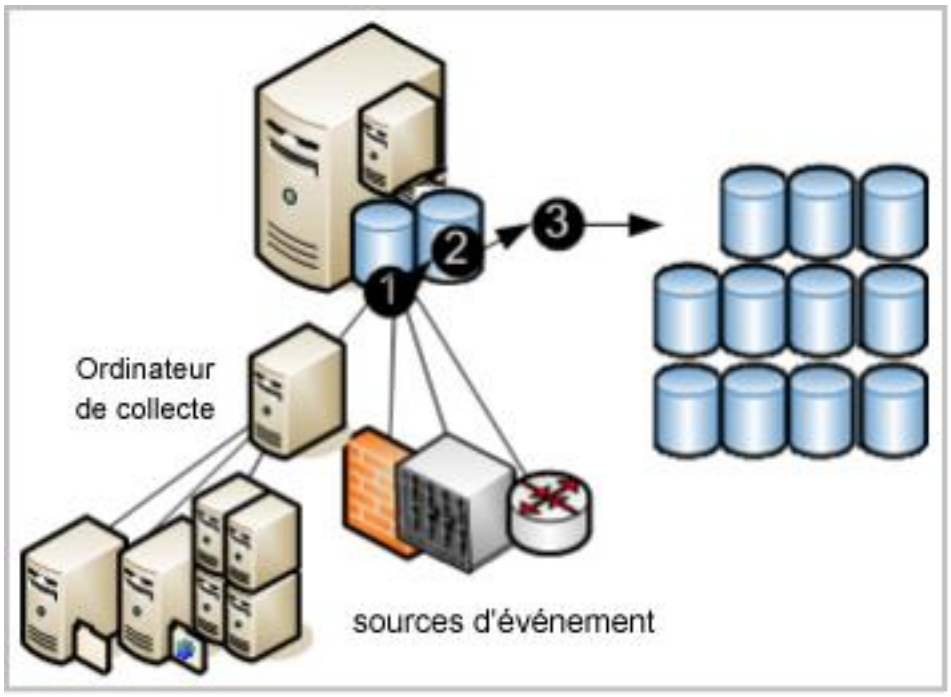
  Pour la collecte avec agent, un agent est installé lorsqu'une ou plusieurs sources d'événement sont exécutées et qu'un connecteur est configuré pour chaque source d'événement.

  Avantage : vous pouvez collecter des journaux provenant d'une source pour laquelle la bande passante du réseau vers CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager. 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 Enterprise Log Manager 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 Enterprise Log Manager*. 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager*.

Alerte de violation de stratégie

CA Enterprise Log Manager 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 Enterprise Log Manager, 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.

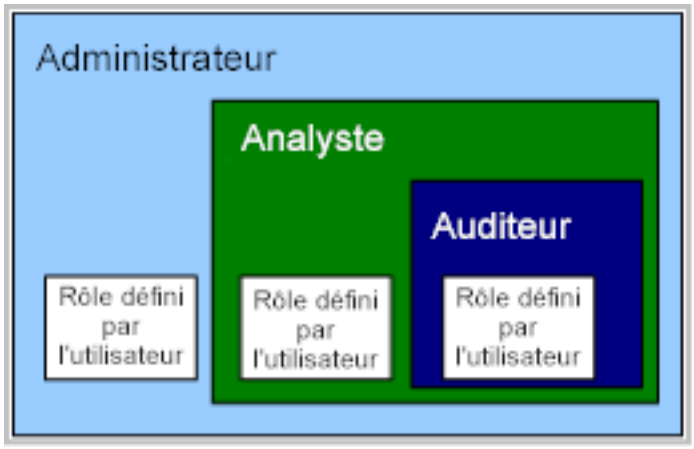
Remarque : Pour plus de détails sur les alertes d'action, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Accès selon un rôle

CA Enterprise Log Manager 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 Enterprise Log Manager.

- 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.



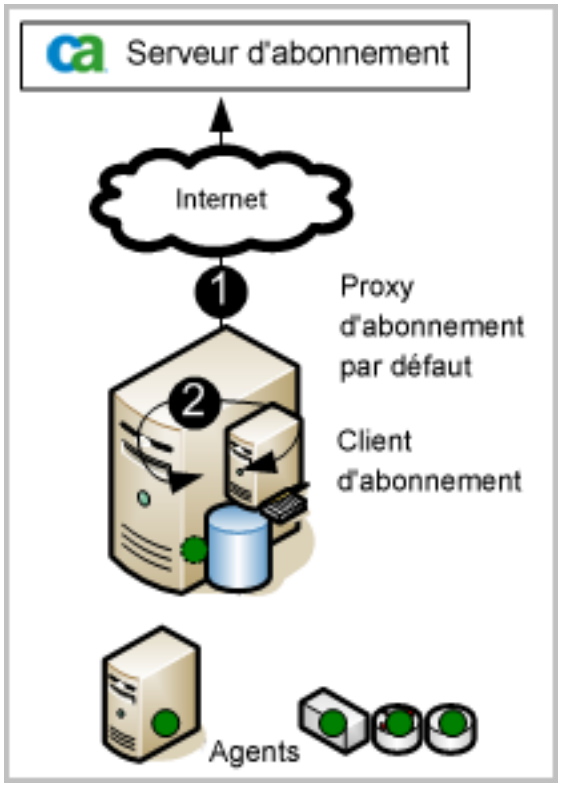
Les administrateurs peuvent personnaliser l'accès à n'importe quelle ressource en créant un groupe d'applications personnalisé avec des stratégies associées, puis en affectant ce groupe d'applications, ou rôle, aux comptes d'utilisateur.

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 Enterprise Log Manager*.

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 Enterprise Log Manager. 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 Enterprise Log Manager, 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 Enterprise Log Manager, 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 Enterprise Log Manager 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 Enterprise Log Manager.
2. En tant que client d'abonnement, le serveur CA Enterprise Log Manager 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*.

Prise en charge des adresses IP IPv6

La spécification des adresses IP était antérieurement limitée à la notation décimale IPv4, avec points. La version actuelle prend désormais en charge les adresses IPv6 dans tout champ d'adresse IP. IPv6 utilise des adresses IP de 128 bits au lieu des adresses de 32 bits utilisées par IPv4. Toute stratégie basée sur la version des adresses IP prend en charge IPv6, ainsi qu'IPv4.

Vous pouvez utiliser des adresses IPv6 mappées IPv4 ou le format IPv6 traditionnel. Le format d'adresse IPv6 mappée IPv4 permet de représenter l'adresse IPv4 d'un noeud IPv4 comme une adresse IPv6, comme suit :

- Le format IPv6 favori est rédigé sous la forme de huit groupes de quatre chiffres héxadécimaux (x:x:x:x:x:x:x:x). Chaque x correspond à quatre chiffres hexadécimaux des huit parties de 16 bits de l'adresse.
- Une adresse IPv6 mappée IPv4, très pratique dans un environnement comportant à la fois des noeuds IPv4 et IPv6, prend le format 0:0:0:0:0:FFFF:d.d.d.d, où chaque d représente une valeur décimale de l'adresse (notation décimale IPv4, avec points).

  Important : Les adresses IPv6 compatibles IPv4 au format 0:0:0:0:0:0:d.d.d.d sont maintenant abandonnées, conformément à la RFC 4291, car les mécanismes de transition IPv6 actuels n'utilisent plus ces adresses.

Voici une adresse IPv6 valide au format traditionnel.

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Si un ou plusieurs groupes de quatre chiffres sont à 0000, ces zéros peuvent être omis et remplacés par deux signes deux-points (::). Les zéros en début de groupe peuvent également être omis. Les adresses IP données en exemple ci-après sont équivalentes.

- 2001:0db8:0000:0000:0000:0000:1428:57ab
- 2001:0db8::1428:57ab
- 2001:db8:0:0:0:0:1428:57ab
- 2001:db8::1428:57ab

Si vous remplacez des adresses IPv4 par des adresses mappées IPv4, conformez-vous aux exemples ci-dessous.

- 0:0:0:0:0:FFFF:192.168.2.128
- 0:0:0:0:0:FFFF:172.16.2.128

Vous pouvez également utiliser la forme compressée présentée ci-dessous.

- ::FFFF:192.168.2.128
- ::FFFF:172.16.2.128

Chapitre 4 : Fonctionnalités r12.1 ajoutées et modifiées

Ce chapitre traite des sujets suivants :

Ouvrez API Access (page 31)
Alertes donnant lieu à une action : Intégration de CA IT PAM (page 32)
Alertes pouvant être déclenchées : Intégration de SNMP avec des produits NSM (page 32)
Accès ODBC et JDBC (page 33)
Pertinence d'identité et d'actif : Intégration de CA IT PAM (page 33)
Collecte de journal directe étendue par l'agent par défaut (page 34)
Planification automatique des mises à jour pour les clients d'abonnement (page 34)

Ouvrez API Access

CA Enterprise Log Manager vous permet d'utiliser des appels d'API pour accéder à des données depuis le référentiel d'événements, à l'aide du mécanisme requête et rapport, puis de les afficher dans un navigateur Web. Vous pouvez également utiliser l'API pour intégrer des requêtes ou des rapports CA Enterprise Log Manager dans une interface CA ou d'un produit tiers.

Les fonctionnalités de l'API CA Enterprise Log Manager sont les suivantes :

- Appels API authentifiés et sécurisés
- Enregistrement de produits pour authentification unique
- Récupération d'une liste de requêtes ou de rapports filtrée à l'aide d'une balise
- Affichage d'une requête ou d'un rapport dans l'interface CA Enterprise Log Manager interactive afin de les filtrer et de les intégrer dans une interface utilisateur

Vous pouvez obtenir plus d'informations sur l'API dans le *Manuel de programmation API* et dans l'aide en ligne.

Alertes donnant lieu à une action : Intégration de CA IT PAM

Via des alertes planifiées qui interrogent les volumes d'enregistrements de journaux, CA Enterprise Log Manager détecte les éventuelles violations de contrôle et toute activité informatique suspecte. CA Enterprise Log Manager notifie le personnel chargé de la sécurité informatique qui enquête sur chaque alerte de déterminer si une action est requise pour y remédier. Les activités d'investigation typiques concernent souvent la routine et conviennent parfaitement à l'automatisation. Via une intégration étroite entre CA Enterprise Log Manager et CA IT PAM, ces actions de réponse de routine peuvent être effectuées automatiquement. Le personnel chargé de la sécurité informatique n'a pas à se charger des tâches répétitives, et peut donc se concentrer sur les problèmes les plus importants seulement.

L'intégration de CA IT PAM vous permet de créer des requêtes dans CA Service Desk, en exécutant un processus de sortie de l'événement/de l'alerte CA IT PAM prédéfini à partir des alertes. Vous pouvez aussi exécuter des processus de sortie de l'événement/de l'alerte IT PAM personnalisés depuis CA Enterprise Log Manager, qui automatisent d'autres réponses à des événements suspects.

Pour plus de détails, consultez la section "Utilisation de processus d'événement/d'alerte CA IT PAM" du chapitre Alertes d'action du *Manuel d'administration* CA Enterprise Log Manager.

Alertes pouvant être déclenchées : Intégration de SNMP avec des produits NSM

Des alertes sont générées lorsque des requêtes planifiées récupèrent des événements indiquant une activité suspecte. Vous pouvez automatiser l'envoi d'alertes de ce type sous forme d'interruptions SNMP vers des produits de surveillance de sécurité réseau, tels que CA Spectrum ou CA NSM. Vous préparez les produits de destination à recevoir et à interpréter des interruptions SNMP depuis CA Enterprise Log Manager, configurez les emplacements de destination, puis spécifiez les informations d'événement à envoyer.

