

CA Enterprise Log Manager

Manuel d'implémentation

Version 12.5



La présente documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si (i) un autre accord régissant l'utilisation du logiciel CA mentionné dans la Documentation passé entre vous et CA stipule le contraire ; ou (ii) si un autre accord de confidentialité entre vous et CA stipule le contraire.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2010 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Produits CA référencés

Ce document fait référence aux produits CA suivants :

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

Support technique

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

Modifications de la documentation

Les mises à jour suivantes ont été réalisées depuis la dernière version de la présente documentation.

- Corrélation d'événements : changements apportés aux chapitres Planification des serveurs et Configuration des services pour fournir des informations sur cette nouvelle fonctionnalité. Les changements incluent des informations sur les serveurs de corrélation dédiés et sur la planification des rôles de serveur, ainsi que sur la configuration des serveurs et des règles de corrélation.
- Améliorations apportées à la remise et à la surveillance d'abonnement : changements apportés au chapitre Configuration des services pour fournir des informations sur les changements appliqués à la configuration d'abonnement
- Virtualisation : changements apportés au chapitre Virtualisation pour fournir des informations sur le changement appliqué aux paramètres requis pour le déploiement d'un modèle OVF

Informations complémentaires :

[Planification des serveurs](#) (page 20)

[Configuration du service de corrélation](#) (page 184)

Table des matières

Chapitre 1 : Introduction	15
A propos de ce manuel	16
Chapitre 2 : Planification de votre environnement	19
Planification des serveurs	20
Rôles des serveurs	21
Exemple : Architectures réseau	26
Planification de la collecte de journaux	29
Planification d'espace disque	31
A propos du serveur CA EEM	32
Consignes de collecte de journaux	33
Planification de fédération	34
Création d'une carte de fédération	35
Exemple : Carte de fédération pour une grande entreprise	37
Exemple : Carte de fédération pour une PME	39
Planification des utilisateurs et des accès	42
Planification du magasin d'utilisateurs	42
Utilisateurs ayant le rôle Administrator	47
Planification de la stratégie de mots de passe	47
Planification des mises à jour d'abonnement	50
Service d'abonnement	51
Fonctionnement de l'abonnement	52
Planification des mises à jour d'abonnement	54
Exemple : Configuration d'abonnement avec six serveurs	61
Planification d'agent	63
A propos de la collecte d'événements Syslog	63
Les agents et le certificat d'agent	65
A propos des agents	66
A propos des intégrations	67
A propos des connecteurs	68
Dimensionnement de votre réseau CA Enterprise Log Manager	70

Chapitre 3 : Installation de CA Enterprise Log Manager 73

Présentation de l'environnement CA Enterprise Log Manager	73
Création des DVD d'installation	75
Installation d'un serveur CA Enterprise Log Manager	76
Feuille de calcul du serveur CA Enterprise Log Manager	77
Installation de CA Enterprise Log Manager	83
Vérifier que le processus iGateway s'exécute	84
Vérification de l'installation du serveur CA Enterprise Log Manager	87
Affichage des événements d'autosurveillance	88
Mise à niveau des serveurs et des agents CA Enterprise Log Manager existants pour la prise en charge de la norme FIPS	89
Conditions préalables à la mise à niveau pour la prise en charge de la norme FIPS	92
Instructions concernant la mise à niveau	93
Mise à niveau d'un serveur CA EEM distant	94
Désactivation de l'accès d'ODBC et de JDBC au magasin de journaux d'événements	94
Activation des opérations en mode FIPS	94
Affichage du tableau de bord des agents	96
Ajout de serveurs CA Enterprise Log Manager à une fédération en mode FIPS existante	98
Remarques concernant l'installation d'un système disposant de lecteurs SAN	100
Installation avec des lecteurs SAN désactivés	101
Installation avec des lecteurs SAN activés	107
Configurations initiales du serveur CA Enterprise Log Manager	108
Comptes d'utilisateur par défaut	109
Structure des répertoires par défaut	110
Image du système d'exploitation personnalisé	110
Affectations de ports par défaut	111
Liste des processus liés	113
Durcissement de système d'exploitation	116
Redirection des ports du pare-feu pour les événements Syslog	116
Installation du client ODBC	117
Configuration requise	117
Configuration du service Serveur ODBC	118
Installation du client ODBC sur les systèmes Windows	119
Création d'une source de données ODBC sur les systèmes Windows	120
Test de la connexion du client ODBC à la base de données	122
Test de la récupération du serveur à partir de la base de données	123
Installation du client JDBC	123
Configuration requise pour le client JDBC	124

Installation du client JDBC sur les systèmes Windows	125
Installation du client JDBC sur les systèmes UNIX	125
Paramètres de connexion JDBC	126
Considérations sur les URL JDBC	126
Dépannage de l'installation	127
Résoudre une erreur de configuration de l'interface réseau	129
Vérifier que le package RPM est installé	130
Enregistrement du serveur CA Enterprise Log Manager auprès du serveur CA EEM	130
Acquisition de certificats auprès du serveur CA EEM	131
Importation de rapports CA Enterprise Log Manager	132
Importation de fichiers de mappage de données CA Enterprise Log Manager	133
Importation de fichiers de grammaire commune aux événements	133
Importation de fichiers de règles de corrélation	134
Importation de fichiers de gestion commune des agents	135
Importation de fichiers de configuration CA Enterprise Log Manager	136
Importation des fichiers de suppression et de récapitulation	136
Importation des fichiers de jetons d'analyse	137
Importation des fichiers de l'interface utilisateur CA Enterprise Log Manager	138

Chapitre 4 : Configuration des utilisateurs de base et des accès **139**

A propos des utilisateurs de base et des accès	139
Configuration du magasin d'utilisateurs	140
Acceptation du magasin d'utilisateurs par défaut	140
Référence à un répertoire LDAP	141
Référence à CA SiteMinder comme magasin d'utilisateurs	142
Configuration des stratégies de mots de passe	144
Conservation des stratégies d'accès prédéfinies	145
Création du premier administrateur	146
Création d'un nouveau compte d'utilisateur	147
Affectation d'un rôle à un utilisateur global	148

Chapitre 5 : Configuration des services **151**

Sources d'événement et configurations	151
Modification de configurations globales	152
Utilisation des Paramètres et filtres globaux	155
Sélection de l'utilisation des requêtes fédérées	156
Configuration de l'intervalle global de mise à jour	156
Configuration du magasin de journaux d'événements	157

A propos du service du magasin de journaux d'événements	158
A propos des fichiers d'archive	158
A propos de l'archivage automatique	159
Organigramme de stratégie de sauvegarde et de déplacement de base de données	161
Configuration de l'authentification non interactive pour l'archivage automatique	162
Exemple : Configuration de l'authentification non interactive pour la topologie en étoile	164
Exemple : Configuration de l'authentification non interactive au niveau de trois serveurs	173
Exemple : Archivage automatique sur trois serveurs	175
Paramètres du magasin de journaux d'événements dans l'environnement de base	181
Définition des options des magasins de journaux d'événements	183
Configuration du service de corrélation	184
Application de règles de corrélation et de notifications d'incidents	185
Utilisation de règles de corrélation prédéfinies	186
Définition des serveurs de collecte	190
Conception et application des notifications d'incidents	190
Création d'une destination de notification	191
Remarques sur le service d'incidents	195
Remarques sur le serveur ODBC	196
Remarques sur le serveur de rapports	197
Configuration de l'abonnement	198
Configuration d'un proxy d'abonnement en ligne	199
Configuration d'un proxy d'abonnement hors ligne	200
Configuration d'un client d'abonnement	201
Configuration des listes de proxys	202
Modules à télécharger	203
Définition d'une planification d'abonnement	209

Chapitre 6 : Configuration de la collecte d'événements **211**

Installation d'agents	211
Utilisation de l'Explorateur d'agent	212
Configuration de l'agent par défaut	213
Examen des intégrations et écouteurs Syslog	214
Création d'un connecteur Syslog pour l'agent par défaut	214
Vérification de la réception des événements Syslog par le serveur CA Enterprise Log Manager	215
Exemple : Activation de la collecte directe à l'aide du détecteur ODBCLogSensor	216
Exemple : Activation de la collecte directe à l'aide du détecteur WinRMLinuxLogSensor	223
Affichage et contrôle de l'état d'un agent ou d'un connecteur	229

Chapitre 7 : Création de fédérations	231
Requêtes et rapports dans un environnement fédéré	231
Fédérations hiérarchiques	232
Exemple de fédération hiérarchique	233
Fédérations maillées	234
Exemple de fédération maillée	235
Configuration d'une fédération CA Enterprise Log Manager	235
Configuration d'un serveur CA Enterprise Log Manager en tant que serveur enfant	236
Affichage du graphique de fédération et du contrôleur de l'état du serveur	237
Chapitre 8 : Utilisation de la bibliothèque d'ajustement d'événement	239
A propos de la bibliothèque d'ajustement d'événement	239
Prise en charge de nouvelles sources d'événement avec la bibliothèque d'ajustement d'événement	240
Fichiers de mappage et d'analyse	240
Annexe A : Remarques pour les utilisateurs de CA Audit	243
Présentation des différences entre les architectures	243
Architecture CA Audit	245
Architecture CA Enterprise Log Manager	247
Architecture intégrée	250
Configuration d'adaptateurs CA	251
A propos du routeur et du collecteur SAPI	252
A propos du module d'extension d'événements iTechnology	255
Envoi d'événements CA Audit à CA Enterprise Log Manager	256
Configuration d'iRecorder pour envoyer des événements à CA Enterprise Log Manager	256
Modification d'une stratégie CA Audit existante pour envoyer des événements à CA Enterprise Log Manager	258
Modification d'une stratégie r8 SP2 pour envoyer des événements à CA Enterprise Log Manager	260
Quand importer des événements	261
A propos de l'utilitaire d'importation SEOSDATA	262
Importation à partir d'une table SEOSDATA en temps réel	262
Importation des données d'une table SEOSDATA	263
Copie de l'utilitaire d'importation d'événements sur un serveur d'outils de données Solaris	264
Copie de l'utilitaire d'importation sur un serveur d'outils de données Windows	265
Présentation de la ligne de commande LMSeosImport	265
Création d'un rapport d'événements	269

Prévisualisation des résultats de l'importation	270
Importation d'événements provenant d'une base de données de collecteur Windows.....	271
Importation d'événements provenant d'une base de données de collecteur Solaris	271

Annexe B : Remarques pour les utilisateurs de CA Access Control **273**

Intégration avec CA Access Control	273
Modification des stratégies CA Audit pour envoyer des événements à CA Enterprise Log Manager	275
Configuration de l'adaptateur du collecteur SAPI pour recevoir des événements CA Access Control	276
Modification d'une stratégie CA Audit existante pour envoyer des événements à CA Enterprise Log Manager	278
Vérification et activation de la stratégie modifiée	282
Configuration d'un iRecorder CA Access Control pour envoyer des événements à CA Enterprise Log Manager	283
Configuration du module d'extension d'événements iTech pour des événements CA Access Control	284
Téléchargement et installation d'un iRecorder CA Access Control	285
Configuration d'un iRecorder CA Access Control autonome	285
Importation d'événements CA Access Control provenant d'une base de données de collecteur CA Audit	287
Tâches requises avant l'importation d'événements CA Access Control	288
Création d'un rapport d'événements SEOSDATA sur des événements CA Access Control	290
Prévisualisation de l'importation d'événements CA Access Control	292
Importation d'événements CA Access Control	295
Affichage de requêtes et de rapports sur des événements CA Access Control	296

Annexe C : Remarques sur CA IT PAM **299**

Scénario : Utilisation de CA EEM sur CA Enterprise Log Manager pour l'authentification CA IT PAM	300
Processus d'implémentation de l'authentification CA IT PAM	300
Préparation de l'implémentation de l'authentification CA IT sur un CA EEM partagé	302
Copiez un fichier XML dans le serveur de gestion CA Enterprise Log Manager	303
Enregistrez CA IT PAM avec un CA EEM partagé	303
Copie du certificat dans le serveur CA IT PAM	305
Définition des mots de passe pour les comptes d'utilisateur CA IT PAM prédéfinis	305
Installation de composants tiers requis par CA IT PAM	307
Installation du domaine CA IT PAM	308
Démarrez le service du serveur CA ITPAM.	309

Lancez la console du serveur CA IT PAM et connectez-vous.	310
--	-----

Annexe D : Récupération après sinistre **311**

Planification de la récupération après sinistre	311
A propos de la sauvegarde du serveur CA EEM	312
Sauvegarde d'une instance d'application CA EEM	313
Restauration d'un serveur CA EEM pour l'utiliser avec CA Enterprise Log Manager	314
Sauvegarde d'un serveur CA Enterprise Log Manager	315
Restauration d'un serveur CA Enterprise Log Manager à partir des fichiers de sauvegarde	315
Restauration d'un serveur CA Enterprise Log Manager suite à une mise à jour d'abonnement.	317
Remplacement d'un serveur CA Enterprise Log Manager	317

Annexe E : CA Enterprise Log Manager et virtualisation **319**

Hypothèses de déploiement	319
Remarques	319
Création de serveurs CA Enterprise Log Manager à l'aide d'ordinateurs virtuels.....	320
Ajout de serveurs virtuels à votre environnement	321
Création d'un environnement complètement virtuel	325
Déploiement rapide de serveurs CA Enterprise Log Manager virtuels	329
Création de serveurs CA Enterprise Log Manager à l'aide d'ordinateurs virtuels.....	336
Dispositifs virtuels CA Enterprise Log Manager	337
Fonctionnement du dispositif virtuel	338
Feuille de calcul d'installation de dispositifs virtuels	338
Ajout de serveurs virtuels à votre environnement	341
Création d'un environnement complètement virtuel	365
Déploiement rapide de serveurs virtuels	391
Tâches de post-installation.....	401

Chapitre 9 : Glossaire **403**

Index **437**

Chapitre 1 : Introduction

Ce chapitre traite des sujets suivants :

[A propos de ce manuel](#) (page 16)

A propos de ce manuel

Manuel d'implémentation CA Enterprise Log Manager vous donne les instructions nécessaires pour planifier, installer et configurer CA Enterprise Log Manager afin qu'il reçoive des journaux d'événements provenant des sources d'événement de votre réseau. Le manuel est organisé de telle sorte que les tâches débutent avec une description du processus et de ses objectifs. Les processus sont généralement suivis par les concepts correspondants, puis par une ou plusieurs procédures permettant d'atteindre l'objectif.

Manuel d'implémentation CA Enterprise Log Manager est conçu pour les administrateurs système responsables de l'installation, de la configuration et de la maintenance d'une solution de collecte de journaux, de la création d'utilisateurs et de l'affectation ou de la définition de leurs rôles et accès, ainsi que de la conservation des données de sauvegarde.

Ce manuel soutient également le personnel ayant besoin d'informations sur la réalisation des tâches ci-dessous.

- Configuration d'un connecteur ou d'un adaptateur pour collecter les données d'événements
- Configuration de services pour contrôler la génération de rapports ainsi que la conservation, la sauvegarde et l'archivage des données
- Configuration d'une fédération de serveurs CA Enterprise Log Manager
- Configuration de l'abonnement pour obtenir les mises à jour du contenu, de la configuration et du système d'exploitation

Vous trouverez ci-dessous un récapitulatif du contenu.

Section	Description
Planification de votre environnement	Décrit les activités de planification pour les domaines comme la collecte de journaux, les agents, la fédération, la gestion des utilisateurs et des accès, les mises à jour de l'abonnement et la récupération après sinistre.
Installation de CA Enterprise Log Manager	Fournit des feuilles de calcul pour collecter les informations requises, ainsi que des instructions détaillées pour installer CA Enterprise Log Manager et vérifier l'installation.
Configuration des utilisateurs de base et des accès	Fournit des instructions pour identifier un magasin d'utilisateurs et créer l'utilisateur administratif initial, afin de configurer d'autres informations sur les utilisateurs et les accès.

Section	Description
Configuration des services	Fournit des instructions pour configurer des services, notamment les filtres globaux et locaux, le magasin de journaux d'événements, le serveur de rapports et les options d'abonnement.
Configuration de la collecte d'événements	Fournit des concepts et des instructions pour utiliser ou configurer les composants de la bibliothèque d'ajustement d'événement, y compris les fichiers de mappage et d'analyse, ainsi que les adaptateurs CA.
Création de fédérations	Décrit différents types de fédérations et fournit des instructions pour créer des relations fédérées entre les serveurs CA Enterprise Log Manager et afficher un graphique de fédération.
Utilisation de la bibliothèque d'ajustement d'événement	Apporte des informations intéressantes sur l'utilisation des fichiers d'analyse de message et des fichiers de mappage de données.
Remarques pour les utilisateurs de CA Audit	Décrit les interactions que vous pouvez implémenter entre CA Enterprise Log Manager et CA Audit, comment configurer les iRecorders et les stratégies, et comment importer des données depuis votre base de données de collecteur CA Audit.
Remarques pour les utilisateurs de CA Access Control	Décrit l'intégration auprès de CA Access Control, la modification des stratégies CA Audit pour envoyer des événements à CA Enterprise Log Manager, la configuration d'un iRecorder CA Access Control pour envoyer des événements à CA Enterprise Log Manager, et l'importation d'événements CA Access Control à partir d'une base de données de collecteur CA Audit.
Remarques sur CA IT PAM	Décrit le processus d'installation de CA IT PAM de sorte que le composant EEM situé sur le serveur de gestion CA Enterprise Log Manager handles authentication.
Récupération après sinistre	Décrit les procédures de sauvegarde, de restauration et de remplacement visant à garantir la récupération de votre solution de gestion des journaux en cas de sinistre.
CA Enterprise Log Manager et virtualisation	Décrit le processus à suivre pour créer et configurer un ordinateur virtuel contenant un serveur CA Enterprise Log Manager.

Remarque : Pour plus de détails sur la prise en charge des systèmes d'exploitation ou la configuration système requise, consultez les *Notes de parution*. Pour une présentation de base de CA Enterprise Log Manager et un scénario classique d'utilisation, consultez le *Manuel de présentation*. Pour plus de détails sur l'utilisation et la maintenance du produit, consultez le *Manuel d'administration*. Pour obtenir de l'aide quant à l'utilisation d'une page CA Enterprise Log Manager consultez l'aide en ligne.

Chapitre 2 : Planification de votre environnement

Ce chapitre traite des sujets suivants :

[Planification des serveurs](#) (page 20)

[Planification de la collecte de journaux](#) (page 29)

[Planification de fédération](#) (page 34)

[Planification des utilisateurs et des accès](#) (page 42)

[Planification des mises à jour d'abonnement](#) (page 50)

[Planification d'agent](#) (page 63)

Planification des serveurs

La première étape de la planification de votre environnement consiste à déterminer le nombre de serveurs CA Enterprise Log Manager nécessaires et le rôle assumé par chaque serveur. Les rôles sont répertoriés ci-dessous.

- **Gestion**
Le serveur stocke des configurations et des contenus prédéfinis et définis par l'utilisateur. Il authentifie également les utilisateurs et autorise l'accès aux fonctions.
- **Collecte**
Le serveur reçoit les journaux d'événements de ses agents et ajuste les événements.
- **Corrélation**
Le serveur reçoit les journaux d'événements des agents ou des serveurs de collecte. Il filtre les événements et crée des incidents en fonction des règles de corrélation appliquées.
- **Génération de rapports**
Le serveur traite les requêtes sur les événements collectés, les requêtes et rapports à la demande, ainsi que les alertes et rapports planifiés.
- **Point de restauration**
Le serveur reçoit les bases de données restaurées de journaux d'événements à des fins d'examen d'événements passés.

Le premier serveur installé est le serveur de gestion ; ce serveur peut également assumer d'autres rôles. Vous pouvez disposer d'un seul serveur de gestion sur un réseau CA Enterprise Log Manager unique. Chaque réseau CA Enterprise Log Manager doit disposer d'un serveur de gestion.

Les architectures possibles sont répertoriées ci-dessous.

- Système à un seul serveur, dans lequel le serveur de gestion assume tous les autres rôles
- Système à deux serveurs, dans lequel le serveur de gestion assume tous les rôles, sauf la collecte. Celle-ci est effectuée par un serveur dédié à ce rôle.
- Système comptant plusieurs serveurs, dans lequel chaque serveur est dédié à un seul rôle

Vous trouverez ci-après des détails sur les rôles des serveurs et les architectures.

Rôles des serveurs

Un système CA Enterprise Log Manager peut posséder un ou plusieurs serveurs. En dédiant différents serveurs à différents rôles, vous optimisez les performances. Mais vous pouvez choisir d'utiliser un serveur pour effectuer plusieurs rôles ou tous les rôles. Tenez compte du poids du traitement lié à chaque rôle de serveur par rapport aux autres facteurs importants dans votre environnement lorsque vous déterminez comment dédier chaque serveur installé.

■ Serveur de gestion

Par défaut, le rôle du serveur de gestion est tenu par le premier serveur CA Enterprise Log Manager installé. Le serveur de gestion réalise les fonctions principales ci-dessous.

- Il agit comme un référentiel commun pour tous les serveurs qui s'enregistrent auprès de lui. Plus précisément, il stocke les utilisateurs d'applications, les groupes d'applications (rôles), les stratégies, les calendriers et les objets d'application.
- Si vous configurez le magasin d'utilisateurs comme un magasin interne, le serveur stocke les utilisateurs globaux, les groupes globaux et les stratégies de mots de passe. Si le magasin d'utilisateurs configuré fait référence à un magasin d'utilisateurs externe, le serveur charge les détails des comptes d'utilisateurs globaux et les détails des groupes globaux provenant du magasin d'utilisateurs référencé.
- Il gère les droits des utilisateurs avec un fichier mappé vers la mémoire haut débit. Il authentifie les utilisateurs lors de la connexion, en fonction de la configuration des utilisateurs et des groupes. Il autorise les utilisateurs à accéder à diverses parties de l'interface utilisateur, en fonction des stratégies et des calendriers.
- Il reçoit toutes les mises à jour de contenu et de configuration téléchargées via l'abonnement.

Vous pouvez avoir un seul serveur de gestion actif sur un réseau de serveurs CA Enterprise Log Manager, mais vous pouvez avoir également un serveur de gestion de basculement (inactif). Si vous créez plusieurs réseaux CA Enterprise Log Manager, chacun doit disposer de son propre serveur de gestion actif.

■ Serveur de collecte

Dans un système à un seul serveur, le serveur de gestion assume le rôle de serveur de collecte. Dans un système à plusieurs serveurs, envisagez de disposer d'un serveur de collecte dédié. Un serveur de collecte réalise les fonctions ci-dessous.

- Il prend en charge la configuration des connecteurs.
- Il accepte les journaux d'événements entrants provenant des connecteurs de ses agents.
- Il accepte les journaux d'événements ajustés entrants, qui sont analysés et mappés au format CEG, ce qui permet de disposer d'une présentation uniforme des données provenant de différentes sources d'événements.
- Il insère les journaux d'événements dans la base de données chaude et, lorsque celle-ci atteint la taille configurée, il la transforme en base de données tiède.
- Il permet l'archivage automatique, fonction qui déplace les informations des bases de données tièdes vers le serveur de génération de rapports associé dans la planification configurée.

Important : Lorsque des serveurs sont dédiés séparément à la collecte et à la génération de rapports, configurez l'authentification non interactive et l'archivage automatique par heure du serveur de collecte au serveur de génération de rapports.

Tenez compte du volume d'événements généré par vos sources d'événement lorsque vous choisissez de dédier ou non des serveurs à la collecte et à l'ajustement d'événements. Tenez également compte du nombre de serveurs de collecte qui doivent archiver automatiquement leurs données sur un seul serveur de génération de rapports.

- Serveur de corrélation

Dans un système à serveur unique, le serveur de gestion assume le rôle de serveur de corrélation. Dans un système à plusieurs serveurs, il est recommandé d'utiliser serveur de corrélation dédié. Un serveur de corrélation réalise les fonctions décrites ci-dessous.

- Prend en charge la configuration et l'application des règles de corrélation et des notifications.
- Accepte les journaux d'événements entrants issus des serveurs de collecte.
- Filtre les événements entrants et crée des incidents en fonction des conditions des règles de corrélation.
- Stocke les incidents dans la base de données des incidents et les événements de leurs composants dans la base de données des événements d'incident.

Important : Lorsque vous dédiez différents serveurs à la corrélation, sélectionnez chaque serveur de collecte dont vous voulez corréler les événements lors de la configuration du service de corrélation.

- Serveur de génération de rapports

Dans un système à un ou deux serveurs, le serveur de gestion assume le rôle de serveur de génération de rapports. Dans un système comptant de nombreux serveurs, envisagez de dédier un ou plusieurs serveurs à la génération de rapports. Un serveur de génération de rapports réalise les fonctions ci-dessous.

- Si l'authentification non interactive et l'archivage automatique sont configurés, il reçoit de nouvelles bases de données d'événements ajustés provenant de ses serveurs de collecte.
- Il traite les invites, requêtes et rapports à la demande.
- Il traite les alertes et rapports planifiés.
- Il prend en charge les assistants de création de requêtes et rapports personnalisés.
- Si l'authentification non interactive et l'archivage automatique sont configurés pour permettre des transactions du serveur de génération de rapports au serveur de stockage distant, les anciennes bases de données sont déplacées sur un serveur de stockage distant.

Si vous prévoyez de générer de nombreux rapports et alertes complexes sur un serveur ayant un volume important d'activité à la demande, il est recommandé de dédier un serveur à la génération de rapports.

- Serveur de stockage distant

Il s'agit d'un serveur de stockage distant, non CA Enterprise Log Manager, qui exécute les fonctions décrites ci-dessous.

- Il reçoit les bases de données archivées automatiquement et fortement compressées provenant des serveurs de rapports, selon des intervalles configurés, avant de supprimer ces bases de données en fonction de l'ancienneté ou du manque d'espace disque disponible. L'archivage automatique vous évite de déplacer manuellement les bases de données.
- Il stocke en local les bases de données froides. Vous pouvez également déplacer ou copier ces bases de données vers un emplacement hors site à des fins de stockage à long terme. Les bases de données froides sont généralement conservées pendant le nombre d'années stipulé par les agences réglementaires gouvernementales.

Les serveurs de stockage distants ne font jamais partie d'une fédération CA Enterprise Log Manager. Toutefois, ils méritent votre considération lorsque vous prévoyez votre architecture.

- Serveur de point de restauration

En général, les serveurs de rapports agissent comme des serveurs de point de restauration pour les bases de données qu'ils ont stockées auparavant. Si vous disposez d'un réseau de grande taille, envisagez de dédier un serveur CA Enterprise Log Manager à ce rôle. Un serveur de point de restauration réalise les fonctions ci-dessous.

- Il est utilisé pour étudier les journaux d'anciens événements.
- Il reçoit les bases de données restaurées provenant d'un serveur de stockage distant, qui détient toutes les bases de données froides. L'utilitaire `restore-ca-elm.sh` vous permet de déplacer des bases de données sur le point de restauration si l'authentification non interactive est configurée pour permettre des transactions du serveur de stockage vers le point de restauration.
- Il traite le catalogue d'archive pour ajouter les bases de données restaurées à ses enregistrements.
- Il conserve les enregistrements restaurés pendant des durées différentes, en fonction de la méthode de restauration.

Le point de restauration dédié permet d'exclure ce serveur de la fédération pour assurer qu'aucun rapport fédéré ne contient d'anciennes données restaurées. Tous les rapports générés sur le serveur de point de restauration reflètent uniquement les données d'événement provenant des bases de données restaurées.

Dédier un serveur à un rôle donné ne signifie pas que vous ne pouvez pas effectuer des fonctions associées à d'autres rôles à partir de ce serveur. Envisagez un environnement comprenant des serveurs de collecte dédiés et un serveur de génération de rapports. Vous avez également la possibilité de planifier une alerte afin de rechercher une condition sur un serveur de collecte si vous devez impérativement en être informé le plus vite possible.

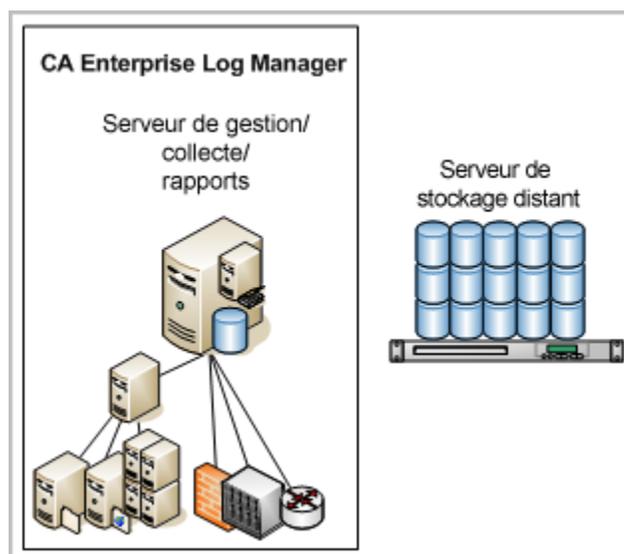
Exemple : Architectures réseau

L'architecture CA Enterprise Log Manager la plus simple est un système à un seul serveur, dans lequel un serveur CA Enterprise Log Manager assume tous les rôles.

- CA Enterprise Log Manager de gestion, de collecte et de génération de rapports s'occupe de la gestion de la configuration/du contenu, de la collecte/l'ajustement et la corrélation des événements, ainsi que des requêtes et des rapports.

Remarque : Un serveur distant non CA Enterprise Log Manager stocke les bases de données archivées des journaux d'événements.

Cette configuration convient pour le traitement d'un volume d'événements peu élevé et de rapports planifiés peu nombreux, comme dans un système de test.

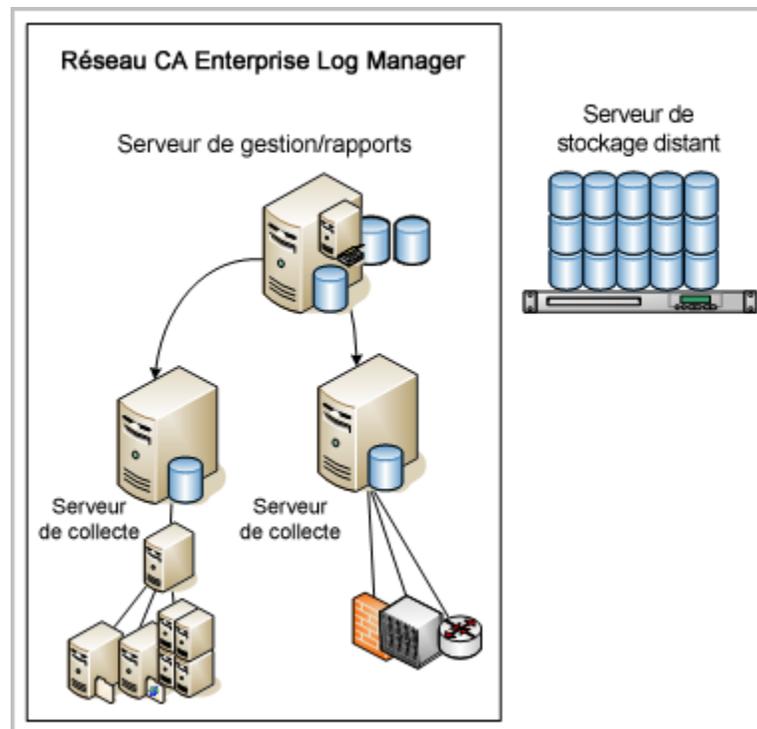


La deuxième architecture la plus simple est un système comptant plusieurs serveurs, dans lequel le premier CA Enterprise Log Manager installé effectue la plupart des rôles.

- CA Enterprise Log Manager de gestion et de génération de rapport s'occupe de la gestion de la configuration/du contenu, ainsi que des requêtes et des rapports et de la corrélation d'événements.
- CA Enterprise Log Manager de collecte s'occupe de la collecte et de l'ajustement d'événements.

Remarque : Un serveur distant non CA Enterprise Log Manager est configuré pour stocker les bases de données archivées des journaux d'événements.

Cette architecture convient à un réseau affichant un volume d'événements modéré. Les flèches indiquent que la fonctionnalité de gestion du serveur de gestion/rapports conserve les paramètres globaux qui s'appliquent à tous les serveurs. Lorsqu'il y a de nombreux serveurs de collecte, cette architecture est appelée "configuration en étoile".

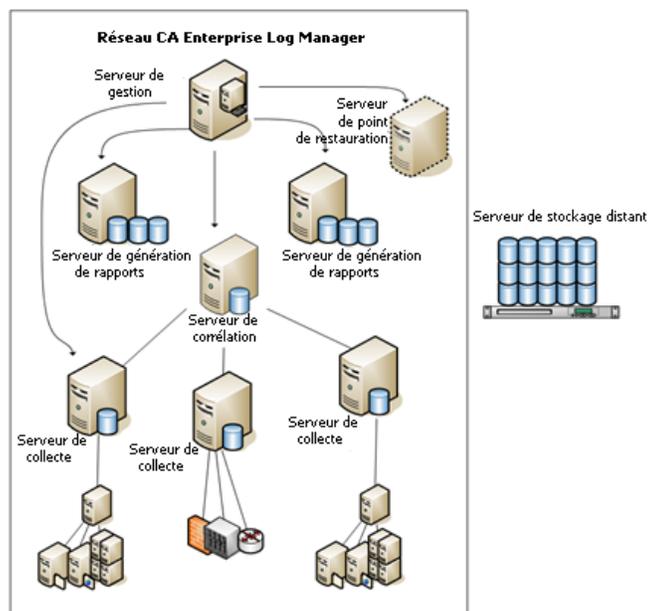


Sur un réseau important, qui gère un volume d'événements élevé, de nombreux rapports planifiés et alertes, ainsi que la personnalisation continue, vous pouvez dédier un ou plusieurs serveurs CA Enterprise Log Manager à des rôles uniques.

- CA Enterprise Log Manager de gestion s'occupe de la gestion de la configuration/du contenu.
- CA Enterprise Log Manager de rapports gère les requêtes et les rapports.
- CA Enterprise Log Manager de collecte s'occupe de la collecte et de l'ajustement d'événements.
- CA Enterprise Log Manager de corrélation traite la corrélation d'événements.
- CA Enterprise Log Manager de point de restauration gère éventuellement l'examen des événements à partir des bases de données d'archive restaurées.

Remarque : Un serveur distant non CA Enterprise Log Manager est configuré pour stocker les bases de données archivées des journaux d'événements.

Cette configuration est idéale pour les très grands réseaux. Les flèches indiquent que le serveur de gestion conserve les paramètres globaux qui s'appliquent à tous les serveurs.



Planification de la collecte de journaux

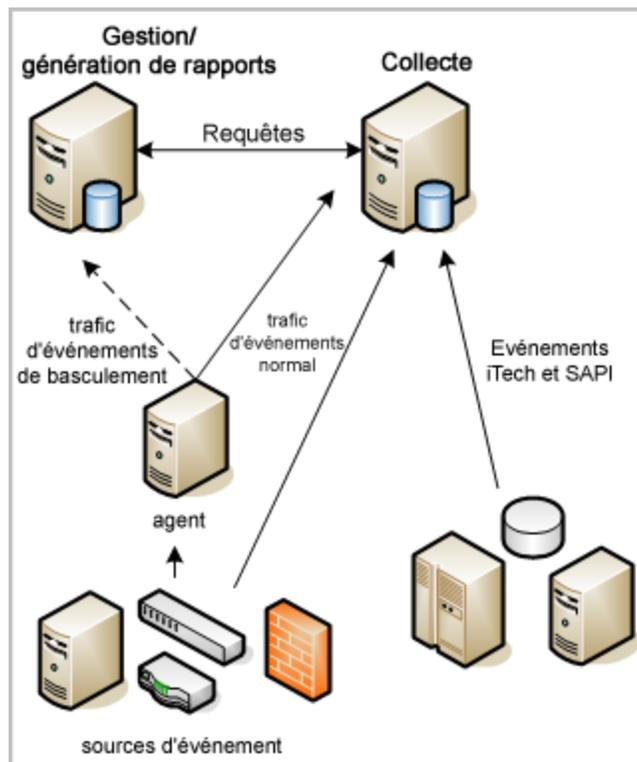
La planification de la collecte de journaux pour votre réseau est basée sur le nombre d'événements par seconde que vous devez traiter à des fins de stockage et la durée pendant laquelle vous devez conserver les données en ligne (dans ce sens, *en ligne* signifie pouvant faire l'objet d'une recherche immédiate). Généralement, vous disposez seulement de 30 à 90 jours de mise en ligne des données.

Chaque réseau dispose de ses propres volumes d'événements en fonction du nombre d'unités, des types d'unités et du degré de réglage des unités et applications réseau telles que les pare-feu, pour répondre aux besoins d'informations sur les événements de l'entreprise. Par exemple, en fonction de leur configuration, certains pare-feu peuvent générer d'énormes volumes d'événements inutiles.

Nous vous recommandons de planifier votre collecte d'événements pour que votre volume total d'événements soit uniformément réparti sur vos serveurs CA Enterprise Log Manager, sans forcer l'un d'entre eux à dépasser le niveau normal d'utilisation constante. Pour conserver d'excellentes performances avec les volumes d'événements d'une entreprise, nous vous recommandons d'installer au moins deux serveurs CA Enterprise Log Manager fédérés.

- Un serveur CA Enterprise Log Manager de rapports traite les requêtes et les rapports, les alertes et la gestion de celles-ci, les mises à jour d'abonnement, ainsi que l'authentification et l'autorisation des utilisateurs.
- Un ou plusieurs serveurs CA Enterprise Log Manager de collecte sont spécifiquement configurés pour optimiser les insertions dans la base de données.

L'illustration ci-dessous présente un exemple simple de ce type de réseau CA Enterprise Log Manager fédéré. Deux serveurs CA Enterprise Log Manager, un pour les rapports et un pour la collecte, gèrent le trafic d'événements provenant de différentes sources d'événement. Les deux serveurs peuvent partager des données pour les requêtes, les rapports et les alertes.



Le serveur de *collecte* gère principalement le trafic de journaux d'événements entrants et se concentre sur les insertions dans la base de données. Il utilise une stratégie de conservation brève des données, au maximum 24 heures. Un script automatisé déplace les journaux d'événements stockés vers un serveur de rapports chaque jour, ou plus souvent, en fonction du volume d'événements. La fédération et l'utilisation de requêtes fédérées entre les deux serveurs vous garantissent de recevoir des rapports précis à partir des journaux d'événements sur les *deux* serveurs.

Le serveur de *rapports* réalise plusieurs fonctions.

- Il traite les requêtes et les rapports.
- Il planifie et gère les alertes.
- Il déplace les fichiers archivés vers un serveur de stockage distant.
- Il permet la collecte par basculement d'éléments collectés par des connecteurs pour le serveur de collecte.

Un script de sauvegarde automatisé déplace les données du serveur de rapports au serveur distant (stockage sauvegardé). Si vous décidez de restaurer des données à partir du stockage sauvegardé, vous le faites généralement sur le serveur de rapports. Si l'espace est limité sur le serveur de rapports, vous pouvez également restaurer sur le serveur de collecte. Comme le serveur de collecte ne stocke pas de grandes quantités de données et qu'il est fédéré, les résultats des rapports sont les mêmes.

De plus, le serveur de rapports peut fonctionner comme récepteur de basculement pour les événements collectés par un connecteur sur un agent distant, si le serveur de collecte cesse de recevoir les événements pour une raison quelconque. Vous pouvez configurer le basculement au niveau de l'agent. Le traitement par basculement envoie les événements à un ou plusieurs serveurs CA Enterprise Log Manager alternatifs. La collecte d'événements par basculement n'est pas disponible pour les événements provenant de sources d'événement héritées, collectés par les écouteurs SAPI et iTech.

Informations complémentaires :

[CA Enterprise Log Manager et virtualisation](#) (page 319)

Planification d'espace disque

Lorsque vous planifiez votre environnement, assurez-vous de disposer d'un espace disque suffisant pour prendre en charge des volumes d'événements importants. Chaque serveur de collecte doit disposer d'un espace disque suffisant pour pouvoir contenir sa part de charges de pointe et les volumes d'événements normaux. Pour un serveur de rapports, l'espace disque est calculé en fonction du volume d'événements et de la période requise de conservation en ligne.

Les bases de données chaudes ne sont pas compressées. Les bases de données tièdes sont compressées. Les bases de données chaudes et tièdes sont considérées comme étant en ligne. Vous pouvez effectuer des recherches ou générer des rapports sur leurs données. En général, vous disposez à tout moment d'un maximum de données couvrant 30 à 90 jours pour les rapports et la recherche immédiate. Les enregistrements antérieurs sont stockés sur un serveur distant. Vous pouvez les restaurer selon vos besoins, à des fins de recherche et de génération de rapport.

Les serveurs de collecte prennent en charge aussi bien les bases de données chaudes que les bases de données tièdes. Comme la période de conservation d'un serveur de collecte est très courte (comprise entre 1 et 23 heures), le stockage à long terme n'est pas un facteur important.

Il existe une base de données chaude sur le serveur de gestion pour l'insertion des événements d'autosurveillance.

Les serveurs de rapports prennent en charge de petites bases de données chaudes et un grand nombre de bases de données tièdes. Les serveurs de rapports doivent également disposer d'un espace supplémentaire suffisant pour prendre en charge les fichiers restaurés pendant un certain temps. Lorsque vous utilisez le stockage lié direct, les partitions sont automatiquement étendues pour offrir une plus grande capacité de stockage.

A propos du serveur CA EEM

CA Enterprise Log Manager utilise le serveur CA Embedded Entitlements Manager (CA EEM) en interne pour gérer les configurations, autoriser et authentifier les utilisateurs, coordonner les mises à jour d'abonnement avec le contenu et les fichiers binaires, ainsi que pour effectuer d'autres fonctions de gestion. Dans l'environnement CA Enterprise Log Manager de base, vous installez CA EEM lorsque vous installez le serveur CA Enterprise Log Manager de gestion. Dès lors, CA EEM gère les configurations de tous les serveurs CA Enterprise Log Manager de collecte et de tous leurs agents et connecteurs.

Vous pouvez également choisir d'installer le serveur CA EEM sur un serveur distant à l'aide des packages d'installation fournis sur le disque d'installation de l'application ou vous pouvez utiliser un serveur CA EEM existant, utilisé par d'autres produits CA.

Le serveur CA EEM dispose de sa propre interface Web. Toutefois, la quasi-totalité de vos activités de configuration et de maintenance se déroulent dans l'interface utilisateur CA Enterprise Log Manager. Vous n'avez normalement pas besoin d'interagir directement avec les fonctions du serveur CA EEM intégré, sauf pour les configurations du basculement et les fonctions de restauration qui font partie de la récupération après sinistre.

Remarque : L'installation du serveur CA Enterprise Log Manager implique que vous utilisiez le mot de passe du compte d'administration CA EEM par défaut, EiamAdmin, pour enregistrer correctement un serveur CA Enterprise Log Manager. Lorsque vous installez le premier serveur CA Enterprise Log Manager de gestion, vous créez ce nouveau mot de passe au cours de l'installation. Lorsque vous installez d'autres serveurs CA Enterprise Log Manager avec le même nom d'instance d'application, vous créez automatiquement un environnement réseau dans lequel vous pouvez configurer ultérieurement des relations de fédération entre les serveurs CA Enterprise Log Manager.

Consignes de collecte de journaux

Observez les consignes de collecte de journaux suivantes lors de votre phase de planification.

- Le trafic de l'agent au serveur CA Enterprise Log Manager est toujours chiffré, que vous utilisiez la collecte de journaux sans agent ou avec agent.
- Envisagez d'utiliser un mécanisme local de collecte Syslog pour contourner des problèmes potentiels de remise garantie.

Lorsque vous déterminez l'utilisation de la collecte directe par l'agent par défaut, de la collecte avec agent, lorsque l'agent est installé sur l'hôte avec la source d'événement, ou de la collecte sans agent, lorsque l'agent est installé sur un point de collecte distant des sources d'événement, tenez compte des facteurs ci-après.

- Prise en charge des plates-formes
Par exemple, WMI fonctionne uniquement sous Windows pour le détecteur de journaux.
- Prise en charge des pilotes pour certains détecteurs de journaux
Par exemple, vous avez besoin d'un pilote ODBC pour faire fonctionner ODBC.
- Possibilité d'accéder à distance à la source des journaux
Par exemple, pour les journaux basés sur des fichiers, vous avez besoin d'un lecteur partagé pour qu'ils fonctionnent à distance.

Planification de fédération

Pour CA Enterprise Log Manager, une *fédération* est un réseau de serveurs qui stockent, génèrent des rapports et archivent des données d'événement. Une fédération vous permet de contrôler le regroupement et l'examen de vos données sur un réseau. Vous pouvez configurer les relations de vos serveurs entre eux, ainsi que la manière dont sont envoyées les requêtes d'un serveur à l'autre. De plus, vous pouvez activer et désactiver les requêtes fédérées spécifiques selon vos besoins.

La décision d'utiliser une fédération est fondée sur l'association du volume d'événements requis et des vos besoins professionnels pour séparer les données des journaux et générer des rapports sur elles. CA Enterprise Log Manager prend en charge les fédérations hiérarchiques et maillées, ainsi que les configurations qui associent les deux types. Tous les serveurs CA Enterprise Log Manager que vous souhaitez fédérer doivent utiliser le même nom d'instance d'application dans CA EEM. Chaque installation de serveur CA Enterprise Log Manager s'enregistre automatiquement auprès du serveur CA EEM à l'aide d'un nom d'instance d'application.

Vous pouvez configurer une fédération à tout moment après avoir installé votre premier serveur CA Enterprise Log Manager et au moins un serveur supplémentaire. Toutefois, vous obtiendrez de meilleurs résultats en planifiant votre fédération *avant* l'installation. La création d'une carte de fédération détaillée vous permet d'effectuer les tâches de configuration en alliant rapidité et précision.

Au niveau du *réseau*, le fait de disposer de plusieurs serveurs CA Enterprise Log Manager vous permet de traiter des volumes d'événements plus élevés. Du point de vue des *rapports*, l'utilisation d'une fédération vous permet de contrôler les personnes pouvant accéder aux données d'événement et la quantité de données qu'elles peuvent afficher.

Dans un environnement de base comprenant deux serveurs, le serveur de gestion assume le rôle de serveur de rapports. Sur le serveur CA Enterprise Log Manager de gestion, le serveur CA EEM interne gère les configurations de fédération de manière centrale et globale (vous pouvez modifier les options de configuration depuis n'importe quel serveur CA Enterprise Log Manager sur le réseau). Vous configurez le serveur CA Enterprise Log Manager de collecte comme enfant du serveur de rapports, pour que les requêtes et les rapports incluent les données les plus récentes.

Remarque : Si vous disposez d'un serveur CA EEM existant que vous prévoyez d'utiliser avec CA Enterprise Log Manager, configurez les serveurs CA Enterprise Log Manager de la même manière. Le serveur CA EEM dédié distant stocke ces configurations.

Vous pouvez également définir des options de configuration locales pour supplanter les configurations globales, en permettant aux serveurs CA Enterprise Log Manager sélectionnés de fonctionner différemment des autres. Les exemples incluent l'envoi de rapports et d'alertes par courriel par le biais d'un serveur de messagerie différent ou la planification de rapports propres à une branche d'un réseau, à divers moments.

Informations complémentaires :

[Fédérations hiérarchiques](#) (page 232)

[Fédérations maillées](#) (page 234)

[Requêtes et rapports dans un environnement fédéré](#) (page 231)

[Configuration d'une fédération CA Enterprise Log Manager](#) (page 235)

Création d'une carte de fédération

La création d'une carte de fédération constitue une étape utile lors de la planification et de l'implémentation de la configuration de votre fédération. Plus votre réseau est important, plus cette carte est utile lors des tâches réelles de configuration. Vous pouvez utiliser un programme commercial de graphisme ou de dessin, ou encore tracer la carte à la main. Plus vous fournissez de détails sur votre carte, plus vous pourrez terminer rapidement la configuration.

Pour créer une carte de fédération

1. Commencez votre carte avec les deux serveurs CA Enterprise Log Manager de base (gestion et collecte) et indiquez les détails de chacun.
2. Décidez si vous avez besoin d'autres serveurs de collecte et s'ils représentent le sommet d'une hiérarchie ou une unité dans un maillage.
3. Décidez quel type de fédération (hiérarchique ou maillée) répond le mieux à vos besoins.
4. Identifiez les opportunités de hiérarchies, de branches ou d'interconnexions en fonction de vos besoins professionnels en termes de rapports, de conformité et de débit d'événements.

Par exemple, si votre entreprise a des bureaux sur trois continents, vous pouvez décider de créer trois fédérations hiérarchiques. Vous pouvez ensuite décider de mailler les hiérarchies à un niveau supérieur, pour que les cadres dirigeants et les responsables de la sécurité puissent produire des rapports couvrant l'ensemble du réseau. Vous devez au minimum fédérer les serveurs CA Enterprise Log Manager d'insertion et de requête de l'environnement de base.

5. Décidez combien de serveurs CA Enterprise Log Manager vous devez déployer au total.

Cette valeur est basée sur le nombre d'unités de votre réseau et sur le volume d'événements générés.

6. Décidez du nombre de couches de serveurs fédérés nécessaires.

Ce nombre est fondé en partie sur les décisions prises lors des étapes 2 et 3.

7. Identifiez les types d'événements reçus par chaque serveur CA Enterprise Log Manager de la fédération.

Si votre réseau compte un grand nombre d'unités Syslog et seulement quelques serveurs Windows, vous pouvez décider d'affecter expressément un serveur CA Enterprise Log Manager à la collecte d'événements Windows. Vous pouvez avoir besoin de plusieurs serveurs pour gérer le trafic des événements Syslog. En planifiant à l'avance quels serveurs CA Enterprise Log Manager reçoivent quels types d'événements, vous simplifiez la configuration des écouteurs et services locaux.

8. Tracez une carte de ce réseau pour l'utiliser lors de la configuration des serveurs CA Enterprise Log Manager fédérés (enfants).

Si vous les connaissez, incluez les noms DNS et les adresses IP sur votre carte. Vous utiliserez les noms DNS des serveurs CA Enterprise Log Manager pour configurer les relations de fédération entre eux.

Exemple : Carte de fédération pour une grande entreprise

Lors de la création d'une carte de fédération, tenez compte des types de rapports pour lesquels vous souhaitez différents ensembles de données consolidées. Par exemple, envisagez le scénario pour lequel vous souhaitez des données consolidées à l'aide de trois types de groupements de serveurs.

- Tous les serveurs

Pour obtenir des rapports système sur les événements d'autosurveillance, l'inclusion de tous les serveurs vous permet d'évaluer simultanément la santé de l'ensemble de votre réseau CA Enterprise Log Manager de serveurs.

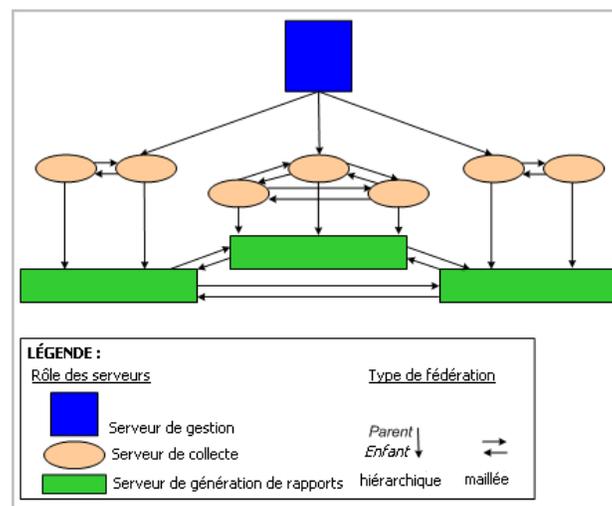
- Tous les serveurs de rapports

Pour les rapports récapitulatifs et de tendances, dans lesquels vous souhaitez examiner les données collectées par tous les agents qui envoient des données à tous les serveurs de collecte, tout en veillant à ce que vos serveurs de collecte ne traitent pas les requêtes sur les nouveaux événements non compressés, vous devez exécuter des rapports fédérés qui incluent uniquement les serveurs de rapports.

- Un ensemble de serveurs de collecte avec leur serveur de rapports

Pour les rapports dont vous souhaitez limiter les données à un paramètre local avec un serveur de rapports, tout en souhaitant que ce rapport inclut les événements qui n'ont pas encore été envoyés à ce serveur par ses serveurs de collecte, vous devez exécuter des rapports fédérés sur ce sous-ensemble de serveurs.

Vous trouverez ci-dessous un exemple de carte de fédération qui vous permet d'atteindre ces objectifs de génération de rapports.



Pour implémenter la conception de cette carte de fédération, effectuez les actions énumérées ci-dessous.

- Créez une fédération hiérarchique du serveur de gestion vers un serveur de collecte lié à chaque serveur de rapports, pour laquelle le serveur de gestion est le parent et chaque serveur de collecte est l'enfant.
- Créez une fédération totalement maillée entre les serveurs de collecte pour chaque serveur de rapports.
- Créez une fédération hiérarchique de chaque serveur de collecte vers son serveur de rapports, pour laquelle le serveur de collecte est le parent et le serveur de rapports est l'enfant.
- Créez une fédération totalement maillée entre les serveurs de rapports.

Pour atteindre un objectif donné de génération de rapports, il est important d'exécuter le rapport depuis un serveur représenté par un emplacement précis sur votre carte de fédération. Vous trouverez plusieurs exemples ci-dessous.

- Pour générer un rapport système sur des événements d'autosurveillance qui se produisent sur chaque CA Enterprise Log Manager de votre réseau, exécutez le rapport depuis le serveur de gestion.
- Pour générer des rapports récapitulatifs et de tendances depuis tous les serveurs de rapports de votre réseau, exécutez le rapport depuis n'importe quel serveur de rapports.
- Pour générer un rapport sur des données se trouvant sur un serveur de rapports et sur ses serveurs de collecte, exécutez le rapport depuis l'un de ces serveurs de collecte.

Exemple : Carte de fédération pour une PME

Avant de créer une carte de fédération, vous devez déterminer le nombre de serveurs que vous voulez affecter à chaque rôle. Dans l'exemple suivant, un serveur est dédié à la gestion et à la génération de rapport et les autres serveurs sont dédiés à la collecte. Cette configuration est recommandée pour les environnements de taille moyenne. Vous pouvez considérer l'architecture constituée par le serveur de gestion/de rapports et les serveurs de collecte comme étant une configuration en étoile dans laquelle le centre est le serveur de gestion/de rapports. Le diagramme de la carte de fédération ne représente pas cette configuration, mais indique les niveaux afin que vous puissiez facilement distinguer les paires fédérées hiérarchiquement des paires maillées.

Lors de la création d'une carte de fédération, tenez compte des rapports et des alertes pour lesquels vous souhaitez différents ensembles de données consolidées. Par exemple, envisagez le scénario pour lequel vous souhaitez des données consolidées à l'aide de deux types de groupements de serveurs.

- Serveur de gestion/rapports uniquement

Pour la plupart des rapports, lorsque vous souhaitez examiner les événements récemment archivés (tièdes) tout en évitant que les requêtes des nouveaux événements (chauds) soient traitées par vos serveurs de collecte.

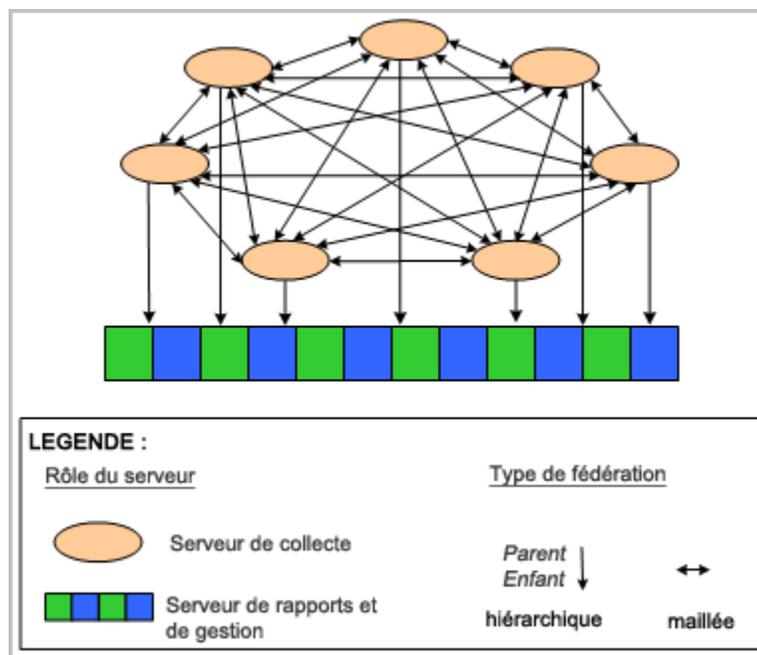
Remarque : Les événements sont généralement archivés depuis les serveurs de collecte (branches) vers le serveur de rapports (centre), toutes les heures.