Pour plus de détails, consultez la section "Utilisation d'interruptions SNMP" du chapitre Alertes d'action du *Manuel d'administration* CA Enterprise Log Manager.

Accès ODBC et JDBC

CA Enterprise Log Manager autorise l'accès en lecture seule aux informations de journal d'événements collectées, à l'aide d'ODBC et de JDBC. Vous pouvez utiliser cet accès pour effectuer des tâches comme :

- Créer des rapports clients à l'aide d'outils tels que BusinessObjects Crystal Reports
- Récupérer les informations du journal sélectionné pour une utilisation avec un moteur de corrélation
- Examiner des journaux pour détecter une intrusion ou un programme malveillant

Les fonctions d'accès ODBC et JDBC utilisent un client que vous installez sur le serveur approprié de votre réseau. Le serveur CA Enterprise Log Manager installe automatiquement ses composants côté serveur pendant la mise à jour de l'abonnement et l'installation.

Pour obtenir des informations d'installation, consultez le *Manuel d'implémentation*. Le *Manuel d'administration* contient des informations de configuration et des exemples.

Pertinence d'identité et d'actif : Intégration de CA IT PAM

L'intégration de CA IT PAM vous permet de maintenir des valeurs mises à jour pour une clé spécifique, en exécutant un traitement des valeurs dynamiques CA IT PAM. Un traitement des valeurs dynamiques est un traitement qui récupère les valeurs actuelles à partir de référentiels qui stockent des données actuelles. Si vous créez un traitement qui récupère des valeurs pour des actifs critiques à partir de votre fichier ou base de données d'actifs, vous pouvez mettre à jour la clé Critical_Assets dans des rapports et des requêtes prédéfinis en cliquant sur un bouton.

Pour plus de détails, consultez la section "Activation de l'importation de valeurs dynamiques" du chapitre Requêtes et rapports du *Manuel d'administration* CA Enterprise Log Manager.

Collecte de journal directe étendue par l'agent par défaut

Lors de l'installation de CA Enterprise Log Manager, l'écouteur Syslog, appelé Syslog_Connector, est déployé sur l'agent par défaut pour permettre la collecte d'événements Syslog. L'intégration de Linux_localsyslog, avec le connecteur associé, Linux_localsyslog_Connector, est également disponible pour collecter des événements Syslog.

L'agent par défaut peut dorénavant collecter directement des éléments autres que les événements Syslog. A l'aide du connecteur WinRm, l'agent par défaut peut collecter des événements de produits exécutés sur des plates-formes Microsoft Windows, comme les services de certificats Active Directory et Microsoft Office Communication Server. A l'aide du connecteur ODBC, l'agent par défaut peut collecter des événements depuis plusieurs bases de données, telles qu'Oracle9i et SQL Server 2005, ainsi que des applications qui stockent leurs événements dans ces bases de données.

Planification automatique des mises à jour pour les clients d'abonnement

Lors de l'installation de votre premier serveur CA Enterprise Log Manager, vous configurez des paramètres globaux pour tous les services, notamment l'abonnement. Pour les abonnements, le premier serveur que vous installez représente le proxy d'abonnement par défaut. Vous configurez l'heure de début et la fréquence de la mise à jour à laquelle ce proxy consulte le serveur d'abonnement CA pour obtenir des mises à jour. Quand vous installez des serveurs supplémentaires, ceux-ci sont, par défaut, installés en tant que clients d'abonnement. Quand vous configurez des serveurs supplémentaires, ceci doit se faire au niveau local. Vous effectuez la configuration locale en sélectionnant le nom du serveur pour configurer et ensuite annuler les configurations globales sélectionnées.

Par défaut, l'heure de début de la mise à jour des clients à abonnement est définie par le paramètre global. Quand le paramètre hérité n'est pas annulé manuellement pour forcer le retard, des problèmes surviennent. Pour empêcher ce problème, la planification des mises à jour pour les clients est désormais automatisée avec un retard de 15 minutes. La planification des mises à jour pour les clients d'abonnement n'exige plus de configuration manuelle.

Chapitre 5 : Fonctionnalités r12.1 SP1 ajoutées et modifiées

Ce chapitre traite des sujets suivants :

Conformité à la norme FIPS 140-2 (page 35)
Modes de fonctionnement (page 36)
Bibliothèques de chiffrement (page 36)
Certificats et fichiers clés (page 38)
Limitations de la prise en charge de la norme FIPS (page 39)
Configuration de Microsoft Internet Explorer pour l'accès à CA Enterprise Log Manager en mode FIPS (page 41)
Configuration de Mozilla Firefox pour l'accès à CA Enterprise Log Manager en mode FIPS (page 41)
Image ISO pour de nouvelles installations (page 43)

Conformité à la norme FIPS 140-2

La norme FIPS (Federal Information Processing Standards) 140-2 est une norme de sécurité pour les bibliothèques cryptographiques et pour les algorithmes qu'un produit doit utiliser pour le chiffrement. Le chiffrement FIPS 140-2 affecte la communication de toutes les données sensibles entre des composants de produits CA et entre des produits CA et des produits tiers. La norme FIPS 140-2 indique la configuration requise pour utiliser des algorithmes cryptographiques dans un système de sécurité protégeant les données sensibles et non classifiées.

CA Enterprise Log Manager offre la compatibilité avec la norme FIPS pour le trafic sécurisé d'événements utilisant des algorithmes conformes à la norme FIPS lors du fonctionnement en mode FIPS. CA Enterprise Log Manager offre également le mode par défaut non FIPS avec lequel le trafic des événements n'est *pas* sécurisé avec les algorithmes conformes à la norme FIPS. Les serveurs CA Enterprise Log Manager d'un réseau fédéré ne peuvent pas utiliser ces deux modes simultanément. Cela signifie qu'un serveur en mode non FIPS ne peut pas partager de requête et de données de rapport avec un serveur fonctionnant en mode FIPS.

Les informations concernant l'activation et la désactivation du mode FIPS sont disponibles dans le *Manuel d'implémentation*, dans la section relative à l'installation de CA Enterprise Log Manager, ainsi que dans l'aide en ligne du service Etat du système.

Informations complémentaires :

Modes de fonctionnement (page 36)
Bibliothèques de chiffrement (page 36)
Algorithmes utilisés (page 37)
Certificats et fichiers clés (page 38)
Limitations de la prise en charge de la norme FIPS (page 39)
Configuration de Microsoft Internet Explorer pour l'accès à CA Enterprise Log Manager en mode FIPS (page 41)
Configuration de Mozilla Firefox pour l'accès à CA Enterprise Log Manager en mode FIPS (page 41)

Modes de fonctionnement

CA Enterprise Log Manager peut fonctionner dans deux modes : mode FIPS et mode non FIPS. Les limites cryptographiques sont les mêmes dans les deux modes, mais les algorithmes sont différents. Par défaut, les serveurs CA Enterprise Log Manager fonctionnent en mode non FIPS. Les utilisateurs possédant le rôle d'administrateur peuvent activer le mode FIPS.

Mode non FIPS

Ce mode mélange des algorithmes de chiffrement pour le transport d'événements et pour les autres communications réalisées entre le serveur CA Enterprise Log Manager et CA EEM qui ne respectent pas forcément les normes FIPS 140-2.

Mode FIPS

Ce mode utilise des algorithmes de chiffrement certifiés FIPS pour le transport d'événements et pour les autres communications réalisées entre le serveur CA Enterprise Log Manager et CA EEM.

Les utilisateurs de niveau administrateur peuvent vérifier les modes de fonctionnement de l'agent dans le noeud Explorateur d'agent de l'onglet Administration, sous-onglet Collecte de journaux.

Pour plus d'informations concernant le passage du mode FIPS au mode non FIPS et inversement, consultez l'aide en ligne, à la rubrique consacrée aux tâches relatives à l'état du système, ou le *Manuel d'implémentation*, à la section concernant la configuration des services.

Bibliothèques de chiffrement

La norme FIPS (Federal Information Processing Standards) 140-2 indique les conditions requises pour l'utilisation des algorithmes cryptographiques dans un système de sécurité protégeant les données sensibles et non classifiées.

CA Enterprise Log Manager intègre également la bibliothèque cryptographique Crypto-C Micro Edition (ME) v2.1.0.2 de RSA, qui a été validée comme conforme les *Conditions de sécurité requises pour les modules cryptographiques* établies par la norme FIPS 140-2. Le numéro de certificat de validation de ce module est 865.

Algorithmes utilisés

Les produits logiciels qui utilisent des modules cryptographiques accrédités par la norme FIPS 140-2 dans leur mode accrédité par la norme FIPS peuvent uniquement utiliser les fonctions de sécurité approuvées par la norme FIPS, telles que AES (algorithme de chiffrement supérieur), SHA-1 (algorithme de hachage sécurisé), et des protocoles de niveau supérieur tels que TLS v1.0, tel que explicitement autorisé dans les normes FIPS 140-2 et dans les manuels d'implémentation.

En mode non FIPS, CA Enterprise Log Manager utilise les algorithmes suivants :

- AES 128
- Triple DES (3DES)
- SHA-1
- MD5
- SSL v3

En mode FIPS, CA Enterprise Log Manager utilise les algorithmes suivants :

- AES 128
- Triple DES (3DES)
- SHA-1
- TLS v1

CA Enterprise Log Manager utilise SHA-1 comme algorithme Digest par défaut pour chiffrer les mots de passe et signer les demandes de serveur.

CA Enterprise Log Manager utilise TLS v1.0 pour la communication avec des annuaires LDAP externes si la connexion LDAP se fait sur TLS, pour la communication entre les composants iTechnology, pour la communication entre l'agent et le service iGateway en mode FIPS et pour le canal d'événements entre un agent et le service logDepot.

Certificats et fichiers clés

Pour la prise en charge de FIPS 140-2, la mise à niveau vers CA Enterprise Log Manager r12.1 SP1 convertit les certificats utilisant le format P12 en certificats utilisant format PEM. Cette conversion aboutit à la génération des fichiers suivants :

- Fichier de certificat avec une extension .cer
- Fichier de clé avec une extension .key

Les fichiers de clé ne sont pas chiffrés et l'utilisateur peut décider d'en sécuriser l'accès sur les hôtes de serveur et d'agent. Le dispositif logiciel CA Enterprise Log Manager utilise plusieurs techniques de durcissement des systèmes d'exploitation pour protéger les clés et les certificats stockés dans le système de fichiers. CA Enterprise Log Manager ne prend pas en charge l'utilisation d'unités de stockage de clés externes.

CA Enterprise Log Manager utilise les certificats et les fichiers de clé suivants :

Nom de certificat/fichier clé	Emplacement	Description
CAELMCert	/opt/CA/SharedComponents/iTechnology (Vous pouvez utiliser le nom variable court ($IGW_LOC) pour accéder à ce répertoire.)	Tous les services CA Enterprise Log Manager utilisent ce certificat pour les communications entre serveurs CA Enterprise Log Manager et entre les serveurs CA Enterprise Log Manager et le serveur CA EEM. Le fichier de configuration CALM.cnf contient une entrée pour ce certificat et pour le fichier de clé correspondant. Les paires de balises commencent par <Certificate> et par <KeyFile> respectivement.
CAELM_AgentCert	$IGW_LOC sur le serveur hôte d'agent	Les agents utilisent ce certificat pour communiquer avec les serveurs CA Enterprise Log Manager. Le serveur de gestion CA Enterprise Log Manager fournit ce certificat à l'agent. Le certificat est valide uniquement pour les serveurs CA Enterprise Log Manager d'une instance d'application donnée.