- Tous les serveurs

Pour les rapports système sur les événements d'autosurveillance, lorsque vous voulez évaluer l'état de santé de tous vos serveurs CA Enterprise Log Manager en une seule opération.

Pour les alertes, lorsqu'il est important de rechercher les événements à partir de tous les serveurs de collecte.

Vous trouverez ci-dessous un exemple de carte de fédération qui vous permet d'atteindre ces objectifs de génération de rapports.



Pour implémenter la conception de cette carte de fédération, effectuez les actions énumérées ci-dessous.

- Créez une fédération totalement maillée entre les serveurs de collecte. Chaque serveur de collecte est à la fois parent et enfant de tous les autres serveurs de collecte.
- Créez une fédération hiérarchique de chaque serveur de collecte vers le serveur de gestion/rapports, dans laquelle le serveur de collecte est le parent et le serveur de gestion/rapports est l'enfant.

Pour atteindre un objectif donné, il est important d'exécuter le rapport ou l'alerte à partir d'un serveur représenté par un emplacement précis de votre carte de fédération et de spécifier correctement si la fédération est requise. Vous trouverez plusieurs exemples ci-dessous.

- Pour planifier un rapport système sur des événements d'autosurveillance qui se produisent sur chaque CA Enterprise Log Manager de votre réseau, exécutez le rapport depuis le serveur de gestion/rapports et sélectionnez l'option Fédéré(e).
- Pour planifier un rapport sur des événements récents (tièdes), exécutez le rapport à partir du serveur de gestion/rapports et désélectionnez l'option Fédéré(e). Ce rapport contient les données archivées récemment collectées par tous les serveurs de collecte. La fédération n'est pas requise.
- Pour planifier une alerte incluant les nouveaux événements (chauds) de chaque serveur de collecte et les événements archivés (tièdes) du serveur de gestion/rapports, exécutez l'alerte à partir de n'importe quel serveur de collecte et sélectionnez l'option Fédéré(e). Vous pouvez limiter la quantité d'informations renvoyées aux serveurs de collecte en spécifiant comme critère de recherche une plage prédéfinie, par exemple au cours de la dernière heure.

Informations complémentaires :

[Configuration d'un serveur CA Enterprise Log Manager en tant que serveur enfant](#) (page 236)

[Exemple : Archivage automatique sur trois serveurs](#) (page 175)

Planification des utilisateurs et des accès

Après avoir installé le premier serveur CA Enterprise Log Manager et y avoir accédé en tant qu'utilisateur EiamAdmin, vous pouvez configurer le magasin d'utilisateurs, configurer un utilisateur en temps qu'administrateur et définir des stratégies de mots de passe.

La planification des utilisateurs et des accès est limitée aux éléments ci-dessous.

- Déterminez si vous devez accepter le magasin d'utilisateurs par défaut sur ce serveur CA Enterprise Log Manager ou configurer un magasin d'utilisateurs externe. Si la configuration est nécessaire, enregistrez les valeurs requises dans les feuilles de calcul fournies.
- Identifiez l'utilisateur qui agira comme le premier administrateur. Seul un administrateur peut configurer des paramètres CA Enterprise Log Manager.
- Définissez les stratégies de mots de passe en ayant pour objectif de promouvoir des mots de passe sûrs pour les utilisateurs de CA Enterprise Log Manager.

Remarque : Vous ne pouvez configurer des stratégies de mots de passe que lorsque vous configurez le magasin d'utilisateurs sur ce CA Enterprise Log Manager.

Informations complémentaires :

[Feuille de calcul du répertoire LDAP externe](#) (page 44)

[Feuille de calcul CA SiteMinder](#) (page 46)

Planification du magasin d'utilisateurs

Après avoir installé le premier serveur CA Enterprise Log Manager, connectez-vous à CA Enterprise Log Manager et configurez le magasin d'utilisateurs. Le magasin d'utilisateurs configuré est l'emplacement de stockage des noms d'utilisateur et des mots de passe utilisés pour l'authentification, ainsi que d'autres détails d'ordre général.

Avec toutes les options du magasin d'utilisateurs, les détails des utilisateurs de l'application sont stockés dans le magasin d'utilisateurs CA Enterprise Log Manager. Ils incluent notamment des informations comme les rôles, les favoris des utilisateurs et la dernière connexion.

Tenez compte des éléments ci-dessous lors de la planification du magasin d'utilisateurs à configurer.

- Utilisation du magasin d'utilisateurs CA Enterprise Log Manager (par défaut)

Les utilisateurs sont authentifiés par leur nom d'utilisateur et leur mot de passe, créés dans CA Enterprise Log Manager. Vous configurez des stratégies de mots de passe. Les utilisateurs peuvent modifier leurs propres mots de passe et déverrouiller d'autres comptes d'utilisateur.

- Référence à partir de CA SiteMinder

Les noms d'utilisateur, les mots de passe et les groupes globaux sont chargés depuis CA SiteMinder vers le magasin d'utilisateurs CA Enterprise Log Manager. Les utilisateurs sont authentifiés par leur nom d'utilisateur et leur mot de passe référencés. Vous pouvez affecter le groupe global à une stratégie nouvelle ou existante. Vous ne pouvez pas créer de nouveaux utilisateurs, modifier les mots de passe ou configurer des stratégies de mots de passe.

- Référence à partir du répertoire LDAP (Lightweight Directory Access Protocol)

Les noms d'utilisateur et les mots de passe sont chargés depuis le répertoire LDAP vers le magasin d'utilisateurs CA Enterprise Log Manager. Les utilisateurs sont authentifiés par leur nom d'utilisateur et leur mot de passe référencés. Les informations des comptes d'utilisateur chargés créent des comptes d'utilisateur globaux. Vous pouvez affecter aux utilisateurs globaux un rôle d'utilisateur correspondant à l'accès que vous souhaitez lui attribuer dans CA Enterprise Log Manager. Vous ne pouvez pas créer de nouveaux utilisateurs ou configurer des stratégies de mots de passe.

Important : Nous vous recommandons de sauvegarder les stratégies d'accès prédéfinies fournies avec CA Enterprise Log Manager avant que vous ou tout autre administrateur ne commence à travailler dessus. Pour plus de détails, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Informations complémentaires :

[Acceptation du magasin d'utilisateurs par défaut](#) (page 140)

[Référence à un répertoire LDAP](#) (page 141)

[Référence à CA SiteMinder comme magasin d'utilisateurs](#) (page 142)

Feuille de calcul du répertoire LDAP externe

Avant de référencer un répertoire LDAP externe, collectez les informations de configuration ci-après.

Informations requises	Valeur	Commentaires
Type		Notez le type de répertoire utilisé. CA Enterprise Log Manager prend en charge plusieurs répertoires différents, dont Microsoft Active Directory et Sun ONE Directory. Reportez-vous à l'interface utilisateur pour obtenir la liste complète des répertoires pris en charge.
Hôte		Enregistrez le nom d'hôte du serveur pour le magasin d'utilisateurs ou le répertoire externe.
Port		Enregistrez le numéro de port pour l'écoute du serveur du magasin d'utilisateurs ou du répertoire externe. Le port 389 est le port réservé à LDAP (Lightweight Directory Access Protocol). Si votre serveur de registre n'utilise pas le port 389, enregistrez le numéro de port adéquat.
Nom relatif de base		Enregistrez le nom relatif LDAP servant de base. Le nom relatif est un identifiant unique pour une entrée dans l'arborescence du répertoire LDAP. Aucun espace n'est permis dans le nom relatif de base. Seuls les utilisateurs et groupes globaux détectés sous ce nom relatif sont mappés et peuvent se voir affecter un rôle ou un groupe d'applications CA Enterprise Log Manager.
Mot de passe		Entrez et confirmez le mot de passe de l'utilisateur répertorié à la ligne Nom relatif de l'utilisateur.

Informations requises	Valeur	Commentaires
Nom relatif de l'utilisateur		<p>Entrez les informations d'identification valides pour tout utilisateur valide dans le registre d'utilisateurs où vous pouvez rechercher l'enregistrement de l'utilisateur. Entrez le nom relatif complet de l'utilisateur.</p> <p>Vous pouvez vous connecter avec n'importe quel ID d'utilisateur ayant un rôle d'administration. Le nom relatif de l'utilisateur et le mot de passe associé constituent les informations d'identification utilisées pour la liaison avec l'hôte du répertoire externe.</p>
Utiliser Transport Layer Security (TLS)		Spécifie si votre magasin d'utilisateurs doit utiliser le cadre d'applications TSL pour protéger les transmissions de texte en clair. Lorsqu'il est sélectionné, TLS est utilisé pour réaliser la connexion LDAP vers le répertoire externe.
Inclure les attributs non mappés		Spécifie si vous devez inclure des champs non synchronisés provenant du répertoire LDAP. Les attributs externes non mappés peuvent être utilisés pour la recherche et comme filtres.
Cache des utilisateurs globaux		Spécifie s'il faut stocker les utilisateurs globaux dans la mémoire pour y accéder rapidement. Cette sélection permet des recherches plus rapides, au détriment de la modularité. Pour un petit environnement de test, cette sélection est recommandée.
Durée de mise à jour du cache		Si vous choisissez de mettre en cache les utilisateurs globaux, spécifiez la fréquence (en minutes) de la mise à jour des groupes et utilisateurs globaux mis en cache afin d'inclure les nouveaux enregistrements et les modifications.
Récupérer les groupes d'échange sous forme de groupes d'utilisateurs globaux		Si le type de répertoire externe est Microsoft Active Directory, cette option spécifie que vous souhaitez créer des groupes globaux avec les informations du groupe Microsoft Exchange. Si cette option est sélectionnée, vous pouvez écrire des stratégies à l'encontre des membres des listes de distribution.

Feuille de calcul CA SiteMinder

Avant de référencer CA SiteMinder en tant que magasin d'utilisateurs, collectez les informations de configuration ci-après.

Informations requises	Valeur	Commentaires
Hôte		Définit le nom d'hôte ou l'adresse IP du système CA SiteMinder référencé. Vous pouvez utiliser des adresses IPv4 ou IPv6.
Nom d'administrateur		Nom d'utilisateur du superutilisateur CA SiteMinder qui conserve les objets système et domaine
Mot de passe de l'administrateur		Mot de passe du nom utilisateur associé
Nom de l'agent		Nom de l'agent fourni au serveur de stratégies. Ce nom n'est pas sensible à la casse.
Secret de l'agent		Secret partagé sensible à la casse, tel que défini pour CA SiteMinder. Le secret de l'agent est sensible à la casse.
Cache des utilisateurs globaux		Spécifie s'il faut mettre les utilisateurs globaux en cache dans la mémoire, ce qui permet des recherches plus rapides, au détriment de la modularité. Remarque : Les <i>groupes</i> d'utilisateurs globaux sont toujours mis en cache.
Durée de mise à jour du cache		Intervalle, en minutes, après lequel le cache d'utilisateurs est automatiquement mis à jour.
Inclure les attributs non mappés		Spécifie s'il faut inclure les attributs externes non mappés pour les utiliser comme filtres ou dans des recherches.
Récupérer les groupes d'échange sous forme de groupes d'utilisateurs globaux		Si le type de répertoire externe est Microsoft Active Directory, cette option spécifie que vous souhaitez créer des groupes globaux avec les informations du groupe Microsoft Exchange. Si cette option est sélectionnée, vous pouvez écrire des stratégies à l'encontre des membres des listes de distribution.
Type de magasin d'–autorisations		Définit le type de magasin d'utilisateurs en cours d'utilisation.

Informations requises	Valeur	Commentaires
Nom du magasin d'autorisations		Spécifie le nom affecté du magasin d'utilisateurs référencé dans le champ Type de magasin d'autorisations.

Utilisateurs ayant le rôle Administrator

Seuls les utilisateurs affichant le rôle Administrator peuvent configurer les composants CA Enterprise Log Manager.

Une fois le premier CA Enterprise Log Manager installé, vous accédez au CA Enterprise Log Manager par le biais d'un navigateur, vous vous connectez avec vos informations d'identification EiamAdmin et vous configurez le magasin d'utilisateurs.

L'étape suivante consiste à affecter le groupe d'applications Administrator au compte de l'utilisateur qui doit effectuer la configuration. Si vous avez configuré le magasin d'utilisateurs comme le magasin d'utilisateurs CA Enterprise Log Manager par défaut, vous créez un nouveau compte d'utilisateur et vous lui affectez le rôle Administrator. Si vous avez référencé un magasin d'utilisateurs externe, vous ne pouvez pas créer de nouvel utilisateur. Dans ce cas, recherchez l'enregistrement d'utilisateur de la personne qui doit être l'administrateur, puis ajoutez le groupe d'applications Administrator au compte de cet utilisateur.

Planification de la stratégie de mots de passe

Si vous acceptez le magasin d'utilisateurs par défaut, vous définissez de nouveaux utilisateurs et définissez des stratégies de mots de passe pour ces comptes d'utilisateur à partir de CA Enterprise Log Manager. L'utilisation de mots de passe sûrs vous permet de protéger vos ressources informatiques. Les stratégies de mots de passe permettent la mise en oeuvre de la création de mots de passe sûrs et peuvent permettre d'éviter l'utilisation de mots de passe non sécurisés.

Les stratégies de mots de passe par défaut fournies avec CA Enterprise Log Manager offrent une forme très *légère* de protection par mot de passe. Par exemple, la stratégie par défaut permet aux utilisateurs de se servir de leur nom d'utilisateur comme mot de passe et de déverrouiller les mots de passe. Elle autorise les mots de passe à ne jamais expirer et n'effectue aucun verrouillage lié aux échecs de tentatives de connexion. Les options par défaut sont intentionnellement définies sur un niveau très faible de sécurité des mots de passe, pour vous permettre de créer vos propres stratégies personnalisées.

Important : Vous devez modifier les stratégies de mots de passe par défaut pour qu'elles correspondent aux restrictions de mot de passe en vigueur dans votre entreprise. Il n'est pas recommandé d'exécuter CA Enterprise Log Manager dans des environnements de production avec les stratégies de mots de passe par défaut.

Pour votre stratégie de mots de passe personnalisée, vous pouvez refuser ces activités, appliquer des stratégies sur les attributs du mot de passe tels que la longueur, le type de caractère, l'ancienneté et la réutilisation, ou encore établir une stratégie de verrouillage basée sur un nombre configurable d'échecs de tentatives de connexion.

Informations complémentaires :

[Configuration des stratégies de mots de passe](#) (page 144)

Nom d'utilisateur comme mot de passe

Pour que les mots de passe soient sûrs, les meilleures pratiques de sécurité stipulent que les mots de passe ne doivent pas contenir le nom d'utilisateur ou correspondre à celui-ci. La stratégie de mots de passe par défaut active cette option. Même si cette option peut paraître utile lors du paramétrage d'un mot de passe temporaire pour de nouveaux utilisateurs, mieux vaut désélectionner cette stratégie de mots de passe. Ainsi, vous empêchez les utilisateurs d'utiliser ce genre de mots de passe non sécurisés.

Ancienneté et réutilisation du mot de passe

Observez les consignes ci-dessous lorsque vous décidez des stratégies d'ancienneté et de réutilisation.

- La stratégie de réutilisation du mot de passe peut garantir qu'un mot de passe donné n'est pas réutilisé fréquemment. Cette stratégie crée un historique des mots de passe. Un paramètre 0 indique que l'historique des mots de passe n'est pas appliqué. Un paramètre supérieur à 0 spécifie le nombre de mots de passe enregistrés pour comparaison lors de la modification du mot de passe. Une stratégie de mots de passe sûrs doit empêcher les utilisateurs de réutiliser un mot de passe pendant un an au minimum.
- L'*ancienneté maximale* recommandée pour un mot de passe varie en fonction de la longueur et de la complexité du mot de passe. Selon une règle générale, un mot de passe est acceptable lorsqu'il ne peut pas être révélé par une attaque en force en moins de temps que l'ancienneté maximale autorisée du mot de passe. L'ancienneté maximale correcte est comprise entre 30 et 60 jours.
- Le paramétrage d'une *ancienneté minimale* empêche les utilisateurs de redéfinir plusieurs fois des mots de passe au cours d'une seule session, pour travailler sur une stratégie de restriction de réutilisation. La meilleure pratique courante recommande 3 jours.
- Si vous définissez une ancienneté de mot de passe, nous vous recommandons d'avertir les utilisateurs pour qu'ils réinitialisent leur mot de passe. Vous pouvez définir l'avertissement pour qu'il se produise à la moitié de l'ancienneté ou plus près de son expiration.
- Vous devez verrouiller les comptes d'utilisateur après un nombre raisonnable d'échecs de connexion. Vous empêchez ainsi que les pirates ne parviennent à deviner les mots de passe. Le nombre de tentatives avant le verrouillage du compte est généralement compris entre trois et cinq.

Longueur et format du mot de passe

Observez les consignes ci-dessous lorsque vous décidez d'appliquer ou non des restrictions de longueur.

- En raison du mode de chiffrement, les mots de passe les plus sûrs comportent sept ou quatorze caractères.
- Veillez à ne pas dépasser les restrictions de longueur de mot de passe imposées par les systèmes d'exploitation les plus anciens sur votre réseau.

Observez les consignes ci-dessous lorsque vous décidez d'appliquer ou non des stratégies sur le nombre maximum de caractères répétés ou sur le nombre minimum de caractères numériques.

- Les mots de passe sûrs ne peuvent pas être trouvés dans un dictionnaire.
- Les mots de passe sûrs incluent un ou plusieurs caractères provenant, au minimum, de trois des quatre jeux de caractères que sont les lettres minuscules, les lettres majuscules, les chiffres et les caractères spéciaux.

Planification des mises à jour d'abonnement

Cette section contient des informations et des procédures sur la planification de mises à jour d'abonnement pour votre environnement CA Enterprise Log Manager.

Informations complémentaires :

[Service d'abonnement](#) (page 51)

[Fonctionnement de l'abonnement](#) (page 52)

[Planification des mises à jour d'abonnement](#) (page 54)

[Architecture d'abonnement](#) (page 56)

[Architecture d'abonnement hors ligne](#) (page 59)

Service d'abonnement

Votre environnement peut contenir un serveur effectuant toutes les tâches, ou divers serveurs, chacun dédié à un ou plusieurs rôles spécifiques, tels que la collecte, la corrélation et la génération de rapports. Utilisez le service d'abonnement pour maintenir à jour tous vos serveurs avec les mises à jour de contenu, de système d'exploitation et de produit les plus récentes.

Le service d'abonnement utilise un système de client proxy pour la livraison des mises à jour. CA publie des mises à jour, mises en package dans *des modules*, vers le serveur d'abonnement CA. Dans votre environnement, un ou plusieurs de serveurs servent de *proxys* d'abonnement. Ces proxys contactent le serveur d'abonnement CA via Internet, téléchargent des modules de mise à jour et les installent automatiquement. Tous les autres serveurs de votre environnement sont des clients d'abonnement, qui téléchargent des mises à jour à partir des proxys à tour de rôle.

Dans certains environnements, des stratégies de sécurité ou d'autres éléments limitent l'accès du réseau à Internet. Dans ce type de cas, mettez à jour votre environnement CA Enterprise Log Manager via l'abonnement hors ligne.

L'abonnement hors ligne requiert le téléchargement de mises à jour à partir du site FTP d'abonnement hors ligne CA. Copiez-les manuellement vers un proxy CA Enterprise Log Manager ne disposant pas de l'accès à Internet, appelé *proxy hors ligne*. Les mises à jour se poursuivent normalement, à l'aide de clients d'abonnement qui téléchargent et installent des mises à jour à partir de ce proxy hors ligne.

Remarque : Par défaut, le service d'abonnement n'est pas configuré pour effectuer des mises à jour automatiques. Pour utiliser le service d'abonnement, configurez des paramètres ; par exemple, choisissez des modules et définissez une planification de mises à jour.

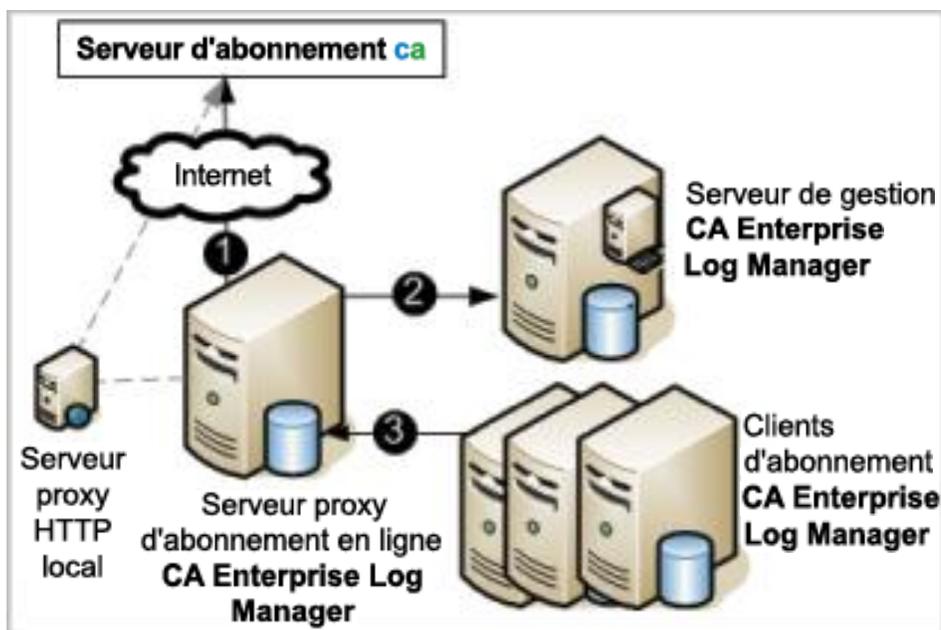
Fonctionnement de l'abonnement

L'abonnement implique les composants ci-dessous.

- Serveur d'abonnement CA
- Serveur proxy HTTP (facultatif)
- Un ou plusieurs serveurs proxys d'abonnement CA Enterprise Log Manager
- Serveur de gestion CA Enterprise Log Manager
- Un ou plusieurs clients d'abonnement CA Enterprise Log Manager

Vous pouvez configurer les mises à jour d'abonnement pour qu'elles s'effectuent automatiquement, selon une planification d'abonnement définie. Vous pouvez également effectuer des mises à jour d'abonnement à la demande ; pour ce faire, lancez manuellement le processus de mise à jour.

Le diagramme suivant illustre le processus du service d'abonnement en détail.



1. Le serveur proxy d'abonnement contacte le serveur d'abonnement CA. Vous pouvez configurer des serveurs proxys pour qu'ils contactent le serveur d'abonnement directement ou via votre proxy HTTP local. Les proxys contactent le serveur d'abonnement CA automatiquement, selon une planification définie, ou à la demande, lors du lancement manuelle d'une mise à jour. Le serveur proxy télécharge et installe automatiquement les mises à jour système d'exploitation et de produit.

Si vous utilisez un abonnement hors ligne, téléchargez manuellement les fichiers de mise à jour sur un système différent de votre environnement CA Enterprise Log Manager, et copiez-les vers le serveur proxy hors ligne.

2. Le serveur proxy d'abonnement envoie les mises à jour de contenu et d'intégration vers le serveur de gestion. Par défaut, le serveur de gestion est le premier serveur CA Enterprise Log Manager installé ; il stocke toutes les informations de contenu, comme les rapports, les intégrations et les règles de corrélation, de votre environnement.
3. Les clients d'abonnement contactent le proxy d'abonnement pour obtenir des mises à jour, automatiquement ou à la demande. Les clients téléchargent et installent automatiquement les mises à jour.

Remarque : Les proxys d'abonnement installent les mises à jour qu'ils téléchargent avant de les mettre à disposition des clients.

Planification des mises à jour d'abonnement

La planification de l'architecture de mises à jour d'abonnement pour votre environnement CA Enterprise Log Manager permet d'assurer que tous les serveurs reçoivent les mises à jour sélectionnées, en temps voulu et de façon sécurisée.

Pour planifier des mises à jour d'abonnement pour votre environnement CA Enterprise Log Manager, suivez le processus suivant. Pour plus d'informations, reportez-vous aux procédures associées.

1. Tout d'abord, élaborer une structure de clients proxys pour vos serveurs CA Enterprise Log Manager. Choisissez des serveurs qui serviront de proxys et ceux qui serviront de clients, tout en tenant compte du rôle de chaque serveur et des éléments relatifs au trafic réseau.
2. Prenez en compte les restrictions d'accès Internet dans votre environnement et choisissez un ou plusieurs proxys hors ligne en fonction de vos besoins.
3. Prenez en compte les problèmes liés à la sécurité Internet et au trafic et choisissez d'inclure ou non un proxy HTTP local dans votre architecture d'abonnement. Les proxys d'abonnement en ligne peuvent contacter le serveur d'abonnement CA directement ou à l'aide de votre proxy HTTP local.
4. Choisissez de télécharger ou non toutes les mises à jour automatiquement, selon la planification d'abonnement définie, ou sélectionnez-en à télécharger manuellement. Par exemple, pour les stratégies de sécurité internes, vous devrez peut-être tester certaines mises à niveau avant de les appliquer à votre environnement.
5. Choisissez la fréquence de mise à jour de votre environnement CA Enterprise Log Manager. Des mises à jour sont régulièrement disponibles ; la fréquence dépend du type de mise à jour. Pour plus d'informations sur les types de mises à jour, reportez-vous à la rubrique Modules à télécharger de la section Informations complémentaires.

Remarque : Avant d'effectuer des mises à jour d'abonnement, confirmez que vous disposez d'espace disque suffisant pour les télécharger vers chaque serveur CA Enterprise Log Manager. Si l'espace disque disponible sur un serveur est inférieur à 5 Go, le service d'abonnement émet un événement d'auto-surveillance et interrompt le téléchargement.

Informations complémentaires :

[Architecture d'abonnement](#) (page 56)

[Architecture d'abonnement hors ligne](#) (page 59)

[Modules à télécharger](#) (page 203)

Architecture d'abonnement

Votre environnement CA Enterprise Log Manager peut être un système à serveur unique ou en inclure plusieurs. Elaborez l'architecture d'abonnement en fonction du nombre de serveurs CA Enterprise Log Manager dans votre environnement et de leurs rôles. Les architectures possibles sont répertoriées ci-dessous.

- Environnement à serveur unique
- Environnement contenant plusieurs serveurs et un proxy d'abonnement
- Environnement contenant plusieurs serveurs et plusieurs proxys d'abonnement

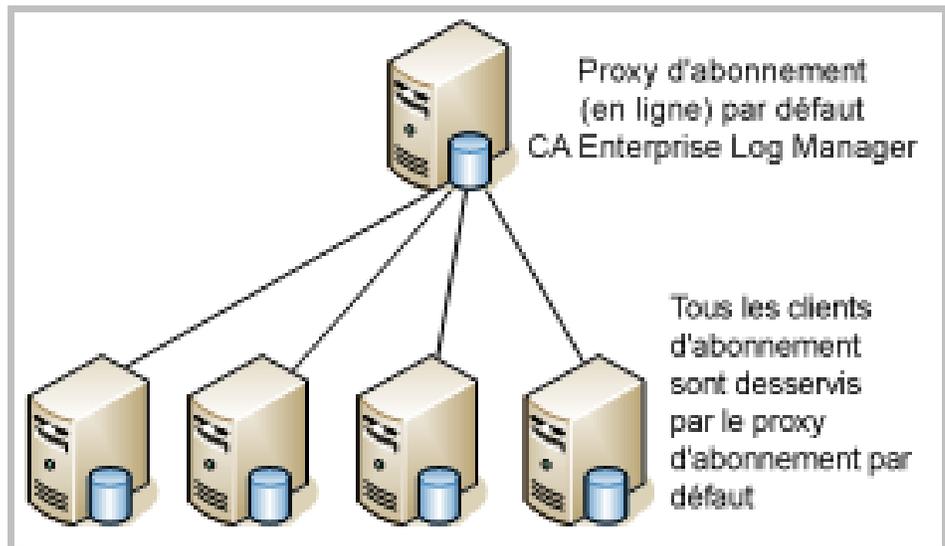
Remarque : Lorsque vous choisissez une architecture d'abonnement, tenez compte du nombre de proxys hors ligne dont vous avez besoin. Pour plus d'informations, reportez-vous à la rubrique Architecture d'abonnement hors ligne de la section Informations complémentaires.