Nom de certificat/fichier clé	Emplacement	Description
itpamcert	Serveur CA IT PAM	Ce certificat est utilisé pour les communications avec CA IT PAM. Pour plus d'informations, consultez la documentation relative à CA IT PAM.
rootcert	$IGW_LOC	Ce certificat est un certificat racine signé par iGateway pendant l'installation.
iPozDsa	$IGW_LOC	Le serveur CA EEM, aussi bien local que distant, utilise ce certificat. Pour plus d'informations, reportez-vous à la documentation CA EEM.
iPozRouterDsa	$IGW_LOC	Le serveur CA EEM, aussi bien local que distant, utilise ce certificat. Pour plus d'informations, reportez-vous à la documentation CA EEM.
iTechPoz-trusted	/opt/CA/Directory/dxserver/config/ssld	CA Directory utilise ce certificat.
iTechPoz-<nom_hôte>-Router	/opt/CA/Directory/dxserver/config/ssld	CA Directory utilise ce certificat.

Limitations de la prise en charge de la norme FIPS

Les fonctionnalités CA Enterprise Log Manager suivantes et les interopérations de produit ne prennent pas en charge les opérations en mode FIPS :

Accès d'ODBC et de JDBC au magasin de journaux d'événements

ODBC et JDBC sous CA Enterprise Log Manager utilise un SDK sous-jacent qui ne prend pas en charge les opérations en mode FIPS. Les administrateurs de réseaux fédérés qui exigent des opérations FIPS doivent désactiver manuellement le service ODBC sur chaque serveur CA Enterprise Log Manager. Consultez le *Manuel d'implémentation*, à la section relative à la désactivation de l'accès d'ODBC et de JDBC au magasin de journaux d'événements.

Partage d'un serveur CA EEM

CA Enterprise Log Manager r12.1 SP1 utilise CA EEM r8.4 SP3, qui est compatible avec la norme FIPS. L'activation du mode FIPS sur le serveur CA Enterprise Log Manager désactive la communication entre le produit CA EEM partagé et les produits qui ne prennent pas en charge CA EEM r8.4 SP3.

CA IT PAM, par exemple, n'est pas compatible avec la norme FIPS. Si vous procédez à la mise à niveau de votre serveur CA Enterprise Log Manager vers le mode FIPS, un échec d'intégration avec CA IT PAM se produit.

Vous pouvez partager un serveur CA EEM entre CA Enterprise Log Manager r12.1 SP1 et CA IT PAM r2.1 SP2 et r2.1 SP3 uniquement en mode non FIPS.

Si votre installation de CA IT PAM ne partage pas le même serveur CA EEM, CA Enterprise Log Manager r12.1 SP1 peut s'exécuter en mode FIPS et il peut communiquer avec CA IT PAM ; toutefois, ces canaux de communication ne sont pas compatibles avec la norme FIPS.

Correspondance des modes de fonctionnement requise pour les liaisons LDAP

La réussite de la communication avec un magasin d'utilisateurs externes dépend de ce qui suit :

- Les serveurs CA Enterprise Log Manager et leur serveur CA EEM de gestion doivent fonctionner dans le même mode FIPS.
- Si vous utilisez TLS v 1.0 pour la connexion, le serveur CA EEM doit fonctionner dans le même mode FIPS qu'un magasin d'utilisateurs externes sur lequel la norme FIPS est activée.

  Remarque : La compatibilité avec la norme FIPS n'est pas disponible lors de l'utilisation de communications non chiffrées entre le serveur CA EEM et le magasin d'utilisateurs externes ou lorsque le serveur CA EEM et le magasin d'utilisateurs fonctionnent dans des modes FIPS différents.

Interruptions SNMP

Vous pouvez utiliser SNMP V2 ou SNMP V3 pour envoyer des événements SNMP. Les deux sont pris en charge en mode non FIPS.

Si la norme FIPS est activée sur le serveur de destination des interruptions SNMP, vous devez activer la sécurité V3, puis choisir SHA comme protocole d'authentification et AES comme protocole de chiffrement. Effectuez ces sélections dans la page Destination de l'assistant de planification des alertes d'action.

Configuration de Microsoft Internet Explorer pour l'accès à CA Enterprise Log Manager en mode FIPS

Lorsque le mode FIPS est activé, des opérations de configuration supplémentaires peuvent s'avérer nécessaires pour pouvoir afficher l'interface utilisateur du serveur CA Enterprise Log Manager dans votre navigateur. Utilisez la procédure suivante pour définir les options obligatoires pour accéder à CA Enterprise Log Manager dans Microsoft Internet Explorer 7 ou 8.

Remarque : L'accès à un serveur CA Enterprise Log Manager fonctionnant en mode FIPS n'est pas possible dans Microsoft Internet Explorer 6.

Configuration de Microsoft Internet Explorer 7 ou 8

1. Ouvrez le navigateur et sélectionnez Outils, Options Internet.
2. Sélectionnez l'onglet Avancé et descendez jusqu'à la section Sécurité.
3. Sélectionnez l'une des options suivantes :
   - Utiliser SSL 2.0
   - Utiliser SSL 3.0
   - Utiliser TLS 1.0
4. Cliquez sur OK.

Configuration de Mozilla Firefox pour l'accès à CA Enterprise Log Manager en mode FIPS

Lorsque le mode FIPS est activé, des opérations de configuration supplémentaires peuvent s'avérer nécessaires pour pouvoir afficher l'interface utilisateur du serveur CA Enterprise Log Manager dans votre navigateur. Pour définir les options d'accès à un serveur CA Enterprise Log Manager fonctionnant en mode FIPS dans Mozilla Firefox 3.5.8 (ou version ultérieure), utilisez la procédure suivante.

Remarque : L'accès à CA Enterprise Log Manager requiert l'installation du module d'extension Mozilla Firefox pour Adobe Flash 9 ou 10.

Pour configurer Mozilla Firefox :

1. Ouvrez le navigateur et sélectionnez Tools (Outils), Options.
2. Cliquez sur l'onglet Advanced (Avancé), puis sur le sous-onglet Encryption (Chiffrement).
3. Sélectionnez les deux options suivantes :
   - Utiliser SSL 3.0
   - Utiliser TLS 1.0
4. Sélectionnez le sous-onglet Security (Sécurité), puis indiquez que vous souhaitez utiliser un Master Password (Mot de passe principal).
5. Cliquez sur Change Master Password (Modifier le mot de passe principal) et entrez un mot de passe dans la fenêtre qui s'affiche, puis cliquez sur OK.
6. Cliquez sur le sous-onglet Advanced (Avancé).
7. Cliquez sur Security Devices (Périphériques de sécurité).

   La fenêtre Device Manager (Gestionnaire de périphériques) s'affiche.
8. Sélectionnez le module NSS Internal PKCS #11 (PKCS #11 interne NSS) dans le volet gauche.

   Cette action remplit les données du volet droit.
9. Sélectionnez la ligne NSS Internal PKCS #11 Module et cliquez sur Enable FIPS.
10. Lorsque vous y êtes invité, saisissez le mot de passe principal que vous avez créé précédemment, puis cliquez sur OK.
11. Dans la fenêtre Device Manager (Gestionnaire d'unités), cliquez sur OK.
12. Pour fermer la boîte de dialogue Options, cliquez sur OK.
13. Redémarrez le navigateur.

Informations complémentaires :

Mise à niveau par abonnement (page 11)

Image ISO pour de nouvelles installations

Le Service Pack comprend une image ISO que vous permettra de déployer rapidement CA Enterprise Log Manager ou d'ajouter un nouveau serveur CA Enterprise Log Manager à un déploiement existant. L'image ISO est disponible dans la section Downloads (Téléchargements) sur le site du support en ligne.

Nous vous recommandons d'utiliser l'image ISO la plus récente dans les cas suivants :

- Déploiement de CA Enterprise Log Manager. L'installation de l'image ISO la plus récente permet de réduire le nombre de mises à niveau des souscriptions requises et d'accélérer le déploiement.
- Ajout d'un nouveau serveur CA Enterprise Log Manager après la mise à niveau des serveurs dans un déploiement existant. Indiquez d'abord que les serveurs et les agents du déploiement actuel sont correctement mis à niveau et qu'ils reçoivent correctement les événements. Installez ensuite les nouveaux serveurs au moyen de l'image ISO pour augmenter les capacités et réduire le nombre de mises à jour des souscriptions requises.

Remarque : La procédure d'installation a été modifiée. Une nouvelle invite vous demande si vous voulez effectuer une installation en activant le mode FIPS. Lorsque vous ajoutez un nouveau serveur CA Enterprise Log Manager à un déploiement FIPS existant (le serveur de gestion CA Enterprise Log Manager ou le serveur CA EEM distant utilisent le mode FIPS), activez le mode FIPS pendant l'installation. Si vous n'activez pas ce mode, vous ne pourrez pas enregistrer le nouveau serveur et vous devrez réinstaller. Pour plus d'informations sur le mode FIPS, consultez le *Manuel d'implémentation*.

Chapitre 6 : Problèmes connus

Ce chapitre traite des sujets suivants :

Agents et adaptateurs CA (page 45)
Dispositif (hors interface utilisateur) (page 54)
Ajustement d'événement (page 58)
Requêtes et rapports (page 59)
Abonnement (page 63)
Gestion des utilisateurs et des accès (page 70)
Divers (page 72)

Agents et adaptateurs CA

Les problèmes connus relatifs aux agents et aux adaptateurs CA sont répertoriés ci-dessous.

Dépendance d'installation d'un agent sous Red Hat Linux 4

Symptôme :

Lorsque vous installez l'agent CA Enterprise Log Manager sur des systèmes Red Hat Enterprise Linux 4, l'installation échoue et affiche un message d'erreur signalant des dépendances d'installation.

Solution :

L'agent CA Enterprise Log Manager sur Red Hat Enterprise Linux 4 nécessite le package de développement logiciel. Installez cet ancien package de développement logiciel avant d'installer l'agent.

Précision de l'heure de l'état de l'Agent selon la configuration du serveur NTP

Symptôme :

Si plusieurs serveurs CA Enterprise Log Manager de collecte sont définis manuellement sur des horloges différentes, les heures indiquées pour l'activité de l'agent risquent de diverger.

Solution :

Indiquez un serveur NTP à chaque installation du produit CA Enterprise Log Manager dans votre réseau. La configuration d'un serveur NTP pour chaque serveur synchronise l'heure indiquée pour les agents gérés par différents serveurs.

Prévision d'un délai pour la mise à jour après le déploiement du connecteur en bloc

Symptôme :

Les nouveaux connecteurs ne s'affichent pas immédiatement dans l'explorateur d'agent après la réalisation d'un déploiement du connecteur en bloc.

Solution :

En fonction du nombre de connecteurs, et des agents sur lesquels vous les déployez, attendez quelques minutes pour effectuer la mise à jour de tous les connecteurs situés dans l'explorateur d'agent.

Le déploiement du connecteur en bloc avec une adresse IPv6 n'est pas correct

Symptôme :

Le déploiement de connecteurs, à partir de l'assistant Déploiement du connecteur en bloc qui fournit l'adresse du serveur au format IPV6, ne fonctionne pas comme prévu. Après un certain moment, l'état du connecteur affiche Exécution en cours. Quand vous modifiez le connecteur, vous pouvez constater que le nom du serveur n'affiche que les quatre premiers chiffres de l'adresse IPV6. Les noms d'utilisateur, mots de passe et champs du domaine s'affichent sans être renseignés.