Le premier serveur CA Enterprise Log Manager installé est configuré en tant que *proxy d'abonnement par défaut* ; il télécharge et installe des mises à jour d'abonnement si aucun autre proxy n'est configuré ou disponible. Les serveurs CA Enterprise Log Manager suivants sont, par défaut, configurés en tant que clients d'abonnement. Vous pouvez changer la configuration d'un serveur CA Enterprise Log Manager pour l'utiliser comme proxy d'abonnement en ligne ou hors ligne, ou comme client d'abonnement. Vous pouvez également choisir un proxy d'abonnement en ligne dans votre environnement pour servir de proxy d'abonnement par défaut.

Le *serveur de contenu* fournit des mises à jour de contenu et d'intégration au serveur de gestion, qui stocke et récupère le contenu d'application pour votre environnement. Ce serveur peut être le proxy d'abonnement par défaut, ou vous pouvez configurer un proxy d'abonnement en ligne dans votre environnement qui sera utilisé comme serveur de contenu.

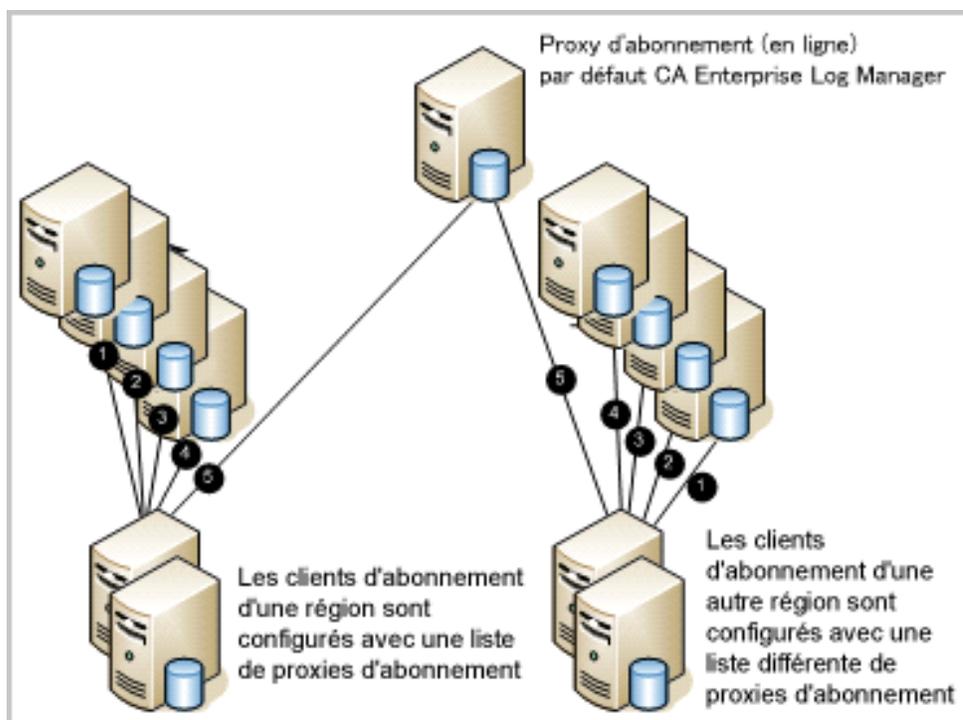
Dans un environnement à serveur unique, le serveur CA Enterprise Log Manager unique est configuré en tant que proxy d'abonnement. Le serveur télécharge et installe automatiquement des mises à jour CA Enterprise Log Manager via le service d'abonnement. Le serveur joue également le rôle de serveur de contenu pour l'environnement.

Dans un environnement de petite taille contenant deux ou plusieurs serveurs, vous pouvez configurer un serveur en tant que proxy d'abonnement et serveur de contenu, tous les autres serveurs étant utilisés comme clients d'abonnement. Vous pouvez choisir le proxy d'abonnement par défaut pour votre environnement, ou sélectionner un autre serveur CA Enterprise Log Manager devant servir de proxy. Le proxy d'abonnement télécharge et installe automatiquement les mises à jour CA Enterprise Log Manager et les clients d'abonnement contactent le proxy pour télécharger leurs mises à jour à tour de rôle. Vous pouvez configurer les clients pour qu'ils téléchargent les mêmes mises à jour que le proxy, ou un sous-ensemble de ce groupe.



Dans un environnement de grande taille contenant plusieurs serveurs, vous pouvez configurer ces serveurs en tant que proxys d'abonnement, chacun fournissant des mises à jour à un groupe limité de clients d'abonnement. Ainsi, le service d'abonnement peut fonctionner efficacement en équilibrant le trafic vers les proxys d'abonnement.

Disposer de plusieurs proxys permet également de configurer des listes de proxys d'abonnement. Grâce à ces listes de proxys, tous les serveurs CA Enterprise Log Manager reçoivent les mises à jour actuelles en temps voulu. Si un proxy spécifique n'est pas disponible lors de la demande de mises à jour CA Enterprise Log Manager par un client, celui-ci contacte chaque proxy figurant sur sa liste de proxys, jusqu'à ce qu'il parvienne à les télécharger. Vous pouvez configurer une liste de proxys globaux pour des mises à jour de client, ainsi que des mises à jour de contenu, pour l'ensemble de votre environnement CA Enterprise Log Manager. Vous pouvez également définir une liste de proxys personnalisée pour des mises à jour de client pour chaque serveur CA Enterprise Log Manager.



Informations complémentaires :

[Planification des mises à jour d'abonnement](#) (page 54)

[Architecture d'abonnement hors ligne](#) (page 59)

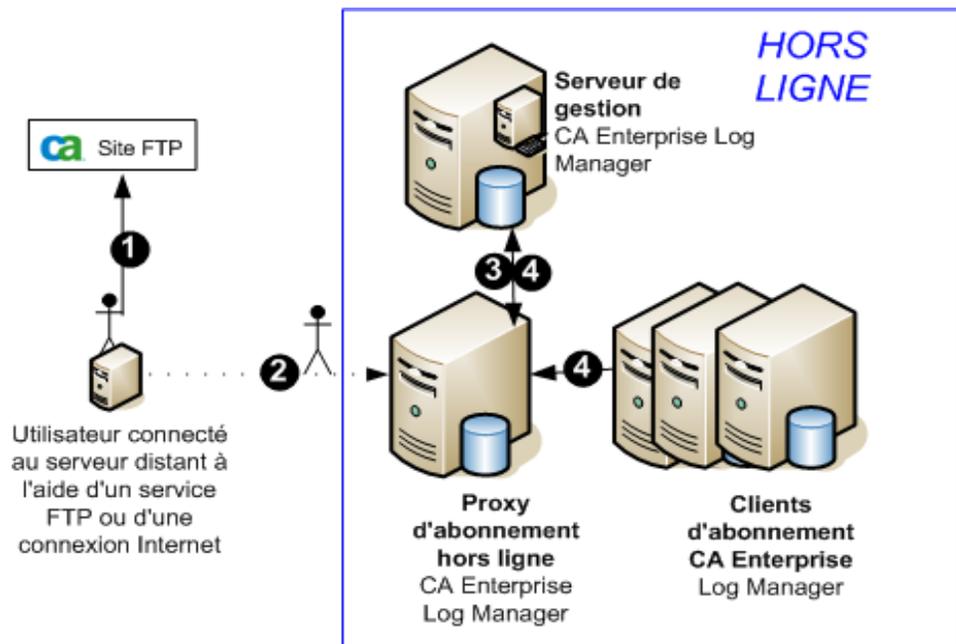
Architecture d'abonnement hors ligne

Si des stratégies de sécurité ou d'autres facteurs limitent l'accès du réseau à Internet, vous pouvez mettre à jour votre environnement CA Enterprise Log Manager via l'abonnement hors ligne. Celui-ci permet d'isoler certains ou l'ensemble de vos serveurs d'Internet, tout en maintenant votre environnement CA Enterprise Log Manager à jour. Il est nécessaire de configurer l'abonnement hors ligne dans les situations suivantes :

- Aucun serveur de votre environnement CA Enterprise Log Manager ne dispose d'accès à Internet.
- Certains serveurs de votre réseau disposent de l'accès à Internet, tandis que d'autres n'ont pas de connexion à un serveur disposant de l'accès à Internet.

La seule différence entre l'abonnement en ligne et hors ligne réside dans le mode de distribution des fichiers de mise à jour au proxy d'abonnement. Dans le cas de l'abonnement en ligne, le proxy contacte le serveur d'abonnement CA via Internet. Dans le cas de l'abonnement hors ligne, vous devez télécharger les mises à jour à partir d'un site FTP CA, puis les copier manuellement sur un serveur CA Enterprise Log Manager configuré en tant que proxy hors ligne.

Le schéma ci-après illustre le processus de l'abonnement hors ligne : Dans cet exemple, l'ensemble de l'environnement CA Enterprise Log Manager se trouve hors ligne.



1. Un administrateur système télécharge les mises à jour à partir d'un site FTP CA vers un système disposant d'un accès Internet FTP.
2. L'administrateur système copie manuellement les fichiers de mise à jour vers un proxy CA Enterprise Log Manager hors ligne. Vous pouvez alors transférer les fichiers à l'aide d'un média physique tel qu'un disque, ou de l'utilitaire scp, inclus dans CA Enterprise Log Manager.
3. La procédure de mise à jour se poursuit de la même manière que pour l'abonnement en ligne. Le proxy hors ligne installe automatiquement les mises à jour et envoie les mises à jour de contenu vers le serveur de gestion.

Remarque : Bien que le proxy hors ligne puisse être configuré de façon à se mettre à jour automatiquement en fonction d'une planification, il est recommandé d'effectuer une mise à jour manuelle lors du transfert de nouveaux fichiers. Ainsi, les mises à jour sont disponibles lorsque les clients d'abonnement en font la demande.

4. Les clients du proxy hors ligne téléchargent les mises à jour, en fonction de la planification définie ou lors d'une mise à jour manuelle.

Remarque : Les clients d'abonnement hors ligne reçoivent toujours toutes les mises à jour qui sont installées manuellement sur le serveur proxy hors ligne. Les modules d'abonnement sélectionnés pour un client d'abonnement hors ligne au niveau local n'ont aucun effet.

L'architecture d'abonnement peut également être mixte. Par exemple, vous pouvez désigner un seul proxy hors ligne et plusieurs autres proxys en ligne. Le proxy hors ligne et les clients qui lui sont affectés demeurent isolés d'Internet, tandis que le reste de l'environnement CA Enterprise Log Manager reçoit des mises à jour via l'abonnement en ligne. En raison de sa complexité, l'architecture mixte n'est pas recommandée. Avant d'implémenter ce type d'architecture, préparez votre stratégie d'abonnement générale avec soin.

Important : Dans un environnement d'abonnement mixte, n'incluez aucun proxy hors ligne dans la liste de proxys des clients d'abonnement en ligne, sans quoi le client d'abonnement en ligne recevra automatiquement toutes les mises à jour manuellement installées, au lieu des modules sélectionnés au niveau global pour votre environnement CA Enterprise Log Manager ou au niveau local pour ce client.

Informations complémentaires :

[Planification des mises à jour d'abonnement](#) (page 54)

[Architecture d'abonnement](#) (page 56)

Exemple : Configuration d'abonnement avec six serveurs

Lorsque vous abordez la configuration de l'abonnement, tenez compte des autres rôles assumés par les serveurs avant de décider de leur rôle d'abonnement. Par défaut, le serveur de gestion, premier serveur installé, est le proxy d'abonnement par défaut. Tous les autres serveurs sont des clients d'abonnement du proxy d'abonnement par défaut. Même si cette situation est acceptable, il est préférable de configurer un proxy d'abonnement en ligne et de laisser le proxy par défaut agir comme proxy de basculement ou proxy redondant. Il est recommandé d'affecter le rôle de proxy en ligne au serveur le moins actif.

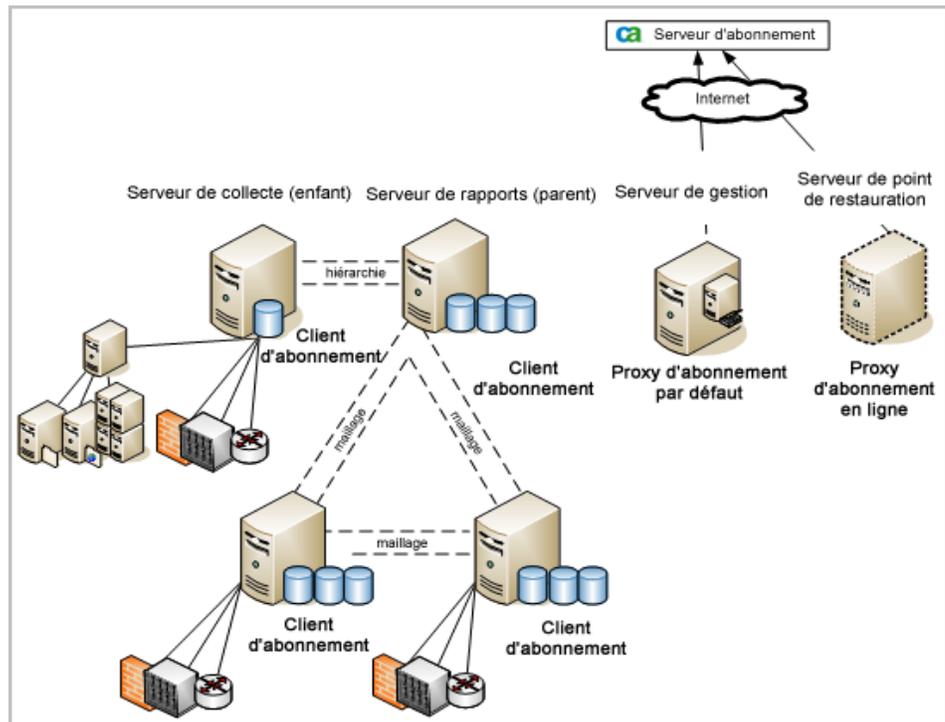
Exemple : Six serveurs parmi lesquels le serveur le moins occupé est le proxy d'abonnement en ligne

Envisagez un scénario comportant six serveurs CA Enterprise Log Manager. Le serveur de gestion est dédié à l'authentification et à l'autorisation des utilisateurs lors de la connexion, ainsi qu'au stockage du contenu d'applications. Quatre serveurs fédérés gèrent le traitement des événements et la génération de rapport. Un sixième serveur constitue un point de restauration dédié pour rechercher des événements provenant de bases de données restaurées. Disposer d'un point de restauration dédié présente un avantage certain : vous pouvez ainsi empêcher l'inclusion d'anciennes données dans les rapports actuels en n'intégrant pas ce serveur dans votre fédération.

Dans cet exemple, le serveur de collecte et le serveur de rapports représentent une configuration dotée d'exigences de traitement exceptionnellement élevées. Ces serveurs sont fédérés dans une configuration hiérarchique, où le serveur de collecte est l'enfant du serveur de rapports. Les deux serveurs agissant tous les deux comme serveurs de collecte et de rapports constituent une configuration dotée de volumes d'événements et de rapports planifiés normaux. Ils sont fédérés entre eux et avec le serveur de rapports dédié dans une fédération maillée : ces trois serveurs sont donc des pairs. Le but de la fédération de serveurs consiste à accroître la possibilité d'obtenir des résultats de requête provenant des serveurs fédérés. Une requête fédérée provenant d'un des serveurs maillés renvoie des événements de ce serveur et des trois autres serveurs de la fédération.

Remarque : Si vous souhaitez exécuter des rapports consolidés sur des événements d'autosurveillance, intégrez le serveur de gestion dans la fédération.

Dans ce scénario, la solution recommandée consiste à configurer le point de restauration sur le proxy d'abonnement en ligne, car c'est le serveur le moins actif. Configurez ensuite chaque client pour qu'il pointe vers ce proxy en ligne, afin que le proxy par défaut agisse comme sauvegarde lorsque le proxy en ligne est occupé ou indisponible.



Informations complémentaires :

[Configuration d'une fédération CA Enterprise Log Manager \(page 235\)](#)

Planification d'agent

Les agents utilisent des connecteurs pour collecter les événements et les acheminer jusqu'au serveur CA Enterprise Log Manager. Vous pouvez configurer un connecteur sur l'agent par défaut installé avec le serveur CA Enterprise Log Manager, mais vous pouvez également installer un agent sur un serveur ou sur une source d'événement de votre réseau. La décision d'utiliser des agents externes dépend du volume d'événements, de l'emplacement des agents, des besoins en filtrage des données et d'autres éléments. La planification de l'installation d'agents implique les éléments ci-dessous.

- Comprendre les relations entre les composants suivants :
 - Intégrations et écouteurs
 - Agents
 - Connecteurs
- Dimensionner votre réseau pour décider du nombre d'agents à installer

Vous devez installer des agents relativement proches des sources d'événement à partir desquelles vous souhaitez collecter des journaux d'événements. La plupart des connecteurs collectent les événements à partir d'une seule et unique source d'événement. Pour les événements Syslog, un seul écouteur Syslog peut recevoir des événements provenant de plusieurs types de sources d'événement. Un agent peut contrôler et gérer le trafic d'événements provenant de plusieurs connecteurs.

A propos de la collecte d'événements Syslog

CA Enterprise Log Manager peut recevoir des événements provenant directement de sources Syslog. La collecte Syslog diffère des autres méthodes de collecte, car plusieurs sources de journaux différentes peuvent envoyer simultanément des événements à CA Enterprise Log Manager. Notez qu'un routeur réseau et un concentrateur VPN sont deux sources d'événement possibles. Ils peuvent tous deux envoyer des événements directement à CA Enterprise Log Manager à l'aide de Syslog, mais les formats et structures des journaux sont différents. Un agent Syslog peut recevoir les deux types d'événements au même moment, à l'aide de l'écouteur Syslog fourni.

En général, la collecte d'événements est composée de deux catégories.

- CA Enterprise Log Manager *écoute* les événements Syslog sur les ports configurables.
- CA Enterprise Log Manager *surveille* les événements d'autres sources à l'aide de WMI par exemple, pour collecter les événements Windows.

Plusieurs sources d'événement Syslog peuvent transmettre des événements par le biais d'un seul connecteur, puisque l'écouteur reçoit l'ensemble du trafic sur un port spécifié. CA Enterprise Log Manager peut écouter les événements Syslog sur n'importe quel port (si vous exécutez un agent en tant qu'utilisateur non root, l'utilisation de ports inférieurs au port 1024 peut faire l'objet de restrictions). Les ports standard peuvent recevoir un flux d'événements composés de différents types d'événements Syslog. Ceux-ci peuvent inclure UNIX, Linux, Snort, Solaris, CiscoPIX, Check Point Firewall 1, etc. CA Enterprise Log Manager gère les événements Syslog à l'aide d'écouteurs, soit un type spécialisé de composant d'intégration. Vous créez des connecteurs Syslog fondés sur des écouteurs et des intégrations.

- L'écouteur fournit les informations de connexion telles que les ports ou les hôtes fiables.
- L'intégration définit les fichiers d'analyse de message (XMP) et de mappage de données.

Comme un seul connecteur Syslog peut recevoir des événements provenant de plusieurs sources d'événement, vous devez envisager d'acheminer ou non les événements Syslog en fonction de leur type ou de leur source. La taille et la complexité de votre environnement déterminent votre manière d'équilibrer la réception de vos événements Syslog.

Plusieurs types Syslog : 1 connecteur

Si un seul connecteur doit traiter des événements provenant de différentes sources Syslog et que le volume d'événements est important, le connecteur doit faire son analyse avec l'ensemble des intégrations (fichiers XMP) appliquées jusqu'à ce qu'il trouve une correspondance pour un événement. Les performances risquent d'être amoindries en raison de l'importance de ce traitement. Toutefois, si le volume d'événements n'est pas trop élevé, un seul connecteur sur l'agent par défaut peut être suffisant pour collecter tous les événements requis pour le stockage.

1 type Syslog : 1 connecteur

Si vous configurez une série de connecteurs uniques pour traiter les événements provenant d'un seul type Syslog, vous pouvez alléger la charge de traitement en la répartissant sur plusieurs connecteurs. Toutefois, si vous avez beaucoup de connecteurs fonctionnant sur un seul agent, vous risquez de perdre en performances, car chaque connecteur est une instance distincte qui nécessite un traitement individuel.

Quelques types Syslog : 1 connecteur

Si votre environnement affiche un volume d'événements plus élevé pour certains types d'événements Syslog, vous pouvez configurer un connecteur pour collecter uniquement ce type d'événements. Vous pouvez ensuite configurer un ou plusieurs autres connecteurs pour collecter plusieurs types d'événements Syslog affichant un volume d'événements moins important dans votre environnement. De ce fait, vous pouvez équilibrer la charge de collecte d'événements Syslog grâce à un petit nombre de connecteurs, gagnant ainsi en performances.

Vous ne devez pas nécessairement créer vos propres écouteurs Syslog, mais vous pouvez le faire le cas échéant. Vous pouvez créer des écouteurs Syslog distincts avec des valeurs par défaut différentes pour les ports, les hôtes fiables, etc. Vous pouvez ainsi simplifier la création des connecteurs, notamment si vous devez créer plusieurs connecteurs pour chaque type d'événement Syslog.

Informations complémentaires :

[Comptes d'utilisateur par défaut](#) (page 109)

[Redirection des ports du pare-feu pour les événements Syslog](#) (page 116)

Les agents et le certificat d'agent

Le certificat CAELM_AgentCert.cer prédéfini est utilisé par tous les agents pour communiquer avec leur serveur CA Enterprise Log Manager.

Si vous choisissez de remplacer ce certificat par un certificat personnalisé, nous vous conseillons de le faire avant d'installer des agents. Si vous implémentez un certificat personnalisé après l'installation et l'enregistrement des agents sur un serveur CA Enterprise Log Manager, vous devez désinstaller chaque agent, supprimer l'entrée de l'agent dans l'Explorateur d'agent, réinstallez l'agent et reconfigurez les connecteurs.

A propos des agents

Après installation, les agents fonctionnent comme un service ou un démon et ce sont des composants de produit facultatifs, utilisés dans une ou plusieurs des situations énumérées ci-dessous.

- Un petit site distant doit collecter des données d'événement, mais il n'a pas besoin d'un dispositif logiciel CA Enterprise Log Manager complet.
- Vous devez filtrer les données à la source des événements, pour réduire le trafic réseau ou la quantité de données stockées.
- Vous devez assurer la remise d'événement vers le magasin de journaux d'événements pour des raisons de conformité.
- Vous devez sécuriser la transmission des journaux sur le réseau grâce au chiffrement des données.

Les agents agissent comme des gestionnaires de processus pour les connecteurs qui collectent des données d'événement provenant d'applications, de systèmes d'exploitation ou de bases de données spécifiques. Les agents disposent de commandes de gestion de connecteur telles que Démarrer, Arrêter et Redémarrer, à partir de l'interface de l'Explorateur d'agent dans CA Enterprise Log Manager. Les agents appliquent également les modifications de configuration des connecteurs et les mises à jour des fichiers binaires.

Vous pouvez installer des agents sur des sources individuelles d'événement, mais aussi sur des serveurs hôtes distants, pour collecter des événements provenant de plusieurs sources. L'installation du serveur CA Enterprise Log Manager installe automatiquement son propre agent. Vous pouvez utiliser cet agent par défaut pour la collecte directe des événements Syslog.

Vous pouvez également afficher l'état d'un agent dans l'Explorateur d'agent sur n'importe quel serveur CA Enterprise Log Manager du réseau. Les agents sont dotés d'un service de surveillance qui redémarre l'agent, si ce dernier s'arrête inopinément, et qui surveille les mises à jour des fichiers binaires des agents et connecteurs. Les agents envoient également des événements d'autosurveillance au magasin de journaux d'événements, pour le suivi des modifications et de l'état.

A propos des groupes d'agents

Vous pouvez également créer des groupes d'agents, qui constituent des regroupements logiques d'agents afin de faciliter la gestion de ces derniers. Après avoir intégré un agent dans un groupe d'agents, vous pouvez modifier les configurations, mais aussi démarrer et arrêter simultanément tous les connecteurs. Par exemple, vous pouvez décider de regrouper les agents par région géographique réelle.

Vous pouvez créer des groupes et déplacer les agents dans ces groupes grâce à l'Explorateur d'agent. Si aucun groupe d'agents n'est défini, tous les agents se retrouvent dans un groupe par défaut, créé lors de l'installation de CA Enterprise Log Manager.

Les configurations d'agents et les enregistrements de groupes d'agents sont stockés sur le serveur de gestion. A chaque nouvelle installation d'agent, le serveur de gestion rend cet agent disponible dans l'Explorateur d'agent pour tous les serveurs CA Enterprise Log Manager auprès desquels il est enregistré sous le même nom d'instance d'application. Vous pouvez ainsi configurer et contrôler tous les agents depuis n'importe quel serveur CA Enterprise Log Manager sur le réseau.

Droits des comptes d'utilisateur des agents

Les agents peuvent fonctionner avec des comptes d'utilisateur avec peu de droits. Vous devez créer un compte d'utilisateur du groupe et du service sur l'hôte cible avant d'installer un agent. Vous spécifiez le nom d'utilisateur au cours de l'installation de l'agent et le programme d'installation définit les droits en conséquence. Pour les systèmes Linux, l'utilisateur de l'agent possède tous les fichiers binaires de l'agent, à l'exception du fichier binaire de surveillance, propriété de l'utilisateur root.

A propos des intégrations

L'ensemble des intégrations prêtes à l'emploi est, pour l'essentiel, une bibliothèque de modèles. Ces modèles fournissent le code spécifique à la collecte d'événements provenant d'un type précis de source de journaux. Une intégration devient un connecteur lorsqu'elle est choisie dans la bibliothèque et configurée avant d'être appliquée à une source d'événement. Les intégrations contiennent les types d'informations ci-dessous.

- Fichier d'accès aux données, avec les informations liées à un type précis de source d'événement

- Fichier d'analyse de message, qui crée des paires nom-valeur à partir des journaux d'événements collectés
- Fichier de mappage de données, qui mappe les paires nom-valeur analysées vers la grammaire commune aux événements, qui forme le schéma de base de données pour le magasin de journaux d'événements du serveur CA Enterprise Log Manager

CA Enterprise Log Manager propose diverses intégrations pour les sources d'événement courantes et communes, notamment les produits CA, mais aussi les pare-feu, bases de données, systèmes d'exploitation, applications, etc., courants. Vous pouvez obtenir d'autres intégrations comme indiqué ci-après.

- Les mises à jour d'abonnement incluent de nouvelles intégrations ou de nouvelles versions d'intégrations existantes.
- L'assistant fourni permet de créer des intégrations personnalisées.

Vous utilisez les intégrations pour préciser le type de collecte d'événements à effectuer lorsque vous configurez des connecteurs.

A propos des connecteurs

Les connecteurs écoutent les événements, mais ils envoient aussi des événements d'état à l'agent de manière périodique, pour les transmettre au serveur CA Enterprise Log Manager. Un *connecteur* est un processus qui utilise un détecteur de journaux et une intégration pour créer une configuration permettant de collecter des événements provenant d'une source d'événement spécifique. Sauf pour Syslog, un connecteur utilise une intégration comme modèle de configuration. Les connecteurs Syslog reposent sur des écouteurs.

Les agents utilisent des connecteurs pour collecter les événements. Après avoir installé un agent, vous pouvez utiliser l'Explorateur d'agent sur n'importe quel serveur CA Enterprise Log Manager pour configurer un ou plusieurs connecteurs sur cet agent. Les serveurs CA Enterprise Log Manager doivent être enregistrés auprès du même serveur de gestion (ou du même serveur CA EEM externe), avec le même nom d'instance d'application, pour configurer des agents de cette façon.