Solution :

L'interface utilisateur CA Enterprise Log Manager envoie le contenu du fichier source en utilisant deux points doubles (::) comme délimiteur séparant chaque source. L'adresse IPv6 contenant des caractères deux points doubles (::), ceux-ci sont traités comme des délimiteurs. L'enregistrement du connecteur n'est pas enregistré correctement.

N'utilisez pas des adresses IPv6 pour effectuer un déploiement du connecteur en bloc. Vous *pouvez* utiliser des noms d'hôte pour configurer le déploiement en bloc des connecteurs. Vous pouvez également configurer un connecteur IPv6 dans l'assistant Création d'un connecteur en utilisant les instructions normales.

Le nom de montage du DVD ne peut pas contenir d'espaces

Symptôme :

Lorsque vous installez un agent manuellement sur un ordinateur Linux, à partir du DVD-ROM du produit, un message d'autorisation refusée s'affiche et l'installation s'arrête.

Solution :

Pour installer un agent à partir du DVD, montez le lecteur de DVD au moyen d'une commande similaire à la commande ci-après :

```
$ mount /dev/cdrom <chemin_local>
```

Le DVD-ROM ne peut pas être monté sur un nom de chemin local (répertoire) dont le nom contient des espaces. Montez le DVD-ROM sur un nom de répertoire ne contenant pas d'espaces, puis installez l'agent.

Echec de la configuration de la source d'événement au niveau du domaine

Symptôme :

La configuration d'un connecteur, de sorte qu'il accède à une source d'événement Windows et lise ses journaux, implique la création d'un compte d'utilisateur à faibles privilèges et l'affectation des autorisations nécessaires à celui-ci. Quand la source d'événement est un hôte Windows Server 2003 SP1, l'une des étapes consiste à définir la stratégie de sécurité locale, à savoir *Emprunter l'identité d'un client après l'authentification*. Quand ce droit d'utilisateur est défini localement, aucun problème ne survient. Cependant, si ce paramètre est appliqué comme stratégie de domaine sur tous les serveurs, l'application globale entraînera la suppression des affectations locales des autres utilisateurs, à savoir les Administrateurs et SERVICE.

Un article du support Microsoft stipule que "... les problèmes se produisent lorsqu'une stratégie de groupe qui définit que le droit d'utilisateur Emprunter l'identité d'un client après l'authentification est lié au domaine. Ce droit d'utilisateur doit être lié uniquement à un site ou à une unité d'organisation (OU)."

Solution :

Consultez l'article 930220 de la Base de connaissances Microsoft pour obtenir des conseils sur la restauration d'une connectivité TCP/IP complète en désactivant les services IPSec et en redémarrant l'ordinateur, et pour consulter les étapes permettant d'ajouter à nouveau les administrateurs et les groupes SERVICE en tant que paramètre de stratégie de groupe. Essayez le lien suivant :

http://support.microsoft.com/kb/930220/fr-fr (traduction automatique).

Microsoft recommande également les méthodes suivantes pour résoudre des problèmes provoqués par l'application du paramètre Emprunter l'identité d'un client après l'authentification en tant que stratégie de groupe :

- Méthode 1 : modifier les paramètres de la stratégie de groupe
- Méthode 2 : modifier le registre

Consultez l'article 911801 de la Base de connaissances Microsoft pour obtenir les étapes d'implémentation des deux solutions recommandées. Essayez le lien suivant :

http://support.microsoft.com/kb/911801/fr-fr (traduction automatique).

Retard d'ODBC et de JDBC suite à l'activation de la communication SSL

Symptôme :

Lorsque la communication agent-serveur CA Enterprise Log Manager est en mode non FIPS, l'activation de la communication SSL entraîne une brève interruption de la communication avec ODBC ou JDBC.

Solution :

Si vous utilisez ODBC ou JDBC et que vous activez SSL, la communication avec le serveur CA Enterprise Log Manager peut ne pas être immédiate. Attendez environ cinq minutes pour que la communication soit restaurée.

SuSE Linux non pris en charge dans les intégrations de la version 4.0.0.0 du détecteur de journaux

Symptôme :

Après la mise à niveau de CA Enterprise Log Manager 12.1 directement vers 12.1 SP1, une instruction incorrecte s'affiche concernant la prise en charge de plate-forme dans l'assistant d'intégration. Si vous sélectionnez la version 4.0.0.0 du détecteur de journaux à la première étape de l'assistant, "Linux_X86_32 SLES11" s'affiche dans la liste de plates-formes disponibles.

Solution :

Ces informations sont incorrectes, SuSE Linux n'est pas pris en charge pour le détecteur de journaux 4.0.0.0. Veuillez ignorer l'instruction. Vous ne pouvez donc pas créer d'intégration personnalisée à l'aide de ce détecteur de journaux.

Restriction sur la configuration des ports

Symptôme :

Lorsque l'écouteur Syslog est configuré avec le port UDP par défaut sur un agent s'exécutant en tant qu'utilisateur non root sur un hôte Linux, le port UDP 514 (port par défaut pour Syslog) n'est pas ouvert et aucun événement Syslog n'est collecté sur ce port.

Solution :

Si l'agent s'exécute en tant qu'utilisateur non root sur un système UNIX, remplacez les ports de l'écouteur Syslog par des ports d'un numéro supérieur à 1 024 ou modifiez le service pour qu'il s'exécute en tant que root.

Risque de diminution des performances en cas de sélection d'un nombre trop important d'intégrations

Symptôme :

Les performances de l'agent par défaut diminuent quand vous spécifiez un trop grand nombre d'intégrations syslog par défaut pour un connecteur. Dans ce cas, les performances sont liées au nombre d'événements par seconde (eps) gérés.

Solution :

Pour chaque intégration, CA Enterprise Log Manager charge des fichiers d'analyse de message (XMP) et de mappage de données (DM). Pendant les opérations, CA Enterprise Log Manager vérifie les événements entrants par rapport aux listes d'expressions régulières. Un plus grand nombre de fichiers prolonge la durée du traitement.

Evitez le ralentissement des performances en supprimant les intégrations inutiles lors de la création d'un connecteur syslog. Après l'installation, vérifiez les intégrations configurées pour le connecteur syslog par défaut et supprimez celles qui ne vous sont pas utiles.

La suppression d'un serveur dans une fédération ne supprime pas l'agent par défaut

Symptôme :

Lors de la suppression d'un serveur CA Enterprise Log Manager dans un groupe de serveurs fédérés, l'agent par défaut du serveur supprimé n'est pas retiré de son groupe d'agents associé.

Solution :

Utilisez le sous-onglet Explorateur d'agent pour supprimer manuellement l'agent dans son groupe.

Les rapports sur les données collectées par le collecteur SAPI de CA n'affichent pas les événements correctement

Symptôme :

Certains champs d'événements collectés à l'aide du collecteur SAPI de CA Audit ne sont pas remplis correctement. En conséquence, la plupart des rapports ne présentent pas ces données comme prévu.

Solution :

Pour collecter les événements provenant de votre infrastructure CA Audit existante, utilisez le routeur SAPI de CA Audit.

La section Remarques pour les utilisateurs de CA Audit du *Manuel d'implémentation* contient des informations supplémentaires sur la configuration du routeur SAPI.

Remise de Syslogs via UDP non garantie

Symptôme :

L'utilisation du protocole UDP de l'écouteur Syslog pour la collecte directe de Syslogs peut poser problème pour la remise garantie.

Solution :

Envisagez d'utiliser un mécanisme local de collecte Syslog pour contourner des problèmes potentiels de remise garantie. Vous pouvez configurer un écouteur Syslog sur un agent installé avec la source d'événement Syslog.

Remarque : Utilisez le port 514, réservé à Syslog, uniquement si l'agent s'exécute en tant qu'utilisateur root. Si l'agent s'exécute en tant qu'utilisateur avec moins de droits, ce qui est recommandé, affectez un port privé. Les ports privés sont numérotés de 49 152 à 65 535.

Conflit de services Syslog sous UNIX

Symptôme :

Dans le scénario suivant, CA Enterprise Log Manager ne reçoit aucun événement Syslog :

Ordinateur 1

Serveur CA Enterprise Log Manager écoutant des événements Syslog provenant de l'ordinateur 2.

Ordinateur 2

Ordinateur RHEL 4.0 avec agent local contenant un connecteur Syslog et envoyant ses événements à l'ordinateur 1 en utilisant l'écouteur Syslog.

Ordinateur 3

Ordinateur UNIX envoyant des événements à l'ordinateur 2 à l'aide du connecteur qui y est installé.

Dans ce cas, l'ordinateur de l'agent ne peut pas capturer les événements provenant de l'ordinateur 3, car le service Syslog du système d'exploitation et le connecteur Syslog s'exécutent sur le même système.

Solution :

Arrêtez le service Syslog sur l'Ordinateur 2 pour recevoir des événements de l'Ordinateur 3 (l'ordinateur UNIX). Vous pouvez également reconfigurer l'environnement afin que les services Syslog ne soient pas en conflit sur le même ordinateur.

Le détecteur de journaux WMI génère plusieurs événements de privilège d'utilisateur

Symptôme :

Lors de l'utilisation d'un connecteur avec le détecteur de journaux WMI pour collecter des événements, vous pouvez observer des événements multiples liés à l'utilisation des privilèges".

Solution :

Ces événements apparaissent si la stratégie d'audit Windows qui enregistre des actions d'utilisation de privilèges ayant abouti, est activée sur le système cible. Ils sont produits par le processus de rassemblement des événements et ne témoignent d'aucun problème. Vous pouvez créer une règle de suppression pour empêcher CA Enterprise Log Manager de les recevoir si vous ne voulez pas qu'ils s'affichent.

Arrêt de la réception d'événements par le détecteur de journaux de fichier texte sur un système d'agent Solaris

Symptôme :

Le détecteur de journaux de fichier texte cesse de recevoir des événements sur un système d'agent Solaris.

Le fichier journal du connecteur contient une erreur indiquant qu'un fichier de bibliothèque (libssl.so.0.9.7) n'a pas réussi à s'ouvrir :

```
[4] 20/07/10 18:55:50 ERROR :: [ProcessingThread::DllLoad] :Error is: ld.so.1:
caelmconnector: fatal: libssl.so.0,9.7: open failed: No such file or directory
[4] 20/07/10 18:55:50 ERROR :: [ProcessingThread::run] Dll Load and Initialize
failed, stopping the connector ...
[3] 20/07/10 18:55:50 NOTIFY :: [CommandThread::run] Cmd_Buff received is START
```

Solution :

Identifiez l'emplacement de la bibliothèque pour permettre à l'agent de recevoir des événements.

Pour résoudre l'erreur sur le système de l'agent Solaris :

1. Accédez au dossier /etc. Exemple :

   ```
   cd /etc
   ```

2. Ouvrez le fichier profile du dossier etc. Exemple :
   ```
   vi /etc/profile
   ```

3. Ajoutez les deux lignes suivantes à la fin du fichier profile :

   ```
   LD_LIBRARY_PATH=/usr/sfw/lib:$LD_LIBRARY_PATH
   ```

   ```
   export LD_LIBRARY_PATH
   ```

4. Fermez la session active dans le système de l'agent Solaris.
5. Ouvrez une nouvelle session sur le système de l'agent Solaris.
6. Arrêtez l'agent CA Enterprise Log Manager sur le système Solaris. Exemple :

   ```
   /opt/CA/ELMAgent/bin/S99elmagent stop
   ```

7. Démarrez l'agent CA Enterprise Log Manager sur le système Solaris. Exemple :

   ```
   /opt/CA/ELMAgent/bin/S99elmagent start
   ```

   Le détecteur de journaux de fichier texte commence à recevoir des événements et l'erreur ne s'affiche plus dans le fichier journal.