Remarque : Bien qu'en théorie il soit possible de configurer jusqu'à 256 connecteurs sur un agent spécifique, un nombre élevé de connecteurs entraîne une baisse des performances. Nous recommandons de configurer 70 connecteurs maximum par agent pour obtenir des performances optimales.

En général, chaque source d'événement sur le réseau est dotée d'un connecteur. Pour les événements Syslog, un connecteur peut être lié à plusieurs sources d'événement, en fonction de vos choix de configuration. Vous pouvez créer plusieurs connecteurs utilisant la même intégration, mais dotés de détails de configuration légèrement différents, pour accéder à des sources d'événement différentes. Certains connecteurs proposent des aides à la configuration, qui collectent les informations nécessaires pour accéder à la source d'événement. Si vous avez besoin d'un connecteur pour lequel aucune intégration n'est actuellement proposée, vous pouvez créer une intégration à l'aide de l'Assistant d'intégration.

A propos des détecteurs de journaux

Un *détecteur de journaux* est le composant, dans un connecteur, qui sait comment accéder aux sources d'événement. CA Enterprise Log Manager fournit des détecteurs de journaux pour les différents types de sources d'événement et de formats de journaux répertoriés ci-dessous.

ACLogSensor

Ce détecteur de journaux lit les événements CA Access Control lorsque celui-ci utilise selogrd pour le routage d'événements.

FileLogSensor

Ce détecteur de journaux lit les événements à partir d'un fichier.

LocalSyslog

Ce détecteur de journaux collecte les événements à partir des fichiers Syslog local d'un serveur UNIX.

ODBCLogSensor

Ce détecteur de journaux utilise ODBC pour se connecter à une source d'événement de base de données et récupérer des événements à partir de celle-ci.

OPSELogSensor

Ce détecteur de journaux lit les événements à partir d'une source d'événement OPSEC Check Point.

SDEELogSensor

Ce détecteur de journaux lit les événements à partir des périphériques Cisco.

Syslog

Ce détecteur de journaux écoute les événements Syslog.

TIBCOLogSensor

Ce détecteur de journaux lit les événements à partir d'une file d'attente du service de message d'événements (EMS) TIBCO dans les implémentations CA Access Control.

W3CLogSensor

Ce détecteur de journaux lit les événements à partir d'un fichier de format de journaux W3C.

WinRMLinuxLogSensor

Ce détecteur de journaux active l'agent (Linux) par défaut sur le serveur CA Enterprise Log Manager pour collecter les événements Windows.

WMILogSensor

Ce détecteur de journaux collecte les événements provenant de sources d'événement Windows à l'aide de l'infrastructure de gestion Windows (WMI).

Vous pouvez disposer d'autres détecteurs de journaux grâce aux mises à jour d'abonnement. Vous trouverez plus d'informations sur la configuration des détecteurs de journaux dans l'aide en ligne et dans le *Manuel d'administration*.

Dimensionnement de votre réseau CA Enterprise Log Manager

Lors de la planification du nombre d'agents nécessaires, envisagez d'utiliser un schéma de dimensionnement simple, comme celui évoqué ci-après. Tout d'abord, déterminez le nombre de connecteurs nécessaires. Vous n'avez pas besoin d'installer un agent sur chaque source d'événement. Toutefois, vous devez configurer un connecteur pour chaque source d'événement non Syslog à partir de laquelle vous envisagez de collecter des événements. Vous pouvez collecter des événements WMI sur un seul connecteur à partir de plusieurs sources d'événement en ajoutant un détecteur de journaux à chaque source d'événement. Pensez à regrouper les volumes d'événements lorsque vous configurez un connecteur de cette manière.

Vous pouvez configurer des connecteurs Syslog de diverses manières. Vous pouvez par exemple configurer un seul connecteur Syslog pour recevoir tous les événements Syslog, quel que soit leur type. Il est toutefois recommandé de fonder vos connecteurs Syslog sur les volumes d'événements provenant de sources d'événements Syslog spécifiques.

Vous pouvez installer des agents sur chaque source d'événement. Nous recommandons cette approche lorsque le nombre d'événements provenant de cette source est élevé. Votre planification doit différencier les agents d'une source d'événement des agents d'un hôte agissant en tant que collecteur de différents types d'événements.

Effets des règles de suppression

Pendant la phase de planification, réfléchissez à l'utilisation de *règles de suppression*, qui empêchent certains événements d'être insérés dans le magasin de journaux d'événements ou d'être collectés par un connecteur. Les règles de suppression sont toujours liées à un connecteur. Vous pouvez appliquer des règles de suppression au niveau de l'agent ou du groupe, ou encore au niveau du serveur CA Enterprise Log Manager lui-même. L'effet obtenu change en fonction de l'emplacement choisi.

- Les règles de suppression appliquées au niveau de l'agent ou du groupe empêchent les événements d'être collectés et réduisent ainsi le volume de trafic réseau *envoyé* au serveur CA Enterprise Log Manager.
- Les règles de suppression appliquées au niveau du serveur CA Enterprise Log Manager empêchent les événements d'être *insérés* dans la base de données et réduisent ainsi le volume d'informations stockées.

Appliquer des règles de suppression à des événements après leur arrivée sur le serveur CA Enterprise Log Manager peut avoir des effets sur les performances, surtout si vous créez plusieurs règles de suppression ou si le flux d'événements est élevé.

Par exemple, imaginons que vous souhaitiez supprimer *certaines* des événements issus d'un pare-feu ou de serveurs Windows qui génèrent des événements dupliqués pour la même action. La non-collecte de ces événements peut accélérer le transport des journaux d'événements que vous souhaitez conserver et permet d'économiser le temps de traitement sur le serveur CA Enterprise Log Manager. Dans ce cas, vous pouvez appliquer une ou plusieurs règles de suppression appropriées sur les composants d'agents.

Si vous souhaitez supprimer tous les événements d'un type donné, issus de diverses plates-formes ou de l'ensemble de votre environnement, appliquez une ou plusieurs règles de suppression appropriées au niveau du serveur CA Enterprise Log Manager. La nécessité de supprimer les événements est évaluée à leur arrivée sur le serveur CA Enterprise Log Manager. Appliquer un grand nombre de règles de suppression au niveau du serveur peut ralentir les performances, étant donné que l'application des règles de suppression s'ajoute à l'insertion des événements dans le magasin de journaux d'événements sur le serveur.

Dans le cas d'implémentations moins importants, la suppression peut être réalisée sur le serveur CA Enterprise Log Manager. Vous pouvez également choisir d'appliquer la suppression au niveau du serveur dans les déploiements utilisant la récapitulation (agrégation). En revanche, si vous insérez uniquement certains des événements issus d'une source d'événement générant des volumes importants d'informations d'événement, vous pouvez choisir de supprimer les événements indésirables au niveau de l'agent ou du groupe d'agents, pour économiser du temps de traitement sur le serveur CA Enterprise Log Manager.

Chapitre 3 : Installation de CA Enterprise Log Manager

Ce chapitre traite des sujets suivants :

[Présentation de l'environnement CA Enterprise Log Manager](#) (page 73)

[Création des DVD d'installation](#) (page 75)

[Installation d'un serveur CA Enterprise Log Manager](#) (page 76)

[Mise à niveau des serveurs et des agents CA Enterprise Log Manager existants pour la prise en charge de la norme FIPS](#) (page 89)

[Ajout de serveurs CA Enterprise Log Manager à une fédération en mode FIPS existante](#) (page 98)

[Remarques concernant l'installation d'un système disposant de lecteurs SAN](#) (page 100)

[Configurations initiales du serveur CA Enterprise Log Manager](#) (page 108)

[Installation du client ODBC](#) (page 117)

[Installation du client JDBC](#) (page 123)

[Dépannage de l'installation](#) (page 127)

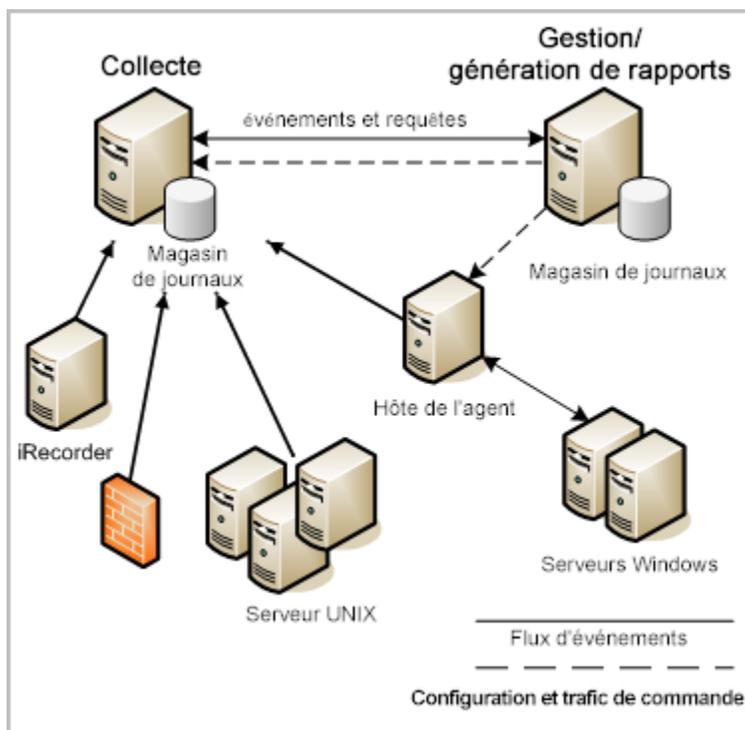
Présentation de l'environnement CA Enterprise Log Manager

CA Enterprise Log Manager est conçu pour s'installer et fonctionner rapidement entre le début de l'installation et le moment où le produit collecte des informations de journaux et génère des rapports. Vous devez installer le dispositif logiciel CA Enterprise Log Manager sur un système dédié.

Important : Comme le serveur CA Enterprise Log Manager est dédié à la collecte hautes performances de journaux d'événements, vous ne devez pas installer d'autres applications sur le serveur l'hébergeant. Sans quoi vous risquez un effet négatif sur les performances.

Vous disposez de nombreuses façons de configurer votre environnement. Nous vous recommandons la configuration spécifique qui suit, afin de garantir la gestion de volumes élevés d'événements dans les environnements d'entreprise.

Pour un environnement de production de base au niveau de l'entreprise, installez au moins deux serveurs CA Enterprise Log Manager sur votre réseau existant. Les serveurs CA Enterprise Log Manager utilisent les serveurs DNS existants de votre réseau pour travailler avec des sources d'événement et des hôtes de l'agent nommés. Un serveur se concentre sur la collecte et l'autre sur les rapports de journaux des événements collectés. Dans un environnement avec deux serveurs, le serveur de gestion installé en premier assume le rôle de serveur de rapports. En tant que serveur de gestion, il effectue l'authentification et l'autorisation des utilisateurs, ainsi que d'autres fonctions de gestion. L'illustration ci-dessous présente cet environnement de base avec certaines sources d'événement.



Sur ce diagramme, les lignes pleines représentent le flux d'événements depuis les sources d'événement vers le serveur de collecte ou depuis un hôte d'agent vers le serveur de collecte. Vous pouvez collecter directement des événements Syslog grâce à l'agent par défaut sur le serveur CA Enterprise Log Manager de collecte. Vous pouvez également configurer un ou plusieurs connecteurs sur un hôte d'agent distinct pour collecter des événements provenant de plusieurs sources Syslog (non illustré sur ce diagramme).

La collecte d'événements Windows utilise l'infrastructure de gestion Windows (WMI) pour surveiller les serveurs Windows et leurs événements. Cela implique que vous configuriez un connecteur WMI sur un agent installé sur un hôte Windows comme point de collecte d'événements. Pour certains autres types d'événements, vous pouvez décider d'utiliser un iRecorder CA autonome sur un serveur hôte.

Vous pouvez configurer et gérer les agents et les connecteurs de ces sources d'événement depuis n'importe quel serveur CA Enterprise Log Manager sur le réseau. Sur le diagramme, les lignes pointillées représentent le trafic de configuration et de contrôle entre le serveur et les agents de gestion d'une part, et chacun des autres serveurs CA Enterprise Log Manager d'autres part. Dans l'environnement représenté sur ce diagramme, vous effectuez des configurations à partir du serveur de gestion. Cela permet au serveur de collecte de se concentrer sur le traitement des événements.

L'environnement de collecte de journaux dans lequel vous installez des serveurs CA Enterprise Log Manager dispose des caractéristiques énumérées ci-dessous.

- Le serveur CA Enterprise Log Manager de gestion traite l'authentification et l'autorisation des utilisateurs ainsi que la gestion des configurations de tous les serveurs, agents et connecteurs CA Enterprise Log Manager sur votre réseau à l'aide de son serveur CA EEM local.

En fonction de la taille de votre réseau et de son volume d'événements, vous pouvez choisir d'installer plusieurs serveurs de gestion et de créer des fédérations de serveurs de collecte pour chaque serveur. Vous pouvez également dédier plusieurs serveurs aux rapports, lorsque tous les serveurs de rapports s'enregistrent auprès de votre unique serveur de gestion. Dans ce scénario, le flux d'événements passe des sources d'événement au serveur de collecte configuré, puis au serveur de rapports configuré.

- Un ou plusieurs serveurs CA Enterprise Log Manager de collecte traitent et stockent les événements entrants.
- Les événements circulent sur votre réseau de collecte de journaux depuis différentes sources d'événement *après* la configuration des connecteurs et adaptateurs correspondants.

Création des DVD d'installation

Le logiciel CA Enterprise Log Manager est disponible sous forme d'images ISO compressées et téléchargeables. Après avoir téléchargé le logiciel, vous devez créer des DVD avant de pouvoir l'installer. Utilisez la procédure suivante pour télécharger les images ISO et créer les disques d'installation.

Pour créer les DVD d'installation

1. A partir d'un ordinateur connecté à Internet, accédez au serveur de téléchargement, à l'adresse <http://ca.com/support> (en anglais).
2. Cliquez sur le lien Technical Support, puis sur le lien Download Center.
3. Choisissez CA Enterprise Log Manager dans le champ Select a Product, puis choisissez la version dans le champ Select a Release.
4. Sélectionnez la case à cocher Select all components, puis cliquez sur Go.
La page Published Solutions Downloads s'affiche.
5. Sélectionnez le package de téléchargement.
La page de la documentation des solutions s'affiche.
6. Utilisez le défilement pour accéder au bas de la page et sélectionnez le lien Download, en regard du nom du package.
Le téléchargement du package démarre.

Remarque : Le téléchargement peut durer un certain temps, en fonction du débit de votre connexion.

7. Décompressez les deux images d'installation.
8. Créez deux disques d'installation distincts en gravant les images disque ISO du système d'exploitation et de CA Enterprise Log Manager sur des DVD-RW séparés.

Les deux disques d'installation contiennent respectivement tous les composants du système d'exploitation et du produit pour votre environnement CA Enterprise Log Manager. Vous pouvez décider d'utiliser d'autres composants, comme des SAPI Records ou des iRecords, dans votre environnement. Il s'agit de téléchargements distincts, disponibles sur le site Web du support CA.

9. Utilisez les disques que vous venez de créer pour les installations.

Installation d'un serveur CA Enterprise Log Manager

Ce processus d'installation comprend les étapes suivantes.

- Remplissez la feuille de calcul du serveur CA Enterprise Log Manager.
- Installez le serveur de gestion CA Enterprise Log Manager.

Remarque : Si vous utilisez un stockage SAN, veillez à ne pas effectuer d'installation sur un lecteur SAN.

- Installez un ou plusieurs serveurs de collecte CA Enterprise Log Manager.
- Installez un ou plusieurs serveurs de rapports (facultatif).

Remarque : Si vous n'installez pas un serveur dédié à la génération de rapport, vous pouvez utiliser le serveur de gestion pour ce rôle.

- Installez un serveur de point de restauration (facultatif).
- Vérifiez l'installation.
- Affichez les événements d'autosurveillance.

Important : Configurez vos disques de stockage dans une baie RAID *avant* de commencer l'installation de CA Enterprise Log Manager. Configurez les deux premiers disques comme la baie RAID 1 et définissez-la comme la baie de démarrage. Configurez les disques restants comme une seule baie RAID 5. Si vous ne configurez pas la baie RAID, vous risquez de perdre des données.

Pour la sécurité générale du serveur CA Enterprise Log Manager lui-même, lors de l'installation, l'utilitaire Grand Unified Boot-loader (GRUB) est protégé par un mot de passe.

Feuille de calcul du serveur CA Enterprise Log Manager

Avant d'installer un serveur CA Enterprise Log Manager, collectez les informations de la table ci-dessous. Une fois la feuille de calcul renseignée, vous pouvez l'utiliser lors de votre travail, pour répondre aux invites de l'installation. Vous pouvez imprimer et renseigner une feuille de calcul distincte pour chaque serveur CA Enterprise Log Manager que vous envisagez d'installer.

Informations CA Enterprise Log Manager	Valeur	Commentaires
Disque du SE		
Type de clavier	<i>valeur adéquate</i>	Spécifiez le type de clavier que vous souhaitez utiliser grâce à son paramètre de langue. La valeur par défaut utilise les paramètres matériels du clavier connecté au serveur lorsque ce dernier démarre.
Sélection du fuseau horaire	<i>le fuseau horaire que vous souhaitez</i>	Sélectionnez le fuseau horaire dont dépend ce serveur.

Informations CA Enterprise Log Manager	Valeur	Commentaires
Mot passe root	<i>nouveau mot de passe root</i>	Créez et confirmez un nouveau mot de passe root pour ce serveur.
Disque de l'application		
Nouveau nom d'hôte	<i>nom d'hôte de ce serveur CA Enterprise Log Manager</i> Exemple : CA-ELM1	Spécifiez le nom d'hôte de ce serveur en utilisant uniquement les caractères pris en charge par les hôtes. Les normes du secteur recommandent les lettres de A à Z (insensibles à la casse), les chiffres de 0 à 9 et le tiret, avec une lettre en premier caractère et un caractère alphanumérique en dernière position. N'utilisez pas le caractère de soulignement dans un nom d'hôte. Remarque : N'ajoutez pas de nom de domaine à cette valeur de nom d'hôte.
Sélection d'une unité	<i>Nom de l'unité</i>	Sélectionnez le nom de l'adaptateur réseau à utiliser pour les collectes de journaux d'événements et les communications. Appuyez sur la barre d'espace pour entrer la configuration d'une unité.
Adresse IP, masque de sous-réseau et passerelle par défaut	<i>valeurs IP correspondantes</i>	Entrez une adresse IP valide pour ce serveur. Entrez un masque de sous-réseau valide et une passerelle par défaut à utiliser avec ce serveur.

Informations CA Enterprise Log Manager	Valeur	Commentaires
Nom de domaine	<i>votre nom de domaine</i>	Entrez le nom de domaine complet au sein duquel opère le serveur, par exemple mycompany.com. Remarque : Le nom de domaine doit être enregistré auprès du serveur DNS (Domain Name Server) de votre réseau pour permettre la résolution du nom d'hôte vers l'adresse IP.
Liste des serveurs DNS	<i>adresses IPv4 ou IPv6 correspondantes</i>	Entrez une ou plusieurs adresses IP de serveur DNS à utiliser sur votre réseau. La liste est séparée par des virgules, sans espace entre les entrées. Si vos serveurs DNS utilisent l'adressage IPv6, entrez ces adresses avec ce format.
Date et heure système	<i>date et heure locales</i>	Entrez de nouvelles date et heure système, le cas échéant.
Mise à jour de l'heure via NTP ?	Oui (recommandé) ou Non	Indiquez si vous souhaitez configurer le serveur CA Enterprise Log Manager pour qu'il mette à jour ses date et heure à partir d'un serveur NTP (Network Time Protocol) établi. Remarque : La synchronisation de l'heure permet de vous assurer que les alertes contiennent des données complètes.
Nom ou adresse du serveur NTP	<i>nom d'hôte ou adresse IP correspondant</i>	Entrez le nom d'hôte ou l'adresse IP valide du serveur NTP auprès duquel ce serveur CA Enterprise Log Manager obtient des informations de date et d'heure.

Informations CA Enterprise Log Manager	Valeur	Commentaires
Contrat de licence du kit de développement Sun Java (JDK)	Oui	Lisez le contrat de licence, en parcourant les pages jusqu'à atteindre la question Acceptez-vous les termes du contrat de licence ci-dessus ? [oui ou non].
Contrat de licence CA	Oui	Lisez le contrat de licence, en parcourant les pages jusqu'à atteindre la question Acceptez-vous les termes du contrat de licence ci-dessus ? [oui ou non].
Serveur CA Embedded Entitlements Manager local ou distant ?	Local pour le premier serveur installé (serveur de gestion) Distant pour chaque serveur supplémentaire	Indiquez si vous prévoyez d'utiliser un serveur CA EEM local ou distant. Pour un serveur CA Enterprise Log Manager de gestion, choisissez l'option locale. L'installation vous invite à créer un mot de passe pour le compte d'utilisateur EiamAdmin par défaut. Pour chaque serveur supplémentaire, choisissez l'option distante. L'installation vous invite à indiquer le nom du serveur de gestion. Que vous choisissiez l'option locale ou distante, vous devez utiliser l'ID et le mot de passe du compte EiamAdmin lors de votre première connexion à <i>chaque</i> serveur CA Enterprise Log Manager.

Informations CA Enterprise Log Manager	Valeur	Commentaires
Entrer le nom du serveur CA EEM	<i>adresse IP ou nom d'hôte</i>	<p>Cette invite s'affiche uniquement si vous sélectionnez l'option distante dans l'invite du serveur local ou distant.</p> <p>Entrez l'adresse IP ou le nom d'hôte du serveur CA Enterprise Log Manager de gestion installé en premier.</p> <p>Le nom d'hôte doit être enregistré auprès du serveur DNS.</p>
Mot de passe de l'administrateur du serveur CA EEM	<i>mot de passe du compte EiamAdmin</i>	<p>Enregistrez le mot de passe du compte d'administrateur par défaut, EiamAdmin.</p> <p>Votre serveur CA Enterprise Log Manager <i>doit</i> disposer de ces informations d'identification de compte pour la connexion initiale.</p> <p>Si vous installez le serveur de gestion, vous créez et confirmez ici un nouveau mot de passe EiamAdmin.</p> <p>Notez ce mot de passe, car vous l'utiliserez à nouveau lors des installations d'autres serveurs et agents CA Enterprise Log Manager.</p> <p>Remarque : Le mot de passe entré ici est également le mot de passe initial du compte caelmadmin par défaut, que vous utiliserez pour accéder directement au serveur CA Enterprise Log Manager via ssh.</p> <p>Si vous le souhaitez, vous pouvez créer d'autres comptes d'administrateur pour accéder aux fonctions CA EEM après l'installation.</p>

Informations CA Enterprise Log Manager	Valeur	Commentaires
Nom d'instance d'application	CAELM	<p>Lorsque vous installez le premier serveur CA Enterprise Log Manager sur votre réseau, vous créez une valeur d'instance d'application dans cette invite.</p> <p>Les autres serveurs CA Enterprise Log Manager utilisent cette valeur pour s'enregistrer auprès du serveur de gestion.</p> <p>Le nom d'instance d'application par défaut est CAELM.</p> <p>Vous pouvez utiliser n'importe quel nom pour cette valeur. Notez ce nom d'instance d'application pour l'utiliser lors d'installations ultérieures de CA Enterprise Log Manager.</p>
Voulez-vous exécuter le serveur CA ELM en mode FIPS ?	Oui ou non	<p>La réponse à cette question indiquera si le serveur CA Enterprise Log Manager sera démarré en mode FIPS.</p> <p>Remarque : Si vous ajoutez un serveur à déploiement de CA Enterprise Log Manager existant, activez également le mode FIPS pour le serveur de gestion CA Enterprise Log Manager ou le serveur CA EEM distant. Dans le cas contraire, vous ne pourrez pas enregistrer le nouveau serveur et vous devrez le réinstaller.</p>

Remarque : L'installation vous permet d'examiner et de modifier les détails du serveur CA EEM avant qu'il ne tente de se connecter.

Si le programme d'installation est incapable de se connecter au serveur de gestion spécifié et que vous décidez de poursuivre l'installation, vous pouvez enregistrer manuellement le serveur CA Enterprise Log Manager avec la fonctionnalité CA EEM intégrée. Dans ce cas, vous devez également importer manuellement les fichiers de contenu, CEG et de gestion des agents. Reportez-vous à la section traitant du dépannage de l'installation pour plus d'informations et d'instructions.

Informations complémentaires :

[Enregistrement du serveur CA Enterprise Log Manager auprès du serveur CA EEM](#) (page 130)

[Acquisition de certificats auprès du serveur CA EEM](#) (page 131)

[Importation de rapports CA Enterprise Log Manager](#) (page 132)

[Importation de fichiers de mappage de données CA Enterprise Log Manager](#) (page 133)

[Importation de fichiers de grammaire commune aux événements](#) (page 133)

[Importation de fichiers de gestion commune des agents](#) (page 135)

Installation de CA Enterprise Log Manager

Utilisez la procédure suivante pour installer un serveur CA Enterprise Log Manager.

Pour installer le logiciel CA Enterprise Log Manager

1. Démarrez le serveur avec le DVD d'installation du SE.
L'installation du système d'exploitation démarre automatiquement.
2. Répondez aux invites à l'aide des informations collectées dans la feuille de calcul du serveur CA Enterprise Log Manager.
Tout refus du contrat de licence interrompt l'installation et arrête le serveur.
3. Répondez à l'invite de redémarrage en retirant le média avant de cliquer sur Redémarrer.
4. A l'invite, insérez le disque de l'application CA Enterprise Log Manager et cliquez sur Entrée.

5. Répondez aux invites à l'aide des informations collectées dans la feuille de calcul.

L'installation se poursuit. Lorsque le message "Installation de CA Enterprise Log Manager terminée." s'affiche, l'installation est terminée.

Remarque : Lorsque vous installez un autre serveur CA Enterprise Log Manager, il se peut que vous remarquiez, dans le journal d'installation, un message d'erreur indiquant que le nom de l'application que l'installation a tenté d'enregistrer auprès du serveur CA EEM existe déjà. Vous pouvez sans risque ignorer cette erreur, car chaque installation de CA Enterprise Log Manager tente de créer le nom de l'application comme s'il s'agissait d'une nouvelle application.

Une fois l'installation terminée, vous devez configurer votre serveur CA Enterprise Log Manager avant de pouvoir recevoir des événements. Cela peut inclure la configuration d'un connecteur sur l'agent par défaut pour recevoir les événements Syslog.

Informations complémentaires :

[Dépannage de l'installation](#) (page 127)

[Configuration de l'agent par défaut](#) (page 213)

Vérifier que le processus iGateway s'exécute

Si vous ne parvenez pas à accéder à l'interface Web du serveur CA Enterprise Log Manager après l'installation et que vous êtes sûr que les ports de l'interface réseau sont correctement configurés, il se peut que le processus iGateway ne s'exécute pas.

Vous pouvez effectuer un contrôle rapide de l'état du processus iGateway à l'aide de la procédure qui suit. Le processus iGateway doit être en cours d'exécution pour que le serveur CA Enterprise Log Manager collecte les événements et pour que l'interface utilisateur soit accessible.