Capacité de réponse nulle de l'agent lors de la présence d'un nombre très élevé d'événements dans le flux

Symptôme :

Un agent CA Enterprise Log Manager ne répond plus et arrête d'accepter des événements. Le message d'erreur suivant apparaît dans le fichier caelmdispatcher.log :

```
[275] 12/07/10 14:32:05 ERROR :: FileQueue::PutEvents Unable to write to new event file
[275] 12/07/10 14:32:05 ERROR :: WriterThread::run Unable to push events to FileQueue, Retrying
[275] 12/07/10 14:32:10 NOTIFY :: FileQueue::UpdateCurrentWriterFile Reached Max files configured limit=10, Not creating any new files for now
```

Solution :

Cela indique que le taux d'événements entrants pour le matériel dans l'environnement est très élevé. Vous pouvez résoudre ce problème en reconfigurant l'agent, en procédant comme suit :

1. Cliquez sur Administration, allez dans l'onglet Collecte de journaux et développez le dossier Explorateur d'agent.
2. Sélectionnez l'agent à reconfigurer, cliquez sur Modifier et réglez les paramètres suivants :

   Nombre maximum de fichiers

   Définit le nombre maximum de fichiers pouvant être créés dans la file d'attente de fichiers de réception d'événements. Le nombre maximum est limité à 1 000 fichiers. Le paramètre par défaut est 10.

   Taille maximum par fichier

   Définit la taille maximum, en Mo, pour chaque fichier de la file d'attente de fichiers de réception d'événements. Quand un fichier atteint la taille maximum, CA Enterprise Log Manager en crée un nouveau. La taille maximum est de 2048 Mo. Le paramètre par défaut est 100 Mo.

   Vous pouvez régler ces paramètres plus tard selon les besoins de votre environnement le taux d'événements par seconde.

Dispositif (hors interface utilisateur)

Les problèmes connus relatifs au dispositif logiciel (et non à l'interface utilisateur CA Enterprise Log Manager) sont répertoriés ci-dessous.

Connexion impossible au serveur CA Enterprise Log Manager sous le nom d'utilisateur EiamAdmin

Symptôme :

Le nom d'utilisateur EiamAdmin et son mot de passe ne sont pas reconnus lorsque vous tentez de vous connecter au serveur CA Enterprise Log Manager (sans utiliser l'interface utilisateur).

Solution :

Pour effectuer des tâches de maintenance, telles que la configuration de l'archivage, l'installation crée un autre nom d'utilisateur, caelmadmin, et lui affecte le même mot de passe que celui fourni à EiamAdmin par le programme d'installation. Utilisez le nom d'utilisateur caelmadmin et son mot de passe pour vous connecter au serveur CA Enterprise Log Manager.

Pour plus d'informations, consultez Comptes d'utilisateur par défaut dans le *Manuel d'implémentation*.

Nombre excessif de fichiers journaux ELMAdapter

Symptôme :

Un grand nombre de fichiers journaux d'adaptateurs peuvent s'accumuler sur le serveur CA Enterprise Log Manager. Cela est atypique, car la norme est que les messages enregistrés doivent s'ajouter dans un seul fichier journal. Ce problème peut être provoqué par l'activation du traçage.

Pour déterminer l'existence de ce problème

1. Planifiez des rapports et des alertes, puis exécutez des requêtes ODBC, telles que la suivante :

   ```
   select event_logname,count(*) from view_event where event_time_gmt >=
   timestampadd(hh,-1,now()) AND event_time_gmt <= now() group by event_logname;
   ```

2. Connectez-vous au serveur CA Enterprise Log Manager à l'aide de SSH et fournissez le nom d'utilisateur et le mot de passe caelmadmin.
3. Utilisez l'accès su à la racine et fournissez le mot de passe racine.
4. Accédez au dossier iTechnology.

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

5. Déterminez si un nombre excessif de fichiers journaux a été créé en raison de la requête lancée via les pilotes ODBC. Ces fichiers sont nommés ELMAdapter_<oaserverpid>_-IP.log.

Solution :

Si le problème existe, assurez-vous que le traçage des erreurs a été désactivé de la façon suivante :

1. Connectez-vous au serveur de gestion CA Enterprise Log Manager à l'aide de SSH et fournissez le nom d'utilisateur et le mot de passe caelmadmin.
2. Utilisez l'accès su à la racine et fournissez le mot de passe racine.
3. Accédez au dossier iTechnology.

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

4. Ouvrez oaserver-dm.ini pour le modifier.
5. Faites défiler jusqu'à [Service_0] et assurez-vous que le traçage est désactivé. Si tel n'est pas le cas, modifiez-le en suivant l'exemple suivant :

   ```
   ServiceDebugLogLevel=0
   ServiceIPLogOption=Disable All Tracing
   ```

6. Redémarrez le service ODBC comme suit :
   a. Cliquez sur l'onglet Administration et le sous-onglet Services.
   b. Cliquez sur Serveur ODBC3.
   c. Effectuez l'une des opérations suivantes :

- Si la fonction Activer le service n'est pas sélectionnée, sélectionnez-la et cliquez sur Enregistrer.
- Si la fonction Activer le service est sélectionnée, décochez la case Activer le service, cliquez sur Enregistrer, sélectionnez Activer le service et cliquez à nouveau sur Enregistrer.

L'importation manuelle de fichiers d'analyse peut nécessiter la modification de la valeur d'expiration

Parfois, un problème peut survenir lors de l'importation de fichiers d'analyse (.XMP) pendant l'installation de CA Enterprise Log Manager. Ce problème se produit la plupart du temps lors de l'installation de CA Enterprise Log Manager sur des serveurs qui ne respectent pas la configuration matérielle minimum ou qui se trouvent sur des réseaux lents.

Symptôme :

Pendant l'installation, une erreur se produit lors de l'importation des fichiers d'analyse. Vous pourrez résoudre ce problème une fois l'installation terminée. Exécutez le script fourni, *EEM/content/ImportCALMXMP.sh* pour importer les fichiers manuellement (vous trouverez de plus amples informations sur ce script dans le *manuel d'implémentation*). En général, cette action résout l'erreur.

Cependant, il arrive que le routeur Cisco ne puisse pas importer le fichier XMP lors de l'exécution du script d'importation manuelle. L'installation du serveur CA Enterprise Log Manager a abouti. Mais l'échec de l'importation du fichier XMP empêche l'installation des connecteurs par défaut sur l'agent local. Vous ne pouvez pas déployer les connecteurs avant d'avoir importer manuellement les fichiers XMP.

Solution :

Si la valeur d'expiration par défaut dépasse celle indiquée dans le script *EEMImportUtility.sh*, cela entraînera un problème d'importation du fichier XMP. Le script *ImportCALMXMP.sh* appelle le script *EEMImportUtility.sh*. La valeur d'expiration par défaut est de 4 minutes. Définissez le délai avant expiration par défaut sur 6 minutes pour permettre un délai suffisant à une importation manuelle sur des serveurs plus lents.

Pour modifier la valeur par défaut du délai avant expiration :

1. Accédez au répertoire EEM/content.
2. Modifiez le fichier, ImportCALMXMP.sh.
3. Localisez la ligne suivante et modifiez la valeur du délai avant expiration comme indiqué ci-après :

   ```
   ./EEMImportUtility.sh -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP" to "./EEMImportUtility.sh -timeout 360000 -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP
   ```

   Remarque : La valeur du délai avant expiration est exprimée en millisecondes.
4. Enregistrez et fermez le fichier.
5. Exécutez le script à nouveau.
6. Déployez manuellement les connecteurs pour syslog et Linux_LocalSyslog sur l'agent par défaut.

Ajustement d'événement

Les problèmes connus relatifs à l'ajustement d'événement sont répertoriés ci-dessous.

Une chaîne de mappage de blocs et des valeurs numériques exigent des opérateurs différents

Symptôme :

Lorsque vous utilisez l'assistant de mappage, les valeurs de mappage de blocs pour des colonnes numériques ou de chaînes de texte ne se comportent pas comme prévu.

Solution :

Lorsque vous créez des mappages de blocs, l'opérateur "Egal à" peut être utilisé uniquement sur les colonnes numériques. Utilisez l'opérateur "Correspondance" pour toutes les colonnes de chaîne de texte.

Impossibilité pour les fichiers DM personnalisés de mapper des événements epSIM (iTech)

Symptôme :

Les fichiers de mappage de données (DM) personnalisées créés pour les événements epSIM (iTechnology) ne peuvent pas mapper les événements après avoir été appliqués au module d'extension iTechnology EventPlugin sous Adaptateurs CA dans l'explorateur de collections de journaux.

Lorsque vous examinez la requête Tous les événements du système pour déterminer si les événements iTech sont mappés selon le fichier DM personnalisé, vous découvrez que les événements iTech ne sont pas mappés et qu'ils ne sont donc pas renvoyés comme résultat de la requête. Le message "Impossible de mapper les événements, car aucun événement n'a été mappé" s'affiche.

Solution :

Ouvrez le fichier DM personnalisé et remplacez $EventLog par $Log. Par exemple :

Modifiez cette ligne : <DM_Field name="event_logname" type="string" value="$EventLog" mapping="direct"/>

par la ligne suivante : <DM_Field name="event_logname" type="string" value="$Log" mapping="direct"/>

Ce changement garantit le mappage des événements. Pendant l'analyse du mappage, ignorez les messages ultérieurs qui indiquent que certains événements n'ont pas été mappés.

Requêtes et rapports

Les problèmes connus relatifs aux requêtes et aux rapports sont répertoriés ci-dessous.

Les résultats de la requête d'alertes d'action peuvent être incomplets

Symptôme :

Quand une alerte d'action est générée, vous pouvez consulter les résultats de la requête immédiatement dans CA Enterprise Log Manager. Pour afficher les résultats dans CA Enterprise Log Manager, cliquez sur l'onglet Gestion des alertes, le sous-onglet Alertes d'action, puis sélectionnez le nom de l'alerte. Les résultats s'affichent dans un graphique. Quand l'alerte d'action appelle un processus de sortie de l'événement/de l'alerte qui ouvre un cas d'assistance CA Service Desk, une URL s'affiche dans le problème du service d'assistance. Quand vous accédez à cette URL et que vous vous connectez, les résultats de la requête pour l'alerte s'affichent sur une seule page. Si vous comparez ces résultats à ceux affichés sur le sous-onglet Alertes d'action, vous remarquerez que les résultats de la requête ne correspondent pas. Par exemple, si les résultats sont affichés pour Nombre, les nombres sur la fenêtre affichée à partir de l'URL risquent d'être supérieurs à ceux affichés dans CA Enterprise Log Manager. Ce problème peut se produire sur des systèmes lourdement chargés quand l'heure de fin dynamique définie pour les Conditions de résultat de l'alerte est inadéquate. Un paramètre inadéquat est un paramètre qui ne laisse pas assez de temps pour que la mise à jour de la base de données se produise avant la lecture de la base de données. La probabilité de cette occurrence a été atténuée grâce à la définition de l'heure de fin dynamique sur Maintenant, -2 minutes pour la plage prédéfinie 5 dernières minutes.

Solution :

Modifiez l'heure de fin dynamique dans l'étape Conditions de résultat de l'alerte d'action, dont la valeur est Maintenant, -2 minutes, par une valeur qui accorde plus de temps, par exemple, Maintenant, -10 minutes.

Restriction sur les requêtes avec plusieurs termes de recherche

Symptôme :

Une requête sur une seule colonne de recherche effectue une recherche sans respecter la casse, comme prévu. Toutefois, une requête sur plusieurs colonnes de recherche respecte la casse et interprète les astérisques (*) littéralement, au lieu de les interpréter comme des caractères génériques. Ce problème survient lorsque le code SQL généré en interne contient un opérateur OR dans la clause Where.

Solution :

Lorsque vous utilisez des invites, limitez vos requêtes aux recherches sur une seule colonne. Si vous créez votre propre requête contenant plusieurs expressions, utilisez l'opérateur logique ET pour connecter vos expressions multiples COMME avec caractères génériques.

Le filtre simple de l'assistant des requêtes échoue lors de l'utilisation de caractères spéciaux

Symptôme :

Les filtres simples de l'assistant des requêtes échouent quand vous saisissez des caractères spéciaux dans une valeur de champ du filtre simple. Vous pouvez enregistrer et exécuter la requête avec les caractères spéciaux suivants :

```
( ) & * > < ? : } {
```

Cependant, la requête s'exécute sans ce champ comme filtre et les données s'affichent même si la condition de correspondance échoue.

Solution :

N'utilisez pas les caractères spéciaux répertoriés dans les valeurs d'un champ du filtre simple.

L'état d'un job planifié ne s'affiche pas après une mise à niveau

Symptôme :

Dans l'onglet Rapports planifiés, sous-onglet Planification de rapport, vous pouvez afficher tous les jobs planifiés et leur état. La colonne Etat affiche Génération en cours pendant le processus de génération du rapport, puis Planifiés lorsque le job est planifié. Après une mise à niveau à partir de la version de base r12.0 GA, la colonne Etat des rapports est effacée, quel que soit l'état du rapport. Lorsqu'un rapport planifié est généré à nouveau, son état s'affiche correctement.

Solution :

L'absence de valeur dans la colonne Etat d'un job planifié est un problème d'affichage temporaire. Aucune mesure à prendre. L'état correct s'affiche dès la prochaine génération du rapport.

Echec de certains jobs d'alerte d'action planifiés trop fréquemment

Symptôme :

Les jobs qui se chevauchent échouent parfois, lorsqu'une alerte d'action qui interroge les événements générés pendant un intervalle donné est planifiée pour s'exécuter plus fréquemment que cet intervalle. Le message suivant s'affiche : "Echec de la génération de l'alerte, car la requête précédente est en cours". Si, par exemple, vous demandez des événements spécifiques générés au cours des trois dernières heures, mais que vous définissez la requête de façon à ce qu'elle s'exécute toutes les heures, le deuxième job commencera avant que le premier job ne soit terminé. Dans ce cas, CA Enterprise Log Manager continue de traiter le premier job planifié et envoie des messages d'échec pour les deux jobs planifiés suivants. Dès que l'intervalle de trois heures s'écoule, une alerte est envoyée si un événement satisfaisant les critères de requête se produit et le traitement de la prochaine exécution de cette alerte commence.

Solution :

Si vous spécifiez uniquement une plage de dates dans l'étape Conditions de résultat, sélectionnez un intervalle récurrent *égal à* l'intervalle que vous avez défini pour Sélection d'une plage de dates. Par exemple, si vous souhaitez connaître les événements satisfaisant des critères spécifiques et qui ont été générés au cours des trois dernières heures, vous devez entre une valeur dans l'option Sélection d'une plage de dates, à l'étape Conditions de résultat, comme ceci :

Heure de fin dynamique : maintenant ou -2 minutes

Heure de début dynamique : maintenant ou -182 minutes

Lorsque vous définissez la planification, vous devez définir l'intervalle de récurrence (étape Jobs de planification) sur une valeur égale à 3 heures (180 minutes) comme suit :

Intervalle de récurrence : 3 heures

La définition d'un intervalle de requête et d'un intervalle de récurrence identiques garantit l'enregistrement de toutes les occurrences d'événement respectant les critères de requête dans une alerte générée. Cette recommandation ne s'applique pas si vous spécifiez un intervalle pour des événements groupés.

Impossible de supprimer des balises qui contiennent des caractères spéciaux

Symptôme :

Les tentatives de suppression d'une requête ou d'une balise de rapport qui contient les caractères spéciaux suivants, ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ?, échouent.

Solution :

N'utilisez pas les caractères spéciaux indiqués lors de la création de balises de requête et de rapport.

Abonnement

Les problèmes connus relatifs à l'abonnement sont répertoriés ci-dessous.

Redémarrage automatique après mise à jour du SE lors d'une mise à niveau de SP

Symptôme :

Si l'option d'abonnement Redémarrage automatique après mise à jour du SE est définie sur oui lorsque vous appliquez la mise à jour du Service Pack, le système d'exploitation redémarre avant la fin de la mise à jour des fichiers binaires CA Enterprise Log Manager. En particulier, la mise à jour des scripts d'arrêt d'iGateway reste incomplète. Cette mise à jour doit être appliquée afin qu'iGateway puisse être arrêté correctement en cas de redémarrage du système d'exploitation.

Solution :

Avant d'appliquer la mise à jour de Service Pack du module Gestionnaire de journaux, définissez sur Non l'option d'abonnement Redémarrage automatique après mise à jour du SE.

Erreur de manque de mémoire sur les ordinateurs disposant de peu de mémoire

Symptôme :

Le téléchargement d'une mise à jour d'abonnement sur un ordinateur disposant de moins de mémoire que les 8 Go recommandés échoue et signale une erreur Java de manque de mémoire. D'importants packages étaient téléchargés à l'aide d'iGateway en l'absence d'un paramètre de taille de tas JVM (Java Virtual Machine, ordinateur virtuel Java).

Solution :

Si vous installez CA Enterprise Log Manager sur du matériel doté de moins de 8 Go de mémoire, modifiez la taille de tas JVM.

Pour modifier la taille de tas JVM :

1. Connectez-vous au serveur CA Enterprise Log Manager en tant que caelmadmin.
2. Accédez au dossier iGateway.
3. Ouvrez le fichier caelm-java.group et localisez la section relative aux paramètres du JVM.
4. Ajoutez la nouvelle ligne, comme affichée dans l'illustration suivante en gras :

```
<JVMSettings>
                <loadjvm>true</loadjvm>
                <javahome>/usr/java/latest/jre</javahome>
                <Properties
name="java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed">
                        <system-
properties>java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed</
system-properties>
                </Properties>
        <Properties name="maxmemory"><jvm-property>-Xmx1250M</jvm-
property></Properties>
        </JVMSettings>
```

5. Enregistrez le fichier caelm-java.group, puis fermez-le.

Important : Le fait de définir la taille du tas JVM peut causer des problèmes lors de l'utilisation de l'option Exporter au format PDF sur de grands ensembles de données. Il est donc recommandé d'utiliser cette option sur les petits ordinateurs uniquement.

La modification des informations d'identification de proxy verrouille le compte de domaine

Symptôme :

Dans un environnement comportant un serveur CA Enterprise Log Manager, les informations d'identification de votre domaine peuvent ne pas fonctionner et votre compte est verrouillé.

Solution :

Le serveur CA Enterprise Log Manager contacte régulièrement le serveur d'abonnement CA afin de vérifier la présence de mises à jour de produits. Si les informations d'identification de proxy (telles que l'ID d'utilisateur et le mot de passe) sont arrivées à expiration ou ont été modifiées, CA Enterprise Log Manager ne peut plus contacter ce serveur d'abonnement et il génère un événement d'autosurveillance pour cet échec de connexion. L'événement d'autosurveillance affiche un message similaire à celui ci-dessous :

```
Impossible de se connecter au serveur de contenu d'abonnement. Soit le serveur est arrêté, soit la connexion est refusée, soit les paramètres du serveur proxy sont incorrects. Vérifiez les paramètres du serveur proxy.
```

Si les tentatives de connexion persistent, malgré leur échec répété, le compte de domaine peut être verrouillé, conformément aux stratégies locales. Vérifiez que les informations d'identification de proxy n'ont pas été modifiées et ne sont pas arrivées à expiration.

Nous recommandons d'éviter une stratégie d'expiration de mot de passe sur le compte de service utilisé pour contacter le serveur d'abonnement.

Apparition unique d'un événement d'autosurveillance de redémarrage

Symptôme :

Si vous sélectionnez un module de système d'exploitation à télécharger par abonnement et que vous spécifiez l'option sans redémarrage pour l'installer, l'événement d'autosurveillance suivant est généré une seule fois : Mises à jour de système d'exploitation installées sur cet hôte... Redémarrez l'ordinateur pour que ces mises à jour prennent effet.

Solution :

L'abonnement génère un événement qui vous rappelle de redémarrer le système d'exploitation une seule fois lorsqu'un redémarrage manuel est requis. Il convient de créer une alerte pour cet événement.

Nouvelle sélection obligatoire des modules d'abonnement après la mise à niveau

Symptôme :

Lors de la mise à niveau de CA Enterprise Log Manager vers la version r12.1, tous les modules d'abonnement sélectionnés précédemment sont déplacés de la liste Sélectionné(s) vers la liste Disponible(s). Ces modules ne sont donc pas pris en compte en cas de nouvelle mise à jour.

Solution :

A l'issue de la mise à niveau, sélectionnez de nouveau les modules à l'aide de la procédure suivante :

Pour sélectionner de nouveau les modules d'abonnement :

1. Connectez-vous à CA Enterprise Log Manager et cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Ouvrez le module d'abonnement pour chaque serveur que vous souhaitez actualiser.
3. A l'aide des contrôles de déplacement d'abonnement, déplacez les modules qui pourront être mis à jour de la liste Disponible(s) vers la liste Sélectionné(s).
4. Cliquez sur Enregistrer.

Le bouton Tester le proxy renvoie une fausse alerte après un changement de configuration.

Symptôme :

Quand vous modifiez les paramètres du serveur proxy CA Enterprise Log Manager après un test réussi, puis testez à nouveau à l'aide du bouton Tester le proxy, un message de confirmation s'affiche que la nouvelle configuration soit correcte ou non.

Solution :

Le bouton Tester le proxy utilise la configuration proxy spécifiée pour accéder à une URL via ce proxy. En général, les serveurs proxy mettent en mémoire cache l'authentification des clients quand ils sont valides et ignorent les informations de connexion suivantes tant que le délai d'inactivité n'a pas été dépassé.

Cela signifie que lorsque le bouton Tester le proxy indique avec raison que votre configuration est valide, les vérifications suivantes des configurations incorrectes risquent d'apparaître comme étant valides pendant une certaine période alors que cela n'est pas vrai.

Deux règles de suppression ne s'appliquent pas correctement

Symptôme :

Les deux règles de suppression suivantes, qui font partie de r12.0, ne s'appliquent pas correctement :

- TMCM - Messages de mises à jour du moteur antivirus et des signatures antivirus
- McAfee - Messages de mises à jour du moteur antivirus et des signatures antivirus

Solution :

Les règles ne s'appliquent pas correctement car le titre contient une esperluette. La mise à jour r12.1 contient les règles de remplacement suivantes :

- TMCM - Messages de mises à jour du moteur antivirus et des signatures antivirus
- McAfee - Messages de mises à jour du moteur antivirus et des signatures antivirus

Utilisez ces règles à la place de celles des anciennes versions qui contiennent une esperluette.

La mise à jour vers r12.1 nécessite le redémarrage de iGateway

Symptôme :

Dans un environnement fédéré, la mise à jour à partir de r12.0 vers r12.1 ne s'effectue pas sans le redémarrage de iGateway.