Pour vérifier le démon iGateway

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su - root
```

4. Utilisez la commande ci-après 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.

Informations complémentaires :

[Résoudre une erreur de configuration de l'interface réseau](#) (page 129)

Démarrage du démon ou service iGateway

Le démon ou service iGateway est le processus qui gère tous les appels adressés à l'interface utilisateur pour CA EEM et pour CA Enterprise Log Manager. Ce processus doit être en cours d'exécution pour que vous puissiez accéder à l'une ou l'autre de ces applications. Utilisez la procédure suivante pour démarrer le processus iGateway s'il ne fonctionne pas déjà.

Remarque : Si vous ne parvenez pas à démarrer iGateway, vérifiez que le dossier "/" contient suffisamment d'espace libre. Un espace disque trop faible empêche le démarrage d'iGateway.

Pour démarrer le démon ou service iGateway

1. Connectez-vous en tant qu'utilisateur caelmadmin pour le serveur CA Enterprise Log Manager.
2. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

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

```
$IGW_LOC/S99igateway start
```

S99igateway est le script de démarrage du processus iGateway et il appartient au compte root. Lorsque le processus iGateway démarre, il s'exécute sous le compte d'utilisateur caelmservice.

Arrêt du démon ou service iGateway

Le démon ou service iGateway est le processus qui gère tous les appels adressés à l'interface utilisateur pour CA EEM et pour CA Enterprise Log Manager. Ce processus doit être en cours d'exécution pour que vous puissiez accéder à l'une ou l'autre de ces applications. Utilisez la procédure suivante pour arrêter le processus iGateway. Vous pouvez agir ainsi pour vous préparer à redémarrer le processus ou lors du retrait d'un serveur CA Enterprise Log Manager du réseau.

Pour arrêter le démon ou service iGateway

1. Connectez-vous en tant qu'utilisateur caelmadmin pour le serveur CA Enterprise Log Manager.
2. Passez à l'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
```

S99igateway est le script d'arrêt du processus iGateway et il appartient au compte root. Lorsque le processus iGateway démarre, il s'exécute sous le compte d'utilisateur caelmservice.

Démarrage du démon ou service de l'agent CA Enterprise Log Manager

Le démon ou service de l'agent CA Enterprise Log Manager est le processus qui gère les connecteurs envoyant les événements collectés à un serveur CA Enterprise Log Manager. Ce processus doit être en cours d'exécution pour que les connecteurs puissent collecter des événements. Utilisez la procédure suivante pour démarrer le processus de l'agent CA Enterprise Log Manager s'il ne fonctionne pas déjà.

Pour démarrer le démon ou service de l'agent CA ELM

1. Connectez-vous en tant qu'utilisateur root ou administrateur Windows.
2. Accédez à une invite de commande, puis entrez la commande ci-après.

```
Linux, UNIX, Solaris : /opt/CA/ELMAgent/bin/S99elmagent start
```

```
Windows : net start ca-elmagent
```

Arrêt du démon ou service de l'agent CA Enterprise Log Manager

Le démon ou service de l'agent CA Enterprise Log Manager est le processus qui gère les connecteurs envoyant les événements collectés à un serveur CA Enterprise Log Manager. Ce processus doit être en cours d'exécution pour que les connecteurs puissent collecter des événements. Utilisez la procédure suivante pour arrêter le processus de l'agent CA Enterprise Log Manager. Normalement, les commandes de démarrage et d'arrêt sont émises depuis l'Explorateur d'agent sur n'importe quel serveur CA Enterprise Log Manager. Vous pouvez utiliser cette commande pour vous préparer à redémarrer un processus d'agent et tous ses connecteurs.

Pour arrêter le démon ou service de l'agent CA ELM

1. Connectez-vous en tant qu'utilisateur root ou administrateur Windows.
2. Accédez à une invite de commande, puis entrez la commande ci-après.

Linux, UNIX, Solaris : `/opt/CA/ELMagent/bin/S99elmagent stop`

Windows : `net stop ca-elmagent`

Vérification de l'installation du serveur CA Enterprise Log Manager

Vous pouvez vérifier l'installation du serveur CA Enterprise Log Manager à l'aide d'un navigateur Web. Vous pouvez effectuer une vérification initiale de l'installation en vous connectant sur le serveur CA Enterprise Log Manager.

Remarque : Lorsque vous vous connectez à l'application CA Enterprise Log Manager pour la première fois, vous devez utiliser les informations d'identification de l'utilisateur EiamAdmin avec lesquelles vous avez installé le serveur CA Enterprise Log Manager. Une fois connecté avec ce compte d'utilisateur, vous pouvez afficher et utiliser uniquement des fonctions spécifiques de gestion des utilisateurs et des accès. Vous devez ensuite configurer votre magasin d'utilisateurs et créer un nouveau compte d'utilisateur CA Enterprise Log Manager pour accéder aux autres fonctionnalités CA Enterprise Log Manager.

Pour vérifier l'installation du serveur CA Enterprise Log Manager

1. Ouvrez un navigateur Web et entrez l'URL ci-dessous.

`https://<adresse_IP_serveur>:5250/spin/cal`

L'écran de connexion à CA Enterprise Log Manager s'affiche.

2. Connectez-vous en tant qu'utilisateur administratif EiamAdmin.

Le sous-onglet Gestion des utilisateurs et des accès de l'onglet Administration s'affiche. Vous pouvez considérer l'installation comme réussie si vous pouvez vous connecter au serveur CA Enterprise Log Manager.

Remarque : Vous devez configurer un ou plusieurs services de sources d'événement avant de pouvoir recevoir des données d'événement et afficher des rapports.

Affichage des événements d'autosurveillance

Vous pouvez utiliser les événements d'autosurveillance pour vérifier que le serveur CA Enterprise Log Manager est correctement installé. Même si vous devez terminer certaines tâches de configuration avant que CA Enterprise Log Manager ne puisse collecter des données de journaux d'événements et générer des rapports sur votre réseau, vous pouvez afficher directement des événements d'autosurveillance générés par le serveur CA Enterprise Log Manager.

La connexion au serveur CA Enterprise Log Manager est le premier et le meilleur test d'une installation réussie. Les événements d'autosurveillance constituent un autre moyen de vérifier l'état du serveur CA Enterprise Log Manager. Différents types d'événements d'autosurveillance sont disponibles. Utilisez la procédure suivante pour afficher des données d'événements supplémentaires provenant d'événements générés par le serveur CA Enterprise Log Manager lui-même.

Pour afficher des événements d'autosurveillance

1. Connectez-vous au serveur CA Enterprise Log Manager.
2. Accédez à l'onglet Rapports.
3. Cliquez sur la balise Système et sélectionnez le rapport Détail des événements d'autosurveillance.

Le rapport des événements d'autosurveillance se charge.

4. Vérifiez que les événements d'autosurveillance pour votre connexion et d'autres actions de configuration préliminaires sont présents dans le rapport.

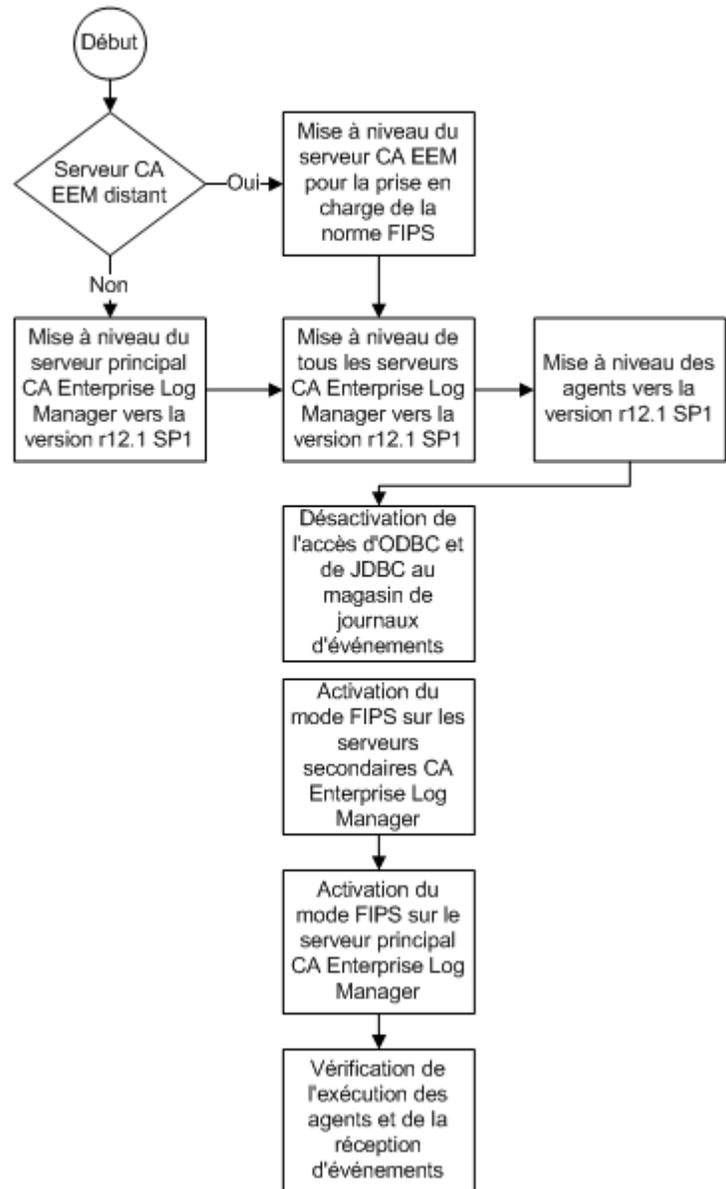
Mise à niveau des serveurs et des agents CA Enterprise Log Manager existants pour la prise en charge de la norme FIPS

Vous pouvez mettre à niveau les serveurs et les agents CA Enterprise Log Manager existants pour la prise en charge de la norme FIPS à l'aide du service d'abonnement. Pour effectuer cette mise à niveau, les conditions suivantes doivent être réunies :

- Vous avez installé CA Enterprise Log Manager r12.1 ou vous avez effectué une mise à niveau vers la version 12.1 à partir de la version 12.0 SP3.
- Vous voulez activer le mode FIPS pour votre fédération CA Enterprise Log Manager.

Pour mettre à niveau vos serveurs, procédez comme suit :

Mise à niveau d'un serveur et des agents CA ELM pour la prise en charge de la norme FIPS



La mise à niveau et l'activation du mode FIPS incluent les étapes suivantes :

1. Effectuez une mise à niveau du serveur principal ou de gestion vers la version 12.1 SP1.

Si vous utilisez un serveur CA EEM distant, assurez-vous que sa version permet les opérations FIPS. Pour plus d'informations sur la mise à niveau pour la prise en charge du mode FIPS, reportez-vous aux *Notes de parution de CA EEM*.

Pour obtenir des instructions détaillées sur l'utilisation du service d'abonnement pour mettre à niveau les serveurs et les agents CA Enterprise Log Manager, reportez vous à la section du *Manuel d'administration* sur les abonnements.

2. Procédez à la mise à niveau de tous les autres serveurs CA Enterprise Log Manager de la fédération vers la version 12.1 SP1.
3. Procédez également à la mise à niveau de tous les agents vers la version 12.1 SP1, puis à la mise à jour des détecteurs de journal de connecteur selon vos besoins.

Important : Si vous avez déployé un connecteur qui utilise le détecteur de journaux Syslog sur un hôte Windows, procédez à la mise à jour de toutes les configurations de ce connecteur. Si le mode d'exécution choisi est FIPS, vous pouvez utiliser le dernier détecteur Syslog pour cette version. Pour obtenir la dernière liste des intégrations qui utilisent le détecteur de journaux Syslog, consultez la Matrice d'intégration de produit https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.html de CA Enterprise Log Manager.

4. Désactivez l'accès d'ODBC et de JDBC au magasin de journaux d'événements.
5. Activez le mode FIPS sur tous les serveurs CA Enterprise Log Manager secondaires de la fédération.

Les agents détectent automatiquement le mode d'exploitation du serveur CA Enterprise Log Manager qui les gère.
6. Activez le mode FIPS sur le serveur principal ou de gestion.
7. A l'aide du tableau de bord Explorateur d'agent, vérifiez que les agents sont exécutés en mode FIPS.

Vous pouvez également vérifier que les agents envoient des événements à l'aide d'une requête ou d'un rapport ou en examinant l'onglet Evénements d'autosurveillance dans la zone Service Etat du système.

Lorsque vous mettez un agent existant à niveau vers la version 12.1 SP1, le traitement d'abonnements procède à la mise à jour de l'agent en mode non FIPS par défaut. Vous pouvez définir le mode FIPS du serveur CA Enterprise Log Manager qui gère un agent. L'agent détecte le mode FIPS de son serveur de gestion et redémarre dans le mode correspondant. Pour afficher le mode FIPS d'un agent si disposez des droits d'administrateur, utilisez le tableau de bord Explorateur d'agent dans l'interface utilisateur de CA Enterprise Log Manager. Pour plus d'informations, consultez les informations sur la mise à niveau dans la section du *Manuel d'implémentation* sur l'installation de CA Enterprise Log Manager ou l'Aide en ligne pour des tâches de gestion d'agents.

Informations complémentaires :

[Activation des opérations en mode FIPS](#) (page 94)

[Affichage du tableau de bord des agents](#) (page 96)

Conditions préalables à la mise à niveau pour la prise en charge de la norme FIPS

Conditions préalables à la mise à niveau de CA Enterprise Log Manager pour la prise en charge de la norme FIPS 140-2 :

- Commencez avec une installation de la version 12.0 SP3 ou 12.1 de CA Enterprise Log Manager.
- Procédez à la mise à niveau vers la version r12.1 SP1 de CA Enterprise Log Manager au moyen de l'abonnement.

Informations complémentaires :

[Ajout de serveurs CA Enterprise Log Manager à une fédération en mode FIPS existante](#) (page 98)

Instructions concernant la mise à niveau

Les instructions suivantes s'appliquent à la mise à niveau de CA Enterprise Log Manager pour la prise en charge de la norme FIPS :

- Si vous disposez de plusieurs serveurs CA Enterprise Log Manager dans une fédération, procédez à la mise à niveau du serveur principal ou du serveur de gestion vers la version 12.1 SP1 en premier lieu. Procédez ensuite à la mise à niveau de tous les autres serveurs indistinctement. Les serveurs mis à niveau démarrent en mode non-FIPS uniquement. Pour activer le mode FIPS, vous devez disposer des droits d'administrateur et définir le mode d'exploitation manuellement.

Important : Pendant le traitement de l'abonnement, ne modifiez pas le mode FIPS des serveurs CA Enterprise Log Manager secondaires. Un échec du traitement pourrait se produire.

- Les serveurs CA Enterprise Log Manager r12.1 SP1 peuvent communiquer avec des agents r12.1, mais la norme FIPS n'est pas prise en charge au niveau des agents tant que la mise à niveau vers la version 12.1 SP1 n'est pas effectuée.
- Lorsque vous activez le mode FIPS, seuls les agents r12.1 SP1 et supérieurs en mode FIPS peuvent communiquer avec le serveur CA Enterprise Log Manager. Lorsque vous activez le mode *non*-FIPS, le serveur CA Enterprise Log Manager est complètement rétrocompatible avec des agents plus anciens, mais les opérations en mode FIPS ne sont pas disponibles. Nous vous recommandons d'installer *uniquement* les agents r12.1 SP1 après avoir mis à niveau vos serveurs CA Enterprise Log Manager vers la version 12.1 SP1.
- Les agents associés à un serveur CA Enterprise Log Manager détectent automatiquement les modifications de mode du serveur et redémarrent en mode correspondant.
- L'ajout d'un nouveau serveur CA Enterprise Log Manager à une fédération existante exécutée en mode FIPS suppose un traitement spécial. Pour plus d'informations sur l'ajout d'un nouveau serveur CA Enterprise Log Manager à une fédération existante, consultez la section du *Manuel d'implémentation* correspondante.

Mise à niveau d'un serveur CA EEM distant

Si vous utilisez un serveur CA EEM autonome pour votre installation CA Enterprise Log Manager, procédez à sa mise à niveau pour la prise en charge de la norme FIPS, avant de mettre à niveau l'un de vos serveurs ou agents CA Enterprise Log Manager. Pour obtenir des instructions détaillées, consultez le *Manuel de prise en main de CA EEM*.

Désactivation de l'accès d'ODBC et de JDBC au magasin de journaux d'événements

Vous pouvez empêcher l'accès d'ODBC et de JDBC aux événements du magasin de journaux d'événements à l'aide des options de la boîte de dialogue de configuration de service ODBC. Si vous envisagez d'exécuter votre réseau fédéré en mode FIPS, désactivez l'accès d'ODBC et de JDBC pour conserver la conformité aux normes de fédération.

Pour désactiver un accès ODBC et JDBC :

1. Connectez-vous au serveur CA Enterprise Log Manager et sélectionnez l'onglet Administration.
2. Cliquez sur le sous-onglet Services, puis développez le noeud de service ODBC.
3. Sélectionnez le serveur approprié.
4. Désactivez la case à cocher Activer le service, puis cliquez sur Enregistrer.

Remarque : Pour vérifier que les services ODBC et JDBC sont désactivés, désactivez l'option d'ODBC pour *tous* les serveurs CA Enterprise Log Manager d'une fédération.

Activation des opérations en mode FIPS

Pour activer et désactiver le mode FIPS, utilisez les options de mode FIPS du service Etat du système. Le mode non-FIPS est défini par défaut. Les administrateurs doivent définir le mode FIPS pour chaque serveur CA Enterprise Log Manager dans une fédération.

Important : Vous ne pouvez pas utiliser des modes mixtes pour une même fédération de serveurs. Si un serveur exécuté dans une fédération utilise un mode différent, il ne pourra pas collecter les données de requêtes et de rapports ou répondre aux demandes provenant d'autres serveurs.

Pour permuter les modes FIPS et non-FIPS :

1. Connectez-vous au serveur CA Enterprise Log Manager.
2. Accédez à l'onglet Administration, puis cliquez sur le sous-onglet Services.
3. Développez le noeud de service Etat du système et sélectionnez un serveur CA Enterprise Log Manager.

La boîte de dialogue Configuration du service s'affiche.

4. Sélectionnez un mode FIPS, activé ou désactivé, dans la liste déroulante.
5. Cliquez sur Enregistrer.

Le serveur CA Enterprise Log Manager redémarre dans le mode sélectionné. Vous pouvez vous connecter de nouveau pour afficher le mode FIPS de l'agent dans l'explorateur d'agent.

6. Vérifiez le serveur CA Enterprise Log Manager en utilisant la boîte de dialogue du service Etat du système après le redémarrage du serveur.

Vous pouvez également utiliser des événements d'autosurveillance pour vérifier que le démarrage du serveur CA Enterprise Log Manager a lieu selon le mode souhaité. Recherchez les événements suivants dans l'onglet Evénements d'autosurveillance de la boîte de dialogue Etat du système :

Mode FIPS activé sur le serveur
Mode FIPS désactivé sur le serveur
Echec de l'activation du mode FIPS sur le serveur
Echec de la désactivation du mode FIPS sur le serveur

La désactivation du mode FIPS pour le serveur principal ou le serveur de gestion interrompt toutes les requêtes et rapports fédérés renvoyant des données, et les rapports planifiés ne s'exécutent pas. Cette condition reste valide jusqu'à ce que tous les serveurs de la fédération s'exécutent de nouveau selon le même mode.

Remarque : La désactivation du mode FIPS sur le serveur CA EEM de gestion ou distant est une des conditions requises pour l'ajout de serveurs CA Enterprise Log Manager à une fédération de serveurs s'exécutant en mode FIPS.

Affichage du tableau de bord des agents

Vous pouvez afficher le tableau de bord de l'agent pour afficher l'état des agents dans votre environnement. Le tableau de bord affiche également des informations telles que le mode FIPS utilisé (FIPS ou non-FIPS) et les détails d'utilisation. Ces détails incluent le chargement d'événements par seconde, le pourcentage d'utilisation de l'UC, l'heure et la date de mise à jour la plus récente.

Pour afficher le tableau de bord des agents

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Collecte de journaux.

La liste du dossier Collecte de journaux s'affiche.

2. Sélectionnez le dossier de l'Explorateur d'agent.

Les boutons de gestion des agents s'affichent dans le volet Détails.

3. Cliquez sur Tableau de bord et contrôleur de l'état des agents : 

Le panneau de recherche d'agents apparaît et affiche l'état de tous les agents disponibles dans un graphique détaillé. Par exemple :

Total : 10 Exécution en cours : 8 En attente : 1 Arrêté : 1 Aucune réponse : 0

4. Sélectionnez des critères de recherche d'agents pour restreindre le nombre d'agents affichés (facultatif). Vous pouvez sélectionner un ou plusieurs des critères ci-dessous.

- Groupe d'agents : renvoie uniquement les agents affectés au groupe sélectionné.
- Plate-forme : renvoie uniquement les agents s'exécutant sur la plate-forme sélectionnée.
- Etat : renvoie uniquement les agents dont l'état correspond à celui que vous avez sélectionné, par exemple Exécution en cours.
- Schéma de nom de l'agent : renvoie uniquement les agents contenant le schéma spécifié.

5. Cliquez sur Afficher l'état.

La liste des agents correspondant à vos critères de recherche apparaît et affiche, entre autres, les informations suivantes.

- Nom et version du connecteur local
- Serveur CA Enterprise Log Manager actuel
- Mode FIPS de l'agent (FIPS ou non-FIPS)
- Dernier enregistrement en date du nombre d'événements reçus par seconde traité par l'agent
- Dernier enregistrement en date du pourcentage d'utilisation de l'UC
- Dernier enregistrement en date du pourcentage d'utilisation de la mémoire
- Mise à jour de configuration la plus récente
- Etat de la mise à jour de la configuration

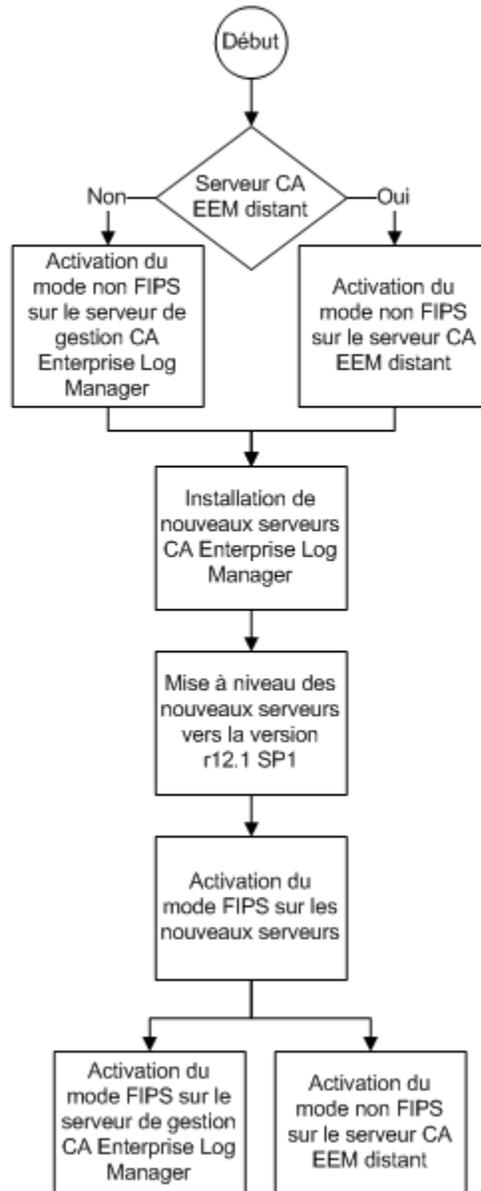
Ajout de serveurs CA Enterprise Log Manager à une fédération en mode FIPS existante

Pour ajouter un nouveau serveur CA Enterprise Log Manager à une fédération de serveurs exécutés en mode FIPS, vous devez suivre plusieurs recommandations. Si vous ne spécifiez pas le mode FIPS lors de l'installation, les serveurs CA Enterprise Log Manager nouvellement installés passeront en mode *non-FIPS* par défaut. Les serveurs exécutés en mode non-FIPS ne peuvent pas communiquer avec des serveurs exécutés en mode FIPS.

Lors de son installation, un serveur CA Enterprise Log Manager doit être enregistré auprès du serveur CA EEM intégré local sur le serveur de gestion ou auprès d'un serveur CA EEM distant autonome. Les processus pour ajouter un serveur à un réseau existant dépendent de l'emplacement du serveur CA EEM de gestion.

Le flux de travaux ci-dessous décrit l'approche à suivre.

Ajout d'un serveur ELM à une fédération en mode FIPS uniquement



Le processus pour ajouter un nouveau serveur inclut les étapes suivantes :

1. Activez le mode FIPS sur le serveur de gestion CA Enterprise Log Manager ou sur le serveur CA EEM distant.
2. L'image ISO ou les DVD de CA Enterprise Log Manager 12.1 SP1 (ou versions ultérieures) permettent d'installer un ou plusieurs serveurs CA Enterprise Log Manager secondaires.

Important : Vous devez activer le mode FIPS lors de l'installation. Si vous ne l'activez pas, le serveur nouvellement installé ne pourra pas communiquer avec le serveur de gestion ou le serveur CA EEM distant et vous devrez réinstaller le nouveau serveur CA Enterprise Log Manager.

L'activation du mode FIPS pour le serveur de gestion CA Enterprise Log Manager ou le serveur CA EEM distant permet d'enregistrer le nouveau serveur CA Enterprise Log Manager et de le rattacher à la fédération.

Informations complémentaires :

[Activation des opérations en mode FIPS](#) (page 94)

[Affichage du tableau de bord des agents](#) (page 96)

Remarques concernant l'installation d'un système disposant de lecteurs SAN

Lorsque vous installez le système d'exploitation pour le dispositif de CA Enterprise Log Manager sur un système disposant de lecteurs SAN, veillez à ne pas effectuer d'installation sur un lecteur SAN. Un échec se produit pour ces installations.

Pour une installation réussie, suivez l'une des approches suivantes :

- Désactivez les lecteurs SAN. Installez le système d'exploitation et l'application CA Enterprise Log Manager normalement. Configurez les lecteurs SAN pour CA Enterprise Log Manager, puis redémarrez CA Enterprise Log Manager pour activer la configuration.
- Laissez les lecteurs SAN activés. Commencez l'installation du système d'exploitation. Quittez la procédure en suivant la description qui s'affiche pour modifier la séquence d'opérations définies dans le fichier kickstart. Reprenez la procédure et terminez l'installation en suivant les instructions.

Installation avec des lecteurs SAN désactivés

CA Enterprise Log Manager est actuellement pris en charge sur des configurations matérielles fixes fournies par Dell, IBM et HP. La configuration matérielle supposée dans l'exemple ci-dessous est la suivante : serveurs HP Blade Servers utilisant une carte QLogic Fiber Channel permettant la connexion au réseau SAN pour l'archivage de données. Les serveurs HP Blade Servers disposent de disques durs SATA configurés en RAID-1 (en mode miroir).

Pour utiliser le fichier de démarrage kickstart directement, veuillez à désactiver les lecteurs SAN avant de commencer l'installation. Lancez le processus d'installation au moyen du DVD OS5 et suivez les instructions pour terminer l'installation.

Remarque : Si lorsque vous lancez l'installation, les lecteurs SAN ne sont pas désactivés, CA Enterprise Log Manager est installé sur le lecteur SAN. Dans ce cas, une fenêtre rouge s'affiche après le redémarrage de CA Enterprise Log Manager avec le message : Illegal Opcode.

Utilisez les procédures suivantes pour installer un dispositif CA Enterprise Log Manager sur un système disposant de lecteurs SAN. Les lecteurs SAN doivent être désactivés avant de lancer l'installation du système d'exploitation.

1. Désactivez les lecteurs SAN.
2. Installez le système d'exploitation sur le dispositif.
3. Installez le serveur CA Enterprise Log Manager.
4. Créez une configuration multi-acheminement pour le stockage SAN.
5. Créez un volume logique.
6. Préparez le volume logique pour CA Enterprise Log Manager.
7. Redémarrez CALM.
8. Vérifiez que l'installation a été effectuée correctement.

Lorsque vous installez le système d'exploitation avec les lecteurs SAN désactivés, vous travaillez avec les fichiers suivants :

lvm.conf

Fichier de configuration pour le gestionnaire de volumes logiques de Linux (LVM2).

multipath.conf (/etc/multipath.conf)

Fichier de configuration pour le multi-acheminement de Linux.

fstab (/etc/fstab)

Fichier de table des systèmes de fichiers qui mappe les périphériques aux répertoires dans un système Linux.

Désactivation de lecteurs SAN

Pour désactiver les lecteurs SAN sur le matériel sur lequel vous souhaitez installer le dispositif logiciel, suivez les procédures recommandées par votre fournisseur de lecteur SAN.

Désactivez les lecteurs SAN avant d'installer le système d'exploitation du dispositif logiciel ou l'application CA Enterprise Log Manager.

Création d'une configuration multi-acheminement pour le stockage SAN

Une configuration multi-acheminement est requise pour un système CA Enterprise Log Manager installé sur un système RAID pour permettre le stockage SAN. Les disques physiques du SAN sont partitionnés en espaces de stockage logiques appelés numéros d'unité logiques (LUN).