Solution :

Les fichiers binaires de la mise à jour sont copiés et extraits sans être installés par le client d'abonnement : ils demeurent tel quel dans le répertoire "/tmp/downloads". Ceci indique que le processus de mise à jour d'abonnement n'est pas terminé. A ce stade, vous devez redémarrer iGateway manuellement à l'aide du processus suivant :

Pour redémarrer le démon ou service iGateway

1. Connectez-vous en tant qu'utilisateur caelmadmin pour le serveur CA Enterprise Log Manager.
2. Basculez sur le compte d'utilisateur root au moyen de la commande ci-dessous.

   ```
   su -
   ```

3. Arrêtez le processus iGateway à l'aide de la commande suivante.

   ```
   $IGW_LOC/S99igateway stop
   ```

4. Démarrez le processus iGateway à l'aide de la commande ci-après.

   ```
   $IGW_LOC/S99igateway start
   ```

Ceci permettra à la mise à jour de s'effectuer.

La mise à niveau vers la version r12.1 SP1 peut requérir le redémarrage d'iGateway

Symptôme :

La mise à niveau de la version r12.1 à la version r12.1 SP1 n'a pas lieu dans les délais. Si le processus d'abonnement n'est pas fini passée une heure et demi ou plus, redémarrez iGateway.

Solution :

Nous recommandons l'utilisation de la procédure suivante pour l'identification de ce problème :

1. Abonnez-vous au contenu (rapports et intégrations) à partir de la version r12.1 GA.
2. Abonnez-vous aux binaires (serveur, agent, modules de SE) à partir de la version r12.1 SP1.

Cela vous permettra de connaître la durée de téléchargement de chaque module (elle peut varier selon la taille du module). Si l'exécution de la portion d'abonnement prend elle aussi trop de temps, redémarrez iGateway dans l'interface utilisateur de CA Enterprise Log Manager.

Pour redémarrer le service iGateway :

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Développez l'entrée Etat du système.
3. Sélectionnez un serveur CA Enterprise Log Manager spécifique.
4. Cliquez sur l'onglet Administration du service.
5. Cliquez sur Redémarrer iGateway.

Mise à jour à des intégrations pour le détecteur de journaux syslog requise dans la version r12.1 SP1 pour les agents pour Windows

Symptôme :

Si vous n'appliquez pas la mise à jour du module d'intégrations lorsque vous mettez à niveau vers la version r12.1 SP1, les connecteurs qui utilisent le détecteur de journaux syslog cesse de fonctionner. L'erreur suivante peut apparaître dans le fichier journal de l'agent :

```
[6072] 09/03/10 17:22:51 ERROR :: MySAX2Handler::fatalError: at line1
[6072] 09/03/10 17:22:51 ERROR :: XMLTree::ParseUsingSAX2:error parsing
stringintruvert/jsp/admin/Login.jsp
[6072] 09/03/10 17:22:51 ERROR :: XMLTree::Parse Exit ParseUsingSAX2 FAILURE
[6072] 09/03/10 17:22:51 ERROR :: HTTP_Processor::ParseRequestXML: Unknown
request format:intruvert/jsp/admin/Login.jsp
```

Vérifiez également la version de l'intégration. Si elle est antérieure à la version 12.1.5104.0, vous devez appliquer la mise à niveau.

Solution :

Appliquez la mise à jour du module d'intégrations, puis mettez à niveau toutes les intégrations qui utilisent le détecteur de journaux syslog vers la version 12.1.5104.0 ou vers une version ultérieure. Vous pouvez également effectuer les étapes de la section Mise à jour des configurations de plusieurs connecteurs dans le *Manuel d'administration*.

Pour obtenir une liste des intégrations qui utilisent le détecteur de journaux syslog, consultez la matrice d'intégrations de produit CA Enterprise Log Manager à l'adresse : https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.html.

Gestion des utilisateurs et des accès

Les problèmes connus relatifs à la gestion des utilisateurs et des accès sont répertoriés ci-dessous.

Restrictions d'accès à partir d'un navigateur sous Windows Vista

Symptôme :

Lorsque vous vous connectez à CA Enterprise Log Manager depuis un ordinateur équipé d'un système d'exploitation Windows Vista SP1, activé IPv6 depuis n'importe quel navigateur, vous ne pouvez pas utiliser les boutons de l'onglet Administration, sous-onglet Gestion des utilisateurs et des accès.

Toutefois, les utilisateurs qui utilisent les informations d'identification de l'utilisateur EiamAdmin ou celles d'un compte d'utilisateur CA Enterprise Log Manager auquel le rôle Administrator a été affecté peuvent accéder à cette fonctionnalité. Cette restriction ne concerne pas les utilisateurs qui accèdent à CA Enterprise Log Manager au moyen d'un navigateur s'exécutant sous un autre système d'exploitation Windows. Elle survient uniquement lors de l'accès à CA Enterprise Log Manager à partir d'un ordinateur Windows Vista au moyen d'une URL au format https://[*adresse-ipv6*]:5250/spin/calm. L'URL suivante constitue un exemple :

```
https://[::FFFF:192.168.00.00]:5250/spin/eiam
```

Solution :

Pour contourner ce problème, accédez à la fonctionnalité Gestion des utilisateurs et des accès à l'aide d'une autre URL.

1. Entrez l'URL ci-dessous à partir de votre navigateur, l'adresse IPv6 étant l'URL de votre serveur de gestion CA Enterprise Log Manager.

   `https://[adresse-ipv6]:5250/spin/eiam`

2. Sélectionnez CAELM dans la liste déroulante Application.
3. Entrez EiamAdmin et le mot de passe de ce compte ou entrez les informations d'identification d'un utilisateur CA Enterprise Log Manager doté du rôle Administrator pour les champs Nom d'utilisateur ou Mot de passe.
4. Cliquez sur l'onglet Manage Identities (Gérer les identités) pour configurer des utilisateurs et des groupes.
5. Cliquez sur l'onglet Manage Access Policies (Gérer les stratégies d'accès) pour configurer ou tester les calendriers.
6. Cliquez sur l'onglet Configurer, serveur EEM pour configurer des utilisateurs, des groupes globaux ou des stratégies de mot de passe.

Restriction sur l'utilisation d'un calendrier avec stratégies d'accès

Symptôme :

Vous avez limité à l'utilisateur ou au groupe l'accès à CA Enterprise Log Manager pendant les heures et les jours spécifiés sur un calendrier, avec une stratégie qui accorde explicitement l'accès. Cependant, ce calendrier ne fonctionne pas comme prévu avec une stratégie qui refuse explicitement l'accès.

Solution :

Pour limiter les heures d'accès d'un groupe, utilisez une stratégie qui accorde explicitement l'accès plutôt qu'une stratégie qui le refuse explicitement.

Divers

Les différents problèmes connus sont répertoriés ci-dessous.

Occasionnellement, CA Enterprise Log Manager ne répond pas

Symptôme :

Il arrive parfois que CA Enterprise Log Manager ne réponde plus. L'interface utilisateur ne répond pas aux demandes des utilisateurs et les demandes internes de l'agent au gestionnaire d'agent s'arrêtent. Toutefois, la collecte des journaux continue.

Solution :

Utilisez la procédure suivante pour arrêter le processus iGateway et le redémarrer :

1. Connectez-vous au serveur CA Enterprise Log Manager qui ne répond pas, au moyen de ssh et en tant qu'utilisateur caelmadmin.
2. Basculez sur le compte d'utilisateur root au moyen de la commande ci-dessous et entrez le mot de passe de l'utilisateur root.

   ```
   su -
   ```

3. Accédez au répertoire $IGW_LOC.

   Par défaut, iGateway se trouve dans le répertoire /opt/CA/SharedComponents/iTechnology.

4. Arrêtez le processus iGateway à l'aide de la commande ci-après.

   ```
   ./S99igateway stop
   ```

5. Démarrez le processus iGateway à l'aide de la commande ci-après.

   ```
   ./S99igateway start
   ```

Echec des appels de requête et de rapport d'API sur certains navigateurs

Symptôme :

Aucun résultat ne s'affiche si vous utilisez des appels getQueryViewer ou getReportViewer d'API ouverte avec Microsoft Internet Explorer 7 ou 8, ou avec Mozilla Firefox.

Solution :

Dans les navigateurs spécifiés, l'API CA Enterprise Log Manager ne parvient pas à reconnaître le paramètre "server" dans l'URL d'appel d'API. Pour éviter ce problème, ne spécifiez pas de paramètre de serveur dans les appels getQueryViewer et getReportViewer. Lorsque l'interface de CA Enterprise Log Manager s'affiche, sélectionnez un serveur dans la liste déroulante Serveur du gestionnaire de journaux, située dans la partie supérieure de la page principale.

Pour plus d'informations sur les URL d'appel d'API, consultez le *Manuel de programmation de l'API CA Enterprise Log Manager*.

Fin de la prise en charge de CAELM4Audit

CA Enterprise Log Manager r12.1 SP1 utilise CA EEM r8.4 SP3 qui n'est pas certifié pour l'utilisation avec CA Audit. L'intégration entre le calm> et CA Audit requiert le partage d'un serveur CA EEM, ce qui signifie que la configuration de l'exécution de CA Audit n'est pas prise en charge.

En outre, CA Audit n'est pas compatible avec la norme FIPS, c'est pourquoi le basculement de CA Enterprise Log Manager en mode FIPS entraîne l'arrêt de l'interface d'administration de CA Audit.

Impact du nom d'application personnalisé sur une requête d'archive

Symptôme :

Dans un environnement muni de plusieurs serveurs CA Enterprise Log Manager qui utilisent le même serveur de gestion, une requête d'archive renvoie en général des résultats provenant des répertoires de tous les serveurs. Cependant, si vous définissez un nom d'application personnalisé lors de l'installation du serveur de gestion CA Enterprise Log Manager au lieu d'accepter la valeur par défaut, CAELM, la requête d'archive ne fonctionnera pas comme prévu. Au lieu de cela, la requête d'archive renvoie des résultats uniquement pour le serveur sur lequel la requête est exécutée. Les résultats provenant d'autres serveurs s'affichent de la façon suivante : *<host>User CERT-custom: Access is denied*.

Solution :

Exécutez la requête sur le catalogue d'archive de chaque serveur CA Enterprise Log Manager séparément.

Paramètres de contraste élevé pour l'écran

Symptôme :

Sous Windows, le seul paramètre de contraste élevé pris en charge est Contraste noir élevé ; les trois autres options de contraste élevé ne sont pas prises en charge. Les options de contraste élevé comprennent Contraste élevé 1, Contraste élevé 2, Contraste noir élevé et Contraste blanc élevé.

Solution :

Lorsqu'un paramètre de contraste élevé est nécessaire, sélectionnez Contraste noir élevé. Pour définir cette option, sélectionnez Affichage dans le Panneau de configuration. Cette option d'accessibilité est définie dans la boîte de dialogue Propriétés d'affichage, onglet Apparence, liste déroulante Modèle de couleurs.

iGateway s'arrête et redémarre continuellement

Symptôme :

L'interface CA Enterprise Log Manager se bloque occasionnellement. La vérification du serveur CA Enterprise Log Manager révèle que le processus iGateway s'arrête et redémarre mais ne réussit pas à rester en état de fonctionnement. Pour vérifier le processus iGateway, procédez comme suit :

1. Accédez à une invite de commande sur le serveur CA Enterprise Log Manager.
2. Connectez-vous en utilisant les informations d'identification du compte caelmadmin.
3. Basculez sur le compte d'utilisateur root au moyen de la commande ci-dessous.

   ```
   su - root
   ```

4. Utilisez la commande suivante pour vérifier que le processus iGateway s'exécute.

   ```
   ps -ef | grep igateway
   ```

   Le système d'exploitation renvoie les informations sur le processus iGateway, ainsi qu'une liste des processus s'exécutant sous iGateway.