Pour créer une configuration multi-acheminement pour le stockage SAN :

1. Connectez-vous au dispositif CA Enterprise Log Manager en tant qu'utilisateur root à l'aide de la commande su.
2. (Facultatif) Pour afficher l'état de la configuration avant la configuration du multi-acheminement et des volumes logiques, créez une liste des répertoires de /dev/mapper. Les résultats sont comparables à ceux-ci :

```
drwxr-xr-x 2 root root    120 Jun 18 12:09 .
drwxr-xr-x 11 root root   3540 Jun 18 16:09 ..
crw----- 1 root root    10, 63 Jun 18 12:09 control
brw-rw---- 1 root disk 253,  0 Jun 18 16:09 VolGroup00-LogVol00
brw-rw---- 1 root disk 253,  2 Jun 18 12:09 VolGroup00-LogVol01
brw-rw---- 1 root disk 253,  1 Jun 18 16:09 VolGroup00-LogVol02
```

3. Ouvrez le fichier de configuration `.../etc/multipath.conf` et modifiez-le comme suit :

- a. Ajoutez la section suivante sous `device{` pour chaque LUN fourni par l'administrateur SAN :

```
device {
    vendor          "NETAPP"
    product         "LUN"
    path_grouping_policy multibus
    features        "1 queue_if_no_path"
    path_checker    readsector0
    path_selector   "round-robin 0"
    failback        immediate
    no_path_retry   queue
}
```

- b. Supprimer les commentaires de la section `blacklist` pour tous les périphériques. La section `blacklist` permet d'activer le multi-acheminement sur les périphériques par défaut.

```
blacklist {
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
    devnode "^hd[a-z]"
    devnode "^cciss!c[0-9]d[0-9]*"
}
```

- c. Enregistrez et fermez le fichier `multipath.conf`.

4. Vérifiez que l'option de multi-acheminement est activée et que les LUN sont répertoriés à l'aide de la commande suivante :

```
multipath -l
```

Remarque : Les chemins d'accès sont affichés comme `mpath0` et `mpath1`. Si les LUN ne sont pas affichés, redémarrez et exécutez le multi-acheminement à nouveau.

5. Affichez les lecteurs disponibles.

```
fdisk -l
```

6. Répertoriez les partitions disponibles et vérifiez que `mpath0` et `mpath1` y sont inclus.

```
ls -la /dev/mapper
```

7. Mappez la première partition comme suit :

```
kpartx -a /dev/mapper/mpath0
```

8. Mappez la seconde partition comme suit :

```
kpartx -a /dev/mapper/mpath1
```

Création d'un volume logique

Vous pouvez utiliser un gestionnaire de volumes pour combiner plusieurs LUN dans un volume logique pour permettre à CA Enterprise Log Manager d'y accéder. Le gestionnaire de volumes logiques (LVM) gère des lecteurs de disque et des périphériques de stockage de masse similaires sur Linux. Les colonnes de stockage créées avec le LVM peuvent être redimensionnées ou déplacées sur des périphériques d'arrière-plans pour le stockage SAN par exemple.

Pour créer un volume logique :

1. Créez le premier volume physique :

```
pvccreate /dev/mapper/mpath0
```

2. Créez le second volume physique :

```
pvccreate /dev/mapper/mpath1
```

3. Affichez tous les volumes physiques sur le système :

```
pvdisk
```

4. Créez le groupe de volumes VolGroup01. Le groupe de volumes VolGroup00 existe déjà.

```
vgcreate VolGroup01 /dev/mapper/mpath0 /dev/mapper/mpath1
```

Remarque : Cette commande permet de créer un volume et d'ajouter les deux volumes physique au groupe.

5. Créez un volume logique dans le groupe de volumes :

```
lvcreate -n LogVol00 -l 384030 VolGroup01
```

6. Créez un système de fichiers.

```
mkfs -t ext3 /dev/VolGroup01/LogVol00
```

Préparation du volume logique pour CA Enterprise Log Manager

Après avoir créé un volume logique, complétez-le avec la structure de répertoires appropriée et affectez les associations de droits de propriété et de groupe requises pour CA Enterprise Log Manager. Utilisez l'éditeur vi pour modifier le fichier fstab afin qu'il pointe vers le volume logique que vous avez créé. Montez ensuite le nouveau répertoire de données.

Pour préparer le volume logique pour CA Enterprise Log Manager :

1. Créez un répertoire temporaire /data1, remplacez les droits de propriété du répertoire /data1 par caelmservice, puis remplacez le groupe associé à ce répertoire par caelmservice :

```
mkdir /data1
chown caelmservice /data1
chgrp caelmservice /data1
```

2. Arrêtez les processus iGateway du serveur CA Enterprise Log Manager :

```
/opt/CA/SharedComponents/iTechnology/S99igateway stop
```

3. Remplacez les répertoires par le répertoire d'exécution de l'agent CA Enterprise Log Manager, arrêtez l'agent et vérifiez que les services sont arrêtés :

```
cd /opt/CA/ELMAgent/bin/
./caelmagent -s
ps -ef | grep /opt/CA
```

4. Remplacez le répertoire par un répertoire /.

5. Montez le nouveau système de fichiers sur /data1, copiez le contenu du répertoire /data dans /data1 et vérifiez que les deux répertoires sont bien les mêmes :

```
mount -t ext3 /dev/VolGroup01/LogVol00 /data1
cp -pR /data/* /data1
diff -qr /data /data1
```

6. Démontez le point de montage de données existant, puis démontez le point de montage du répertoire data1 :

```
umount /data
umount /data1
```

7. Supprimez le répertoire /data et renommez le répertoire /data1 en /data.

```
rm -rf /data
mv /data1 data
```

8. Modifiez la ligne de /etc/fstab qui référence le répertoire /data et pointez-la vers le nouveau volume logique. C'est-à-dire, remplacez /dev/VolGroup00/LogVol02 par /dev/VolGroup01/LogVol00. Les données modifiées sont affichées en caractères gras dans l'exemple de fichier fstab modifié suivant .

Nom de l'unité	Point de montage	fs-type	options	dump-freq pass-num
none	/dev/VolGroup00/LogVol00/	ext3	Valeurs par défaut	1 1
none	/dev/VolGroup01/LogVol00/data	ext3	Valeurs par défaut	2 1
LABEL=/boot	/boot	ext3	Valeurs par défaut	2 1
tmpfs	/dev/shm	tmpfs	Valeurs par défaut	0 0
devpts	/dev/pts	devpts	gid=5,mode=620	0 0
sysfs	/sys	sysfs	Valeurs par défaut	0 0
proc	/proc	proc	Valeurs par défaut	0 0
none	/dev/VolGroup00/LogVol01	swap	Valeurs par défaut	0 0

9. Montez le nouveau répertoire de données et vérifiez que toutes les partitions de /etc/fstab sont montées :

```
mount -a
mount
```

Redémarrez le serveur CA Enterprise Log Manager

Après avoir créé un volume logique, redémarrez CA Enterprise Log Manager pour pouvoir utiliser le volume logique. Pour vérifier la réussite de l'opération, accédez à CA Enterprise Log Manager et affichez les événements renvoyés par la requête Détail de tous les événements du système.

Pour redémarrer le serveur CA Enterprise Log Manager :

1. Démarrez les processus iGateway du serveur CA Enterprise Log Manager :

```
/opt/CA/SharedComponents/iTechnology/S99igateway start
```
2. Démarrez le service ELMAgent.

```
/opt/CA/ELMAgent/bin/caelmagent -b
```
3. Redémarrez le serveur CA Enterprise Log Manager.

Installation avec des lecteurs SAN activés

La rubrique Exemple : Configuration du stockage SAN pour CA Enterprise Log Manager, inclut la recommandation de désactiver les lecteurs SAN (LUN) avant d'installer le système d'exploitation sur le dispositif CA Enterprise Log Manager.

Une alternative vous permet de conserver les lecteurs SAN activés. Pour cela, le fichier kickstart ca-elm-ks.cfg doit être modifié à l'aide d'un outil d'édition ISO, une fois que l'installation du système d'exploitation a été lancée. Ces modifications vous garantissent que l'installation et le démarrage sont effectués à partir du disque dur local et non à partir du SAN.

Pour démarrer à partir du disque local et non à partir du SAN :

1. Démarrez le serveur avec le DVD d'installation du SE.
2. Répondez à la première invite de saisie clavier.
3. Pour afficher l'invite Anaconda/Kickstart, appuyez sur Maj+F2.
4. Saisissez la commande suivante.

```
list-harddrives
```

Une liste des lecteurs disponibles similaire à la liste ci-dessous s'affiche :

```
cciss/c0d0 – 68GB RAID 1 (cciss est un lecteur HP Smart Array)
Sda – 500GB SAN (sda - h correspondent au SAN multiacheminé)
Sdb – 500GB SAN
Sdc – 500GB SAN
Sdd – 500GB SAN
Sde – 500GB SAN
Sdf – 500GB SAN
Sdg – 500GB SAN
Sdh – 500GB SAN
```

5. Identifiez le disque dur local. Dans ce cas, il s'agit de cciss/c0d0.

6. Effectuez la procédure suivante :
 - a. Ouvrez le fichier kickstart du système d'exploitation de CA Enterprise Log Manager, `ca-elm-ks.cfg` pour le modifier. Utilisez un éditeur ISO.
 - b. Identifiez la ligne suivante à modifier :

```
bootloader --location=mbr --driveorder=sda,sdb
```

Remplacez-la par :

```
bootloader --location=mbr --driveorder=cciss/c0d0
```

Cette modification permet le démarrage à partir du disque local uniquement.
 - c. Identifiez les lignes suivantes à modifier :

```
clearpart --all --initlabel  
part /boot --fstype "ext3" --size=100  
part pv.4 --size=0 --grow
```

Remplacez-les par :

```
part /boot --fstype "ext3" --size=100 --ondisk cciss/c0d0  
part pv.4 --size=0 --grow --ondisk cciss/c0d0
```

Cette modification des lignes de définition de partition permet de s'assurer que les partitions sont créées sur le disque `cciss/c0d0` par nom. L'utilisation de `--ondisk` vous permet de remplacer les variables `$disk1` et `$disk2` existantes.
 - d. Supprimez la clause `IF/When` pour le nombre de lecteurs et conservez uniquement le premier ensemble de commandes disque (lignes 57 - 65), si vous l'estimez nécessaire.
 - e. Enregistrez la nouvelle image ISO.
7. Quittez l'invite Anaconda et retournez aux invites d'installation du système d'exploitation.
8. Poursuivez l'installation en utilisant les procédures documentées.

Configurations initiales du serveur CA Enterprise Log Manager

L'installation du premier serveur CA Enterprise Log Manager crée un nom d'application dont la valeur par défaut est CAELM. L'installation enregistre ce nom auprès du serveur CA EEM intégré. Si les installations suivantes utilisent le même nom d'instance d'application, le serveur CA Enterprise Log Manager de gestion gère toutes les configurations sous ce même nom d'instance d'application.

Une fois l'installation terminée, le serveur est doté d'un système d'exploitation et d'un serveur CA Enterprise Log Manager. Le système d'exploitation 32 bits prend en charge le matériel 32 bits et 64 bits. Les configurations initiales affectent les domaines ci-dessous.

- Comptes d'utilisateur par défaut
- Structure des répertoires par défaut
- Image du système d'exploitation personnalisé
- Affectations de ports par défaut

Comptes d'utilisateur par défaut

L'installation de CA Enterprise Log Manager crée un utilisateur d'administration par défaut, caelmadmin, qui possède son propre mot de passe. Si vous devez accéder directement au serveur hôte, vous devez utiliser ce compte pour vous connecter, car la fonction de connexion du compte root est restreinte après l'installation. Le compte caelmadmin permet uniquement la connexion. Dès lors, vous devez passer au compte root grâce à son mot de passe distinct pour pouvoir accéder aux utilitaires d'administration système au niveau du SE.

Le mot de passe par défaut pour ce compte est identique au mot de passe créé pour le compte EiamAdmin. Nous recommandons de modifier le mot de passe du compte caelmadmin immédiatement après l'installation.

L'installation crée également un compte d'utilisateur de service par défaut, caelmservice, que vous *ne pouvez pas* utiliser pour vous connecter au système. Vous pouvez passer au compte de cet utilisateur pour démarrer et arrêter des processus, le cas échéant. Le processus iGateway et le serveur CA EEM intégré (s'il est installé sur le serveur CA Enterprise Log Manager) s'exécutent sous ce compte d'utilisateur, pour offrir une couche supplémentaire de sécurité.

Le processus iGateway ne s'exécute pas sous un compte d'utilisateur root. Le transfert de port est automatiquement activé pour permettre aux demandes HTTPS sur les ports 80 et 443 d'accéder à l'interface utilisateur CA Enterprise Log Manager, en plus du port 5250.

Structure des répertoires par défaut

L'installation de CA Enterprise Log Manager place les fichiers binaires du logiciel sous la structure de répertoires `/opt/CA`. Si le système comporte un deuxième lecteur de disque, il est configuré comme `/data`. L'installation crée un lien symbolique du répertoire `/opt/CA/LogManager/data` vers le répertoire `/data`. Vous trouverez ci-dessous la structure de répertoires d'installation par défaut.

Types de fichiers	Répertoire
Fichiers liés à iTechnology (iGateway)	<code>/opt/CA/SharedComponents/iTechnology</code>
Fichiers liés au serveur CA Enterprise Log Manager EEM	<code>/opt/CA/LogManager/EEM</code>
Fichiers liés à l'installation de CA Enterprise Log Manager	<code>/opt/CA/LogManager/install</code>
Fichiers de données (liens vers <code>/data</code> en cas de lecteurs multiples)	<code>/opt/CA/LogManager/data</code>
Fichiers journaux	<code>/opt/CA/SharedComponents/iTechnology</code>

Dans des circonstances normales, vous ne devez pas avoir besoin d'accéder à l'utilitaire `ssh` sur le serveur CA Enterprise Log Manager, hormis pour déplacer des fichiers d'archive à des fins de sauvegarde et de stockage à long terme, ou encore pour ajouter des lecteurs de disque.

Image du système d'exploitation personnalisé

Le processus d'installation personnalise le système d'exploitation en créant une image minimale et en limitant l'accès à cette image à très peu de canaux. Les services non essentiels ne sont pas installés. Le serveur CA Enterprise Log Manager écoute sur un petit nombre de ports et désactive spécifiquement les ports inutilisés.

Lors de l'installation du système d'exploitation, vous créez un mot de passe pour le compte `root`. Une fois l'installation de CA Enterprise Log Manager terminée, le compte `root` est restreint et ne permet aucune autre connexion. L'installation de CA Enterprise Log Manager crée un utilisateur par défaut, `caelmadmin`, qui dispose uniquement de la fonction de connexion, sans autres droits.

Pour un accès de niveau root au serveur CA Enterprise Log Manager, vous pouvez accéder au serveur avec ce compte, puis passer à l'utilisateur root pour accéder aux outils d'administration. Cela signifie que vous devez connaître les mots de passe *caelmadmin* et *root* pour pouvoir accéder au système en tant qu'utilisateur root.

Aucun autre logiciel de sécurité spécifique n'est installé avec CA Enterprise Log Manager. Pour conserver d'excellentes performances, n'installez pas d'autres applications sur le serveur CA Enterprise Log Manager.

Affectations de ports par défaut

Le serveur CA Enterprise Log Manager est configuré par défaut pour écouter sur le port 5250 et sur les ports 80 et 443 pour le protocole HTTPS. Les processus et démons CA Enterprise Log Manager ne s'exécutent pas sous le compte root, ils ne peuvent donc pas ouvrir de ports inférieurs au port 1024. Par conséquent, l'installation crée automatiquement une redirection (par le biais de tables IP) vers le port 5250 pour les demandes entrantes de l'interface utilisateur sur les ports 80 et 443.

Le démon Syslog du système d'exploitation local du serveur CA Enterprise Log Manager n'est pas configuré, car CA Enterprise Log Manager utilise ses événements d'autosurveillance pour suivre l'état du système. Vous pouvez afficher d'autres événements locaux et générer des rapports sur des actions entreprises sur le serveur CA Enterprise Log Manager local à l'aide des événements d'autosurveillance.

Vous trouverez ci-dessous la liste des ports utilisés par l'environnement CA Enterprise Log Manager.

Port	Composant	Description
53	Serveur CA Enterprise Log Manager	Port TCP/UDP qui doit être disponible dans le cadre des communications DNS pour permettre la résolution des noms d'hôte et des adresses IP des serveurs, tels que les serveurs CA Enterprise Log Manager, le serveur CA EEM distant s'il est configuré et le serveur NTP si la synchronisation NTP a été sélectionnée lors de l'installation. Les communications DNS ne sont pas nécessaire si vous mappez des noms d'hôte aux adresses IP du fichier local <i>/etc/hosts</i> .

Port	Composant	Description
80	Serveur CA Enterprise Log Manager	Communications TCP avec l'interface utilisateur du serveur CA Enterprise Log Manager via HTTPS ; redirection automatique vers le port 5250.
111	Mappeur de ports (SAPI)	Communications des clients Audit avec le processus du mappeur de ports pour recevoir des affectations de ports dynamiques.
443	Serveur CA Enterprise Log Manager	Communications TCP avec l'interface utilisateur du serveur CA Enterprise Log Manager via HTTPS ; redirection automatique vers le port 5250.
514	Syslog	Port d'écoute Syslog UDP par défaut ; valeur du port configurable. Le port est défini par défaut sur 40514 et l'installation applique une règle de pare-feu au serveur CA Enterprise Log Manager pour que l'agent s'exécute en tant qu'utilisateur non root.
1468	Syslog	Port d'écoute Syslog TCP par défaut ; valeur du port configurable.
2123	DXadmin	Port DXadmin LDAP de CA Directory, si vous utilisez un serveur CA EEM sur le même serveur physique que le serveur CA Enterprise Log Manager (serveur de gestion)
5250	Serveur CA Enterprise Log Manager	Communications TCP avec l'interface utilisateur du serveur CA Enterprise Log Manager via iGateway. Communications TCP entre : <ul style="list-style-type: none"> ■ le serveur CA Enterprise Log Manager et le serveur CA EEM, ■ des serveurs CA Enterprise Log Manager fédérés, ■ un agent et le serveur CA Enterprise Log Manager pour les mises à jour d'état.
6789	Agent	Port d'écoute du contrôle et des commandes de l'agent. Remarque : Si vous n'autorisez pas le trafic sortant, vous devez ouvrir ce port pour permettre le bon fonctionnement.
17001	Agent	Port TCP pour les communications sécurisées de l'agent avec le serveur CA Enterprise Log Manager ; numéro de port configurable. Remarque : Si vous n'autorisez pas le trafic sortant, vous devez ouvrir ce port pour permettre le bon fonctionnement.

Port	Composant	Description
17002	ODBC/JDBC	Port TCP par défaut utilisé pour les communications entre le pilote ODBC ou JDBC et le magasin de journaux d'événements CA Enterprise Log Manager.
17003	Agent	Port TCP utilisé pour les communications par le bus de messages Qpid, pour les agents r12.1.
17200	Ecouteur SME de l'exécuteur	Port TCP utilisé par le service de l'exécuteur sur l'hôte local de l'agent pour écouter les événements d'autosurveillance entre les processus de l'agent.
17201	Ecouteur d'événement de l'exécuteur	Port TCP utilisé par le service de l'exécuteur sur l'hôte local de l'agent pour écouter les événements provenant des connecteurs du client
aléatoire	SAPI	Ports UDP utilisés pour la collecte d'événements affectée par le mappeur de ports ; vous pouvez également configurer le routeur et le collecteur SAPI pour utiliser n'importe quel numéro de port fixe au-delà de 1024.

Liste des processus liés

La table suivante représente une liste des processus s'exécutant au sein d'une implémentation CA Enterprise Log Manager. Cette liste n'intègre pas les processus système liés au système d'exploitation sous-jacent.

Nom du processus	Port par défaut	Description
caelmagent	6789, 17001	Il s'agit du processus de l'agent CA Enterprise Log Manager.
caelmconnector	Dépend de ce qu'il écoute ou de ce à quoi il est connecté.	Il s'agit du processus du connecteur CA Enterprise Log Manager. Un processus de connecteur distinct s'exécute pour chaque connecteur configuré sur un agent.
caelmdispatcher		Ce processus CA Enterprise Log Manager gère la soumission d'événements et les informations d'état entre le connecteur et l'agent.
caelmwatchdog	Aucun	Processus de surveillance CA Enterprise Log Manager, qui surveille d'autres processus pour assurer la continuité des opérations

Nom du processus	Port par défaut	Description
caelm-agentmanager		Processus CA Enterprise Log Manager, qui traite les tâches de gestion d'agents telles que le statut et l'abonnement.
caelm-alerting		Processus CA Enterprise Log Manager, qui gère les messages d'alertes par courriel, IT PAM et les interruptions SNMP.
caelm-correlation		Processus CA Enterprise Log Manager, qui gère les règles de corrélation, en communiquant avec le service de corrélation lorsque l'une de ces règles se déclenche.
caelm-eemsessionsponsor		Processus CA EEM principal, qui gère toutes les communications vers CA EEM pour les sponsors locaux s'exécutant sous safetynet sur le serveur CA Enterprise Log Manager. Ce processus peut s'exécuter sous safetynet.
caelm-incidentsservice		Processus CA Enterprise Log Manager, qui gère la génération d'incident et la configuration de la journalisation, en traitant les informations du service de corrélation lorsqu'une règle de corrélation se déclenche.
caelm-logdepot	17001	Processus du magasin de journaux d'événements CA Enterprise Log Manager, qui gère le stockage des événements, la création de fichiers d'archive et d'autres fonctions. Ce processus peut s'exécuter sous safetynet.
caelm-queryservice		Processus CA Enterprise Log Manager, qui gère la configuration et la gestion des requêtes.
caelm-reporter		Processus CA Enterprise Log Manager, qui gère la configuration et la gestion des rapports planifiés, les exportations de rapports et les alertes d'action.
caelm-ruletest		Processus CA Enterprise Log Manager, qui gère les tests de règle effectués avec une fréquence ad hoc.
caelm-sapicollector		Il s'agit du processus du service de collecteur SAPI. Ce processus peut s'exécuter sous safetynet.

Nom du processus	Port par défaut	Description
caelm-sapirouter		Il s'agit du processus du service de routeur SAPI. Ce processus peut s'exécuter sous safetynet.
caelm-systemstatus		Ce processus collecte l'état du système à afficher dans l'interface utilisateur CA Enterprise Log Manager. Ce processus peut s'exécuter sous safetynet.
dxadmind		Processus CA Directory, exécuté sur le serveur où est installé CA EEM.
dxserver		Processus CA Directory, exécuté sur le serveur où est installé CA EEM.
igateway	5250	Processus CA Enterprise Log Manager principal, qui doit être en cours d'exécution pour collecter et stocker des événements
courtier de messages		Processus CA Enterprise Log Manager qui communique entre l'agent et le serveur CA Enterprise Log Manager pour envoyer des événements.
oaserver	17002	Processus CA Enterprise Log Manager qui s'exécute pour gérer le traitement côté serveur des demandes d'accès ODBC et JDBC au magasin de journaux d'événements.
safetynet		Cadre d'applications de processus CA Enterprise Log Manager, qui s'exécute pour assurer la continuité des opérations
ssld		Processus CA Directory, exécuté sur le serveur où est installé CA EEM.

Durcissement de système d'exploitation

Le dispositif logiciel CA Enterprise Log Manager contient une copie rationalisée et durcie du système d'exploitation Red Hat Linux. Les techniques de durcissement suivantes ont été appliquées :

- L'accès au SSH en tant qu'utilisateur root est désactivé.
- L'utilisation de la séquence clé de Ctrl-Maj-Supr pour redémarrer le serveur à partir de la console sans se connecter est désactivée.
- Les redirections sont appliquées aux iptables pour les ports suivants :
 - Le port TCP 80 et 443 sont redirigés vers le 5250.
 - Le port UDP 514 est redirigé vers le 40514.
- Le package GRUB est protégé par mot de passe.
- Lors de l'installation, les utilisateurs avec peu de droits suivants sont ajoutés :
 - caelmadmin - un compte de système d'exploitation disposant de droits de connexion à la console du serveur CA Enterprise Log Manager
 - caelmservice - un compte de service sous lequel sont exécutés les processus d'agent et d'iGateway. Vous ne pouvez pas vous connecter directement avec ce compte.

Redirection des ports du pare-feu pour les événements Syslog

Vous pouvez rediriger le trafic des ports standard vers d'autres ports si vous utilisez un pare-feu entre un agent et le serveur CA Enterprise Log Manager.

Les meilleures pratiques de sécurité indiquent les droits d'utilisateur minimaux nécessaires pour exécuter les processus et démons d'applications. Les démons UNIX et Linux fonctionnant sur des comptes non root ne peuvent pas ouvrir de ports inférieurs à 1024. Le port Syslog UDP standard est 514. Cela peut poser problème pour les unités comme les routeurs et les commutateurs, qui ne peuvent pas utiliser de ports non standard.

Pour résoudre ce problème, vous pouvez configurer le pare-feu pour qu'il écoute le trafic entrant sur le port 514 et qu'il effectue ses envois au serveur CA Enterprise Log Manager sur un autre port. La redirection se produit sur le même hôte, sous forme d'écouteur Syslog. Si vous choisissez d'utiliser un port non standard, vous devez alors reconfigurer chaque source d'événement pour qu'elle envoie ses événements sur ce port.

Pour rediriger le trafic d'événements via un pare-feu

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez à une invite de commande.
3. Entrez une commande afin de rediriger les ports pour votre pare-feu spécifique.

L'exemple ci-dessous illustre les entrées de ligne de commande pour l'outil de filtrage de paquets netfilter/iptables sur un système d'exploitation Red Hat Linux.

```
chkconfig --level 345
```

```
iptables on iptables -t nat -A PREROUTING -p udp --dport 514 -j REDIRECT --to  
<votre_nouveau_port>
```

```
service iptables save
```

4. Remplacez la valeur de la variable *<votre_nouveau_port>* par un numéro de port disponible et supérieur à 1024.

Pour d'autres implémentations, reportez-vous aux instructions de gestion des ports proposées par le fournisseur de votre pare-feu.

Installation du client ODBC

L'installation d'un client ODBC sur des systèmes Windows implique les étapes ci-dessous.

1. Vérifiez que vous disposez des autorisations requises et obtenez une clé de licence pour le pilote du client ODBC (conditions requises).
2. Installez le client ODBC.
3. Créez une source de données à l'aide de l'utilitaire Sources de données (ODBC) de Windows.
4. Configurez la connexion du client ODBC.
5. Testez la connexion à la base de données.

Configuration requise

L'accès ODBC au magasin de journaux d'événements est disponible uniquement dans CA Enterprise Log Manager r12.1 et les versions ultérieures. Pour plus d'informations, avant de procéder à l'installation, reportez-vous aux considérations sur les sources de données ODBC.

Les utilisateurs de cette fonctionnalité doivent appartenir à un groupe d'utilisateurs doté de droits *dataaccess* (accès aux données) dans la stratégie par défaut d'accès aux données (dans les stratégies d'accès CALM). Pour plus d'informations sur les stratégies d'accès, reportez-vous au *Manuel d'administration CA Enterprise Log Manager r12.1*.

Pour un client ODBC, les conditions ci-dessous doivent être remplies.

- Vous devez disposer des droits d'administrateur pour installer le client ODBC sur un serveur Windows.
- L'installation du client ODBC nécessite le service Microsoft Windows Installer. Si celui-ci est introuvable, un message s'affiche.
- Configurez le service Serveur ODBC dans CA Enterprise Log Manager et cochez la case Activer le service.
- Configurez une source de données ODBC pour systèmes Windows à l'aide de l'utilitaire Sources de données (ODBC) accessible via le Panneau de configuration.
- Vous devez être habilité à créer des fichiers dans le répertoire d'installation du client sur les systèmes UNIX et Linux.

Pour plus d'informations sur les plates-formes compatibles avec les clients ODBC et JDBC, reportez-vous à la matrice de certification de prise en charge CA Enterprise Log Manager disponible à l'adresse <http://www.ca.com/Support>.

Configuration du service Serveur ODBC

Cette procédure vous permet de configurer un accès ODBC et JDBC au magasin de journaux d'événements CA Enterprise Log Manager.

Pour configurer un accès ODBC et JDBC

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur Administrator.
2. Accédez à l'onglet Administration, puis cliquez sur le sous-onglet Services.

3. Cliquez sur le service Serveur ODBC pour ouvrir les paramètres globaux ou développez le noeud pour sélectionner un serveur CA Enterprise Log Manager.
4. Définissez un numéro de port dans le champ Port du service, si vous souhaitez utiliser un port autre que celui par défaut.
5. Indiquez si vous souhaitez activer SSL pour chiffrer les données transférées entre le client ODBC et le serveur CA Enterprise Log Manager.

Remarque : Les paramètres Port du service et SSL activé doivent être configurés de la même manière sur le serveur et sur le client ODBC. Par défaut, le numéro du port est 17002 et le chiffrement SSL est activé. Si ces paramètres ne correspondent pas à ceux du client ODBC, les tentatives de connexion échouent.

Installation du client ODBC sur les systèmes Windows

Utilisez la procédure suivante pour installer le client ODBC sur un système Windows.

Remarque : Un compte administrateur Windows est nécessaire pour installer le client ODBC.

Pour installer le client ODBC

1. Dans le DVD de l'application ou l'image d'installation, recherchez le répertoire du client ODBC (\CA\ELM\ODBC).
2. Double-cliquez sur l'application setup.exe.
3. Acceptez le contrat de licence et cliquez sur Suivant.
Le panneau Sélection de l'emplacement de destination apparaît.
4. Entrez l'emplacement de destination ou acceptez celui par défaut, puis cliquez sur Suivant.
Le panneau Sélection du dossier de programmes s'affiche.
5. Sélectionnez un dossier pour le programme ou acceptez celui par défaut, puis cliquez sur Suivant.
Le panneau Lancement de la copie des fichiers apparaît.

6. Cliquez sur Suivant pour démarrer la copie des fichiers.

Le panneau Etat d'installation s'affiche pour indiquer l'état d'avancement de l'installation. Lorsque l'installation a terminé de copier les fichiers, le panneau Assistant InstallShield terminé apparaît.

7. Cliquez sur Terminer afin de compléter l'installation.

Création d'une source de données ODBC sur les systèmes Windows

Utilisez cette procédure pour créer la source de données ODBC requise sur les systèmes Windows. Vous pouvez créer la source de données en tant que DSN utilisateur ou DSN système.

Pour créer la source de données

1. Dans le Panneau de configuration Windows, sélectionnez Outils d'administration.
2. Double-cliquez sur l'utilitaire Sources de données (ODBC). La fenêtre Administrateur de sources de données ODBC s'affiche.
3. Cliquez sur Ajouter pour afficher la fenêtre Créer une nouvelle source de données.
4. Sélectionnez Pilote ODBC CA Enterprise Log Manager, puis cliquez sur Terminer.
La fenêtre Installation du pilote ODBC CA Enterprise Log Manager apparaît.
5. Renseignez les champs tel que décrit dans la section sur les considérations sur les sources de données ODBC, puis cliquez sur OK.

Considérations sur les sources de données ODBC

Ci-dessous sont décrits les champs de source de données ODBC en lien avec CA Enterprise Log Manager.

Nom de la source de données

Nom de la source de données en question. Les applications clientes qui souhaitent utiliser ces données utilisent ce nom pour se connecter à la source de données.

Hôte du service

Indique le nom du serveur CA Enterprise Log Manager auquel le client se connecte. Vous pouvez utiliser aussi bien un nom d'hôte qu'une adresse IPv4.

Port du service

Indique le numéro de port du service TCP sur lequel le serveur CA Enterprise Log Manager écoute, pour les connexions au client ODBC. La valeur par défaut est 17002. La valeur que vous définissez ici doit correspondre à celle du service Serveur ODBC, faute de quoi la connexion échoue.

Source de données du service

Laissez ce champ vide, sinon les tentatives de connexion échouent.

Chiffrement SSL

Indique si le chiffrement des communications entre le client et le serveur CA Enterprise Log Manager doit être utilisé. Par défaut, le chiffrement SSL est activé. La valeur que vous définissez ici doit correspondre à celle du service Serveur ODBC, faute de quoi la connexion échoue.

Propriétés personnalisées

Indique les propriétés de connexion à utiliser avec le magasin de journaux d'événements. Les propriétés sont délimitées par un point-virgule, sans espace. Les valeurs par défaut recommandées sont données ci-dessous.

querytimeout

Indique la durée, en seconde, qui doit s'écouler sans qu'aucune donnée ne soit renvoyée avant que la requête soit fermée. Voici la syntaxe utilisée pour cette propriété.

```
querytimeout=300
```

queryfederated

Indique si une requête fédérée doit être exécutée. Si vous définissez cette valeur sur false, la requête est exécutée uniquement sur le serveur CA Enterprise Log Manager avec lequel la connexion à la base de données est établie. Voici la syntaxe utilisée pour cette propriété.

```
queryfederated=true
```

queryfetchrows

Indique le nombre de lignes à récupérer à chaque opération d'extraction, si la requête a réussi. La valeur minimale est 1 et la valeur maximale 5000. La valeur par défaut est 1000. Voici la syntaxe utilisée pour cette propriété.

```
queryfetchrows=1000
```

offsetmins

Indique le décalage horaire correspondant au fuseau horaire du client ODBC. La valeur 0 correspond à l'heure GMT. Utilisez ce champ pour définir votre propre décalage horaire par rapport à l'heure GMT. Voici la syntaxe utilisée pour cette propriété.

```
offsetmins=0
```

suppressNoncriticalErrors

Indique le comportement du fournisseur d'interface en cas d'erreur non critique, par exemple si une base de données ou un hôte ne répond pas.

Voici la syntaxe utilisée pour cette propriété.

```
suppressNoncriticalErrors=false
```

Test de la connexion du client ODBC à la base de données

Le client ODBC est installé à l'aide de l'outil de requête SQL interactif en ligne de commande, iSQL. Vous pouvez utiliser cet outil pour tester les paramètres de configuration et la connectivité entre le client ODBC et le magasin de journaux d'événements CA Enterprise Log Manager.

Pour tester la connexion du client à la base de données

1. Ouvrez une invite de commande et accédez au répertoire où vous voulez installer le client ODBC.
2. Démarrez l'utilitaire iSQL (odbcisql.exe).
3. Entrez la commande suivante pour tester la connexion du client à la base de données.

```
connect Utilisateur*Mot_de_passe@nom_DSN
```

Remplacez nom_DSN par le nom de la source de données que vous avez créée pour cette connexion ODBC à la base de données. Si les paramètres de connexion sont corrects, un message de retour semblable au message ci-dessous s'affiche.

```
SQL: connecting to database: nom_DSN  
Elapsed time 37 ms.
```

Remarque : Si votre mot de passe contient le symbole @, l'utilitaire iSQL ne s'exécutera pas correctement, car il interprète tout élément suivant "@" comme le nom de la source de données. Pour éviter ce problème, placez des apostrophes de part et d'autre du mot de passe :

```
Connect User*"Password"@DSN_name
```

Test de la récupération du serveur à partir de la base de données

Utilisez cette requête de test pour déterminer si une application cliente ODBC est capable de récupérer des données à partir d'un magasin de journaux d'événements CA Enterprise Log Manager via la connexion à la base de données. Cette procédure requiert l'utilisation du même utilitaire iSQL que celui utilisé pour tester la connexion ODBC.

Remarque : Ne copiez pas et n'utilisez pas les requêtes SQL fournies dans les requêtes et les rapports CA Enterprise Log Manager pour tester la connexion ODBC. Ces instructions SQL sont destinées uniquement à être utilisées par le serveur CA Enterprise Log Manager avec le magasin de journaux d'événements. Créez vos requêtes SQL ODBC conformément à la norme SQL ANSI.

Pour tester la récupération des données du serveur

1. Ouvrez une invite de commande et accédez au répertoire où vous voulez installer le client ODBC.
2. Démarrez l'utilitaire iSQL (odbcisql.exe).
3. Entrez l'instruction SELECT suivante pour tester la récupération à partir du magasin de journaux d'événements.

```
select top 5 event_logname, receiver_hostname, SUM(event_count) as Count from  
view_event where event_time_gmt < now() and event_time_gmt >  
timestampadd(mi,-15,now()) GROUP BY receiver_hostname, event_logname;
```

Installation du client JDBC

Le client JDBC offre via n'importe quel applet, application ou serveur d'applications Java un accès JDBC multiniveau point à point hautes performances aux sources de données. Le client est optimisé pour l'environnement Java, ce qui vous permet d'intégrer la technologie Java et d'étendre les fonctionnalités et les performances de votre système.

Le client JDBC peut être exécuté aussi bien sur les plates-formes 32 bits que 64 bits. Aucune modification des applications existantes n'est requise pour qu'elles s'exécutent sur les plates-formes 64 bits.

L'installation du client JDBC comprend les étapes ci-dessous.

1. Assurez-vous qu'un serveur d'applications Web avec possibilités de configuration des pools de connexions est installé et fonctionne correctement.
2. Obtenez la clé de licence pour le pilote du client JDBC.
3. Installez le client JDBC.
4. Configurez la connexion à la base de données en utilisant les fonctions de gestion de pool de connexions de votre serveur d'applications Web.
5. Testez la connexion à la base de données.

Configuration requise pour le client JDBC

L'accès JDBC au magasin de journaux d'événements est disponible uniquement avec CA Enterprise Log Manager r12.1 et versions ultérieures. Vous pouvez installer le client JDBC sur des systèmes Windows ou UNIX.

Les utilisateurs de cette fonctionnalité doivent appartenir à un groupe d'utilisateurs CA Enterprise Log Manager doté de droits *dataaccess* (accès aux données) dans la stratégie par défaut d'accès aux données (dans les stratégies d'accès CALM). Pour plus d'informations sur les stratégies d'accès, reportez-vous au *Manuel d'administration de CA Enterprise Log Manager r12.1*.

Pour un client JDBC, les conditions ci-dessous doivent être remplies.

- Vous devez disposer des droits d'administrateur pour installer le client JDBC sur un serveur Windows.
- Dans la fenêtre de configuration du serveur ODBC, assurez-vous que la case Activer le service est cochée.
- Vous devez être habilité à créer des fichiers dans le répertoire d'installation du client sur les systèmes UNIX et Linux.
- Pour les applications qui s'exécutent sous J2SE v 1.4.2.x, configurez les connexions à la base de données par programmation, comme défini dans une application spécifique.
- Pour les applications qui s'exécutent sous J2EE 1.4.2.x et versions ultérieures, utilisez un serveur d'applications Web (par exemple, Oracle WebLogic ou Red Hat JBoss) pour configurer la gestion des pools de connexion.

Pour plus d'informations sur les plates-formes compatibles avec les clients ODBC et JDBC, reportez-vous à la matrice de certification de prise en charge CA Enterprise Log Manager disponible à l'adresse <http://www.ca.com/Support>.

Installation du client JDBC sur les systèmes Windows

Utilisez cette procédure pour installer le pilote du client JDBC sur un système Windows.

Pour installer le pilote JDBC

1. Recherchez dans le répertoire CA/ELM/JDBC du DVD de l'application ou de l'image d'installation les deux fichiers .jar suivants.

LMjc.jar
LMssl14.jar

2. Copiez les fichiers .jar dans le répertoire de votre choix sur le serveur de destination, et notez cet emplacement.

Installation du client JDBC sur les systèmes UNIX

Utilisez cette procédure pour installer le pilote du client JDBC sur un système UNIX.

Pour installer le pilote JDBC

1. Recherchez dans le répertoire CA/ELM/JDBC du DVD de l'application ou de l'image d'installation les deux fichiers .jar suivants.

LMjc.jar
LMssl14.jar

2. Copiez les fichiers .jar dans le répertoire de votre choix sur le serveur de destination, et notez cet emplacement.
3. Pour JDBC sous UNIX, exécutez manuellement la commande ci-dessous, ou une commande similaire, à partir du répertoire d'installation, une fois le client JDBC installé.

```
chmod -R ugo+x emplacement_fichier
```

Remplacez *emplacement_fichier* par le répertoire d'installation du client JDBC. Cette étape vous permet d'exécuter les scripts shell fournis avec le client installé.

Paramètres de connexion JDBC

Certaines applications nécessitent des paramètres de connexion particuliers pour utiliser le pilote du client JDBC. Les paramètres courants sont les suivants.

- Chaîne ou URL de connexion
- Nom de classe

Le format de la chaîne ou de l'URL de connexion JDBC est le suivant.

```
jdbc:ca-elm://[CA-ELM_host_name]:[ODBC/JDBCport];ServerDataSource=Default;
```

Le nom de classe du pilote JDBC est :

```
com.ca.jdbc.openaccess.OpenAccessDriver
```

Considérations sur les URL JDBC

Pour accéder aux données d'événements stockées dans CA Enterprise Log Manager avec le client JDBC, vous avez besoin du chemin de classes JDBC et d'une URL JDBC. Le chemin de classes JDBC correspond aux emplacements des fichiers JAR du pilote. L'URL JDBC définit les paramètres utilisés par les classes des fichiers JAR lors du chargement.

Voici un exemple d'URL JDBC complète.

```
jdbc:ca-elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

Les différentes parties de l'URL sont expliquées ci-dessous.

jdbc:ca-elm:

Définit la chaîne protocole:sous-protocole qui désigne le pilote JDBC fourni avec CA Enterprise Log Manager.

//adresse IP:port;

Indique l'adresse IP du serveur CA Enterprise Log Manager auquel vous voulez accéder. Le numéro de port correspond au port à utiliser pour les communications ; il doit être identique à celui défini dans le panneau de configuration du service ODBC CA Enterprise Log Manager. Si les numéros de port sont différents, la tentative de connexion échoue.

encrypted=0|1;

Indique si le chiffrement SSL est utilisé pour les communications entre le client JDBC et le serveur CA Enterprise Log Manager. La valeur par défaut est 0 (pas de chiffrement) ; il n'est pas nécessaire de la préciser dans l'URL. Pour activer le chiffrement, spécifiez encrypted=1 dans l'URL. Le chiffrement de la connexion doit être activé explicitement. De plus, ce paramètre doit correspondre à celui que vous avez configuré dans la boîte de dialogue Service ODBC CA Enterprise Log Manager, faute de quoi la tentative de connexion échoue.

ServerDataSource=Default

Spécifie le nom de la source de données. Définissez cette valeur sur *Default* pour accéder au magasin de journaux d'événements CA Enterprise Log Manager.

CustomProperties=(x;y;z)

Ces propriétés sont identiques aux propriétés ODBC personnalisées. Si vous ne les spécifiez pas explicitement, les valeurs par défaut de l'exemple d'URL sont appliquées.

Informations complémentaires

[Considérations sur les sources de données ODBC](#) (page 120)

Dépannage de l'installation

Vous pouvez examiner les fichiers journaux d'installation ci-dessous pour commencer à dépanner votre installation.

Produit	Emplacement du fichier journal
CA Enterprise Log Manager	/tmp/pre-install_ca-elm.log /tmp/install_ca-elm.<horodatage>.log /tmp/install_ca-elmagent.<horodatage>.log
CA Embedded Entitlements Manager	/opt/CA/SharedComponents/EmbeddedIAM/eiam-install.log
CA Directory	/tmp/etrdir_install.log

L'installation de CA Enterprise Log Manager copie les fichiers de contenu et autres sur le serveur CA EEM à des fins de gestion. Du point de vue du serveur CA EEM, les rapports et autres fichiers CA Enterprise Log Manager sont *importés*. Si l'installation ne peut pas se connecter au serveur CA EEM, l'installation de CA Enterprise Log Manager se poursuit sans importer les fichiers de contenu. Vous pouvez importer les fichiers de contenu manuellement une fois l'installation terminée.

Si vous rencontrez des erreurs lors de l'installation, il est possible que vous souhaitiez effectuer une ou plusieurs actions ci-dessous pour achever votre installation. Chacune de ces actions implique de se connecter au serveur CA Enterprise Log Manager à l'aide du compte par défaut, caelmadmin, puis de passer à l'utilisateur root.

- Résoudre une erreur de configuration de l'interface réseau
- Vérifier que le package RPM est installé
- Vérifier que le démon iGateway s'exécute
- Enregistrer l'application CA Enterprise Log Manager auprès du serveur CA EEM
- Obtenir des certificats numériques
- Importer des rapports CA Enterprise Log Manager
- Importer des fichiers de mappage de données
- Importer des fichiers d'analyse de message
- Importer des fichiers de grammaire commune aux événements (CEG)
- Importer des fichiers de gestion commune des agents.

Résoudre une erreur de configuration de l'interface réseau

Après l'installation, si vous ne parvenez pas à accéder à l'interface utilisateur du serveur CA Enterprise Log Manager, vous rencontrez peut-être une erreur de configuration de l'interface réseau. Vous avez deux options pour résoudre l'erreur.

- Débranchez le câble réseau physique et branchez-le sur un autre port.
- Reconfigurez les adaptateurs logiques de l'interface réseau à partir d'une ligne de commande.

Pour reconfigurer les ports d'adaptateurs réseau à partir d'une ligne de commande

1. Connectez-vous au dispositif logiciel en tant qu'utilisateur caelmadmin et accédez à une invite de commande.
2. Basculez sur le compte d'utilisateur root à l'aide de la commande ci-dessous.

```
su -
```

3. Entrez le mot de passe de l'utilisateur root pour confirmer l'accès au système.

4. Entrez la commande suivante.

```
system-config-network
```

L'interface utilisateur permettant de configurer les adaptateurs réseau s'affiche.

5. Paramétrez les configurations de ports comme vous le souhaitez et quittez l'interface.
6. Redémarrez les services réseau à l'aide de la commande ci-après pour que vos modifications prennent effet.

```
service network restart
```

Vérifier que le package RPM est installé

Vous pouvez effectuer un contrôle rapide de l'installation en vérifiant que le package RPM adéquat est installé.

Pour vérifier le package RPM

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.
4. Vérifiez que le package ca-elm-<version>.i386.rpm est installé à l'aide des commandes ci-après.

```
su - root
```

```
rpm -q ca-elm  
rpm -q ca-elmagent
```

Le système d'exploitation renvoie le nom complet du package s'il est installé.

Enregistrement du serveur CA Enterprise Log Manager auprès du serveur CA EEM

Symptôme :

Lors de l'installation, l'application CA Enterprise Log Manager ne s'est pas enregistrée correctement auprès du serveur CA EEM. L'application CA Enterprise Log Manager dépend du serveur CA EEM pour la gestion des comptes d'utilisateur et des configurations de services. Si l'application CA Enterprise Log Manager n'est pas enregistrée, le logiciel ne fonctionne pas correctement.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Enregistrez manuellement l'application CA Enterprise Log Manager auprès du serveur CA EEM.

Pour enregistrer l'application CA Enterprise Log Manager

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire /opt/CA/LogManager/EEM.
5. Exécutez la commande ci-dessous.

```
./EEMRegister.sh
```

Le script shell enregistre l'application CA Enterprise Log Manager auprès du serveur CA EEM.

Acquisition de certificats auprès du serveur CA EEM

Symptôme :

Lors de l'installation, les certificats numériques n'ont pas été correctement acquis auprès du serveur CA EEM. Les certificats numériques sont nécessaires pour démarrer et exécuter l'application CA Enterprise Log Manager.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Effectuez une acquisition manuelle des certificats auprès du serveur CA EEM.

Pour acquérir les certificats numériques

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire `/opt/CA/LogManager/EEM`.
5. Exécutez la commande ci-dessous.

```
./EEMAcqCert.sh
```

Le script shell effectue le traitement requis pour acquérir les certificats numériques nécessaire.

Importation de rapports CA Enterprise Log Manager

Symptôme :

Lors de l'installation, le serveur CA EEM n'a pas importé correctement le contenu des rapports depuis le serveur CA EEM. Vous devez importer le contenu des rapports pour afficher les données d'événement après les avoir placées dans le magasin de journaux d'événements.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Importez manuellement le contenu des rapports.

Pour importer le contenu des rapports

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. Passez à l'utilisateur `root` au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire `/opt/CA/LogManager/EEM/content`.
5. Exécutez la commande ci-dessous.

```
./ImportCALMContent.sh
```

Le script shell télécharge le contenu des rapports depuis le serveur CA EEM.

Importation de fichiers de mappage de données CA Enterprise Log Manager

Symptôme :

Lors de l'installation, le serveur CA EEM n'a pas importé correctement les fichiers de mappage de données. Vous devez disposer des fichiers de mappage de données pour mapper les données d'événements entrants dans le magasin de journaux d'événements.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Importez manuellement les fichiers de mappage de données.

Pour importer les fichiers de mappage de données

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire /opt/CA/LogManager/EEM/content.
5. Exécutez la commande ci-dessous.

```
./ImportCALMDM.sh
```

Le script shell importe les fichiers de mappage de données depuis le serveur CA EEM.

Importation de fichiers de grammaire commune aux événements

Symptôme :

Lors de l'installation, le serveur CA EEM n'a pas importé correctement les fichiers de grammaire commune aux événements (CEG). La CEG forme le schéma de base de données sous-jacent pour le magasin de journaux d'événements. Vous ne pouvez pas stocker d'événements dans le magasin de journaux d'événements CA Enterprise Log Manager dans les fichiers CEG.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Importez manuellement les fichiers CEG.

Pour importer les fichiers CEG

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire /opt/CA/LogManager/EEM/content.
5. Exécutez la commande ci-dessous.

```
./ImportCALMCEG.sh
```

Le script shell importe les fichiers de grammaire commune aux événements.

Importation de fichiers de règles de corrélation

Symptôme :

Lors de l'installation, le serveur CA EEM n'a pas importé correctement les fichiers de règles de corrélation. Les règles de corrélation permettent d'identifier des modèles d'événements qui doivent être examinés. Vous pouvez importer des groupes ou des règles de corrélation.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Importez les fichiers de règles de corrélation manuellement.

Pour importer des fichiers de règles de corrélation :

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire `/opt/CA/LogManager/EEM/content`.
5. Exécutez l'une des commandes ci-après :

```
./ImportCALMCorrelationGroups.sh
```

Le script shell permet d'importer des groupes de règles de corrélation.

```
./ImportCALMCorrelationRules.sh
```

Le script shell permet d'importer les fichiers de règles de corrélation.

Importation de fichiers de gestion commune des agents

Symptôme :

Lors de l'installation, le serveur CA EEM n'a pas importé correctement les fichiers de gestion commune des agents. Vous ne pouvez pas gérer les agents dans l'interface utilisateur CA Enterprise Log Manager sans ces fichiers.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Importez manuellement les fichiers de gestion des agents.

Pour importer des fichiers de gestion commune des agents

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. Passez à l'utilisateur `root` au moyen de la commande ci-dessous.

```
su -
```
4. Accédez au répertoire `/opt/CA/LogManager/EEM/content`.
5. Exécutez la commande ci-dessous.

```
./ImportCALMAgentContent.sh
```

Le script shell importe les fichiers de gestion commune des agents.

Importation de fichiers de configuration CA Enterprise Log Manager

Symptôme :

Lors de l'installation, le serveur CA EEM n'a pas importé correctement les fichiers de configuration. Vous pouvez démarrer CA Enterprise Log Manager, mais il manque certains paramètres et certaines valeurs dans les zones de configuration des services, et vous ne pouvez pas configurer de manière centralisée les hôtes sans ces fichiers.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Importez manuellement les fichiers de configuration.

Pour importer les fichiers de configuration

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire `/opt/CA/LogManager/EEM/content`.
5. Exécutez la commande ci-dessous.

```
./ImportCALMConfig.sh
```

Le script shell importe les fichiers de configuration.

Importation des fichiers de suppression et de récapitulation

Symptôme :

Lors de l'installation, le serveur CA EEM n'a pas importé correctement les fichiers de suppression et de récapitulation. Vous ne pouvez pas utiliser les règles de suppression et de récapitulation prêtes à l'emploi dans l'interface utilisateur CA Enterprise Log Manager sans ces fichiers.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Importez manuellement les fichiers de suppression et de récapitulation.

Pour importer les fichiers de suppression et de récapitulation

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire /opt/CA/LogManager/EEM/content.
5. Exécutez la commande ci-dessous.

```
./ImportCALMSAS.sh
```

Le script shell importe les fichiers de suppression et de récapitulation.

Importation des fichiers de jetons d'analyse

Symptôme :

Lors de l'installation, le serveur CA EEM n'a pas importé correctement les fichiers de jetons d'analyse. Vous ne pouvez pas utiliser les jetons d'analyse prêts à l'emploi dans l'assistant d'analyse de message sans ces fichiers.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Importez manuellement les fichiers de jetons d'analyse.

Pour importer des fichiers de jetons d'analyse

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire /opt/CA/LogManager/EEM/content.
5. Exécutez la commande ci-dessous.

```
./ImportCALMTOK.sh
```

Le script shell importe les fichiers de jetons d'analyse.

Importation des fichiers de l'interface utilisateur CA Enterprise Log Manager

Symptôme :

Lors de l'installation, le serveur CA EEM n'a pas importé correctement les fichiers de l'interface utilisateur. Vous ne pouvez pas afficher ou utiliser les valeurs des champs déroulants de la plage de temps dynamique sans ces fichiers.

Le script shell mentionné dans la procédure qui suit est copié automatiquement dans le répertoire nommé lors de l'installation.

Solution :

Importez manuellement les fichiers de l'interface utilisateur.

Pour importer les fichiers de l'interface utilisateur

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. Passez à l'utilisateur root au moyen de la commande ci-dessous.

```
su -
```

4. Accédez au répertoire /opt/CA/LogManager/EEM/content.
5. Exécutez la commande ci-dessous.

```
./ImportCALMFlexFiles.sh
```

Le script shell importe les fichiers de l'interface utilisateur.

Chapitre 4 : Configuration des utilisateurs de base et des accès

Ce chapitre traite des sujets suivants :

[A propos des utilisateurs de base et des accès](#) (page 139)

[Configuration du magasin d'utilisateurs](#) (page 140)

[Configuration des stratégies de mots de passe](#) (page 144)

[Conservation des stratégies d'accès prédéfinies](#) (page 145)

[Création du premier administrateur](#) (page 146)

A propos des utilisateurs de base et des accès

La configuration commence par le paramétrage du magasin d'utilisateurs, la création d'un ou plusieurs utilisateurs doté du rôle Administrator prédéfini et la configuration des stratégies de mots de passe. En général, cette configuration est réalisée par l'installateur, qui peut se connecter à CA Enterprise Log Manager avec les informations d'identification EiamAdmin. Une fois cette configuration terminée, les utilisateurs définis comme des administrateurs configurent CA Enterprise Log Manager.

Si la configuration du magasin d'utilisateurs par défaut est acceptée, la configuration minimale devant être atteinte par l'utilisateur EiamAdmin est le compte pour le premier administrateur. Le premier administrateur peut configurer des stratégies de mots de passe avant de configurer les autres composants CA Enterprise Log Manager.

Remarque : Pour plus de détails sur la création d'autres utilisateurs ou sur la création de rôles personnalisés et de stratégies d'accès personnalisées, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Configuration du magasin d'utilisateurs

Le magasin d'utilisateurs est le référentiel des informations générales des utilisateurs. Vous pouvez configurer le magasin d'utilisateurs dès que vous installez un serveur CA Enterprise Log Manager. Seul l'utilisateur EiamAdmin peut configurer le magasin d'utilisateurs, immédiatement après la première connexion en général.

Configurez le magasin d'utilisateurs de l'une des manières ci-dessous.

- Acceptez l'option par défaut : Stocker dans le magasin de données internes.

Remarque : L'option par défaut peut être affichée comme la base de données de gestion CA si, lors de l'installation, vous avez pointé vers un CA EEM autonome.

- Sélectionnez Référencer à partir d'un répertoire externe, qui peut être un répertoire LDAP comme Microsoft Active Directory, Sun One ou Novell CA Directory.
- Sélectionnez Référencer à partir de CA SiteMinder.

Si vous configurez le magasin d'utilisateurs comme un répertoire externe, vous ne pouvez pas créer de nouveaux utilisateurs. Vous pouvez uniquement ajouter des groupes d'applications, ou rôles, prédéfinis ou définis par l'utilisateur aux