Solution :

Pour contourner le problème, procédez comme suit.

1. Accédez à $IGW_LOC (/opt/CA/SharedComponents/iTechnology) et recherchez le fichier ci-dessous.

   ```
   saf_epSIM.*
   ```

   Ce fichier comporte plusieurs versions numérotées séquentiellement, par exemple saf_epSIM.1, saf_epSIM.2, saf_epSIM.3, etc.

2. Renommez le fichier de numéro de version le moins élevé, puis enregistrez-le ailleurs afin de le transmettre au support de CA.
3. Si iGateway ne redémarre pas automatiquement, redémarrez-le manuellement comme suit.
   a. Connectez-vous en tant qu'utilisateur root.
   b. Accédez à une invite de commande, puis entrez la commande ci-après.

      ```
      /opt/CA/SharedComponents/iTechnology/S99igateway start
      ```

L'espace disque maximal pour CA Enterprise Log Manager virtuel est insuffisant

Symptôme :

Il est impossible de créer un ordinateur virtuel avec un espace disque alloué de 512 Go dans VMware ESX Server v3.5. Pour traiter le volume d'événements, mon serveur virtuel CA Enterprise Log Manager nécessite davantage que le maximum de 256 Go.

Solution :

VMWare ESX Server utilise une taille de bloc par défaut de 1 Mo et calcule l'espace disque maximal à partir de cette valeur. Lorsque la taille des blocs est définie sur 1 Mo, l'espace disque maximal prend la valeur par défaut de 256 Go. Si vous souhaitez configurer plus de 256 Go d'espace disque virtuel, vous pouvez augmenter la taille de bloc par défaut.

Pour créer un disque virtuel plus grand

1. Accédez à la console de service du serveur VMware ESX Server.
2. Augmentez la taille de bloc à 2 Mo au moyen de la commande ci-dessous.

   ```
   vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   Dans cette commande, la valeur 2M signifie 512 Go (2 x 256).
3. Redémarrez le serveur VMware ESX Server.
4. Créez un nouvel ordinateur virtuel dont l'espace disque est défini sur 512 Go.

Pour plus d'informations sur cette commande et sur d'autres commandes, consultez la documentation VMware ESX Server.

L'actualisation d'un navigateur déconnecte un utilisateur de CA Enterprise Log Manager

Symptôme :

Si vous actualisez votre navigateur alors que vous êtes connecté à CA Enterprise Log Manager, votre session prend fin et vous êtes déconnecté.

Solution :

CA Enterprise Log Manager ne prend pas en charge l'actualisation des navigateurs en raison de restrictions Flex. Evitez d'actualiser votre navigateur.

Erreur possible au niveau du service ou de l'interface de l'explorateur après le redémarrage d'iGateway

Symptôme :

Si vous cliquez sur un objet dans les services de l'interface CA Enterprise Log Manager ou dans les arborescences d'explorateur immédiatement après le redémarrage d'iGateway, le message d'erreur "Network error on receive" (erreur réseau lors de la réception) risque de s'afficher à la place du contenu demandé.

Solution :

Cette erreur se produit si vous essayez d'accéder à l'un des objets spécifiés pendant son rechargement après le redémarrage d'iGateway. Patientez pendant cinq minutes pour permettre le rechargement et cliquez sur les services ou sur l'élément d'explorateur de votre choix.

Echec des chargements et des exportations avec des navigateurs autres qu'Internet Explorer

Symptôme :

Si vous utilisez Mozilla Firefox, Safari ou Chrome pour accéder à CA Enterprise Log Manager, vous pourrez effectuer pratiquement toutes les tâches CA Enterprise Log Manager, sauf les tâches d'importation et de chargement. Vous trouverez plusieurs exemples ci-dessous.

- Echec de l'importation d'une définition de requête et envoi du message "Erreur d'E/S : Echec de la demande".
- Echec du chargement des fichiers CSV avec l'assistant de déploiement du connecteur en bloc, malgré l'affichage du message suivant : Veuillez patienter pendant le chargement du fichier.

Solution :

Utilisez Microsoft Internet Explorer pour accéder à CA Enterprise Log Manager afin d'importer ou de charger des fichiers.

L'affichage de l'interface utilisateur échoue de manière inattendue lors d'une installation avec un EEM distant

Symptôme :

Lors de l'installation de CA Enterprise Log Manager avec un serveur EEM distant, l'affichage de l'interface utilisateur échoue occasionnellement lors de la connexion initiale. La vérification des fichiers journaux iGateway indique que les services agentmanager, calmreporter, subscclient et subscproxy n'ont pas été démarrés.

La syntaxe du fichier journal peut s'apparenter à celle-ci :

```
[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-msgbroker ] didn't respond OK for the termination
call

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-oaserver ] didn't reaspond OK for the termination
call

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-sapicollector ] didn't reaspond OK for the
termination call

[1087527824] 23/09/09 17:07:46 ERROR :: OutProcessSponsorManager::start :
SponsorGroup [ caelm-java ] failed to start ]

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
agentmanager ] failed to load

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
calmreporter ] failed to load

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscclient ] failed to load

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscproxy ] failed to load
```

Solution :

Vous pouvez résoudre ce problème en redémarrant iGateway, puis en vous reconnectant à l'interface.

Pour redémarrer le service iGateway

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Développez l'entrée Etat du système.
3. Sélectionnez un serveur CA Enterprise Log Manager spécifique.
4. Cliquez sur l'onglet Administration du service.
5. Cliquez sur Redémarrer iGateway.

Chapitre 7 : Problèmes résolus

Ce chapitre traite des sujets suivants :

Problèmes fixés dans la version r12.1 SP1 (page 81)

Problèmes fixés dans la version r12.1 SP1

Les problèmes suivants, signalés par des clients, ont été résolus dans CA Enterprise Log Manager r12.1 SP1.

- 18789166-1
- 18790979-1
- 18955095-1
- 18973282-1
- 18982868-1
- 18988854-1
- 19005999-1
- 19066155-1
- 19077668-1
- 19087827-1
- 19127553-1
- 19176852-1
- 19182913-1
- 19188433-2

Chapitre 8 : Documentation

Ce chapitre traite des sujets suivants :

Bibliothèque (page 83)
Accès à la bibliothèque (page 84)

Bibliothèque

La bibliothèque offre un accès à toute la documentation CA Enterprise Log Manager à partir d'un emplacement central. La bibliothèque offre les opportunités suivantes.

- Liste extensible des contenus de tous les manuels au format HTML
- Recherche de texte intégral dans l'ensemble des manuels, avec classement des résultats de recherche et termes recherchés mis en surbrillance dans le contenu

  Remarque : Si vous recherchez du texte purement numérique, placez un astérisque avant la valeur de recherche.
- Des chemins de navigation reliés aux rubriques du niveau supérieur
- Index unique pour tous les manuels
- Des liens vers les versions PDF des manuels pour impression

Accès à la bibliothèque

Les bibliothèques de documentation de produit CA sont disponibles pour téléchargement dans des fichiers ZIP incluant un index de recherche.

Pour accéder à la bibliothèque CA Enterprise Log Manager :

1. Allez à Rechercher dans la documentation/les manuels.
2. Entrez CA Enterprise Log Manager comme produit, sélectionnez une version et une langue, puis cliquez sur OK.
3. Téléchargez le fichier ZIP sur votre ordinateur ou à un autre emplacement.
4. Ouvrez le fichier ZIP et faites glisser le dossier de bibliothèque vers votre ordinateur ou extrayez-le à un autre emplacement.
5. Ouvrez le dossier de bibliothèque.
6. Ouvrez la bibliothèque :
   - Si la bibliothèque est située sur le système local et que vous utilisez Internet Explorer, ouvrez le fichier Bookshelf.hta.
   - Si la bibliothèque est située sur un système distant ou que vous utilisez Mozilla Firefox, ouvrez le fichier Bookshelf.html.

   La bibliothèque s'ouvre.

Annexe A : Communiqués de tiers

Ce chapitre traite des sujets suivants :

Adaptive Communication Environment (ACE) (page 86)
Logiciel régi par la licence Apache (page 88)
boost 1.35.0 (page 92)
JDOM 1.0 (page 93)
PCRE 6.3 (page 95)
Zlib 1.2.3 (page 97)
ZThread 2.3.2 (page 97)

Adaptive Communication Environment (ACE)

Copyright and Licensing Information for ACE(TM), TAO(TM), and CIAO(TM).

ACE(TM), TAO(TM) and CIAO(TM) are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University Copyright (c) 1993-2003, all rights reserved. Since ACE TAO CIAO are open-source, free software, you are free to use, modify, copy, and distribute--perpetually and irrevocably--the ACE TAO CIAO source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using ACE TAO CIAO.

You can use ACE TAO CIAO in proprietary software and are under no obligation to redistribute any of your source code that is built using ACE TAO CIAO. Note, however, that you may not do anything to the ACE TAO CIAO code, such as copyrighting it yourself or claiming authorship of the ACE TAO CIAO code, that will prevent ACE TAO CIAO from being distributed freely using an open-source development model. You needn't inform anyone that you're using ACE TAO CIAO in your software, though we encourage you to let us know so we can promote your project in the ACE TAO CIAO success stories.

ACE TAO CIAO are provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, ACE TAO CIAO are provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies provide commercial support for ACE and TAO, however. ACE, TAO and CIAO are Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by ACE TAO CIAO or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE, TAO and CIAO web sites are maintained by the Center for Distributed Object Computing of Washington University for the development of open-source software as part of the open-source software community. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the ACE, TAO and CIAO software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source ACE TAO CIAO projects or their designees.

The names ACE(TM), TAO(TM), CIAO(TM), Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE(TM), TAO(TM), or CIAO(TM) nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Logiciel régi par la licence Apache

Ce produit utilise les logiciels Apache suivants :

- Ant 1.6.5
- Formatting Objects Processor (FOP) 0.95
- Jakarta POI 3.0
- Log4cplus 1.0.2
- Log4j 1.2.15
- Quartz 1.5.1
- Xerces-C 2.6.0

Certaines parties de ce produit comprennent des logiciels développés par Apache Software Foundation. Les logiciels Apache sont distribués conformément au contrat de licence suivant.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

'License' shall mean the terms and conditions for use, reproduction,and distribution as defined by Sections 1 through 9 of this document.

'Licensor' shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

'Legal Entity' shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, 'control' means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

'You' (or 'Your') shall mean an individual or Legal Entity exercising permissions granted by this License.

'Source' form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

'Object' form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and versions to other media types.

'Work' shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work(an example is provided in the Appendix below).

'Derivative Works' shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

'Contribution' shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, 'submitted' means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as 'Not a Contribution.'

'Contributor' shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a 'NOTICE' text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an 'AS IS' BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

boost 1.35.0

Ce produit comporte du logiciel distribué conformément au contrat de licence suivant.

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

JDOM 1.0

Ce produit comprend du logiciel développé par JDOM Project (http://www.jdom.org/). Le logiciel JDOM est distribué conformément au contrat de licence suivant.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact.

4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management.

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter and Brett McLaughlin. For more information on the JDOM Project, please see http://www.jdom.org.

PCRE 6.3

Certaines parties de ce produit comprennent des logiciels développés par Philip Hazel. Le logiciel du service informatique de l'université de Cambridge est distribué conformément au contrat de licence suivant.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Fin

Zlib 1.2.3

Ce produit inclut le logiciel zlib développé par Jean-loup Gailly et Mark Adler.

ZThread 2.3.2

Certaines parties de ce produit comprennent des logiciels développés par Eric Crahen. Le logiciel ZThread est distribué conformément au contrat de licence suivant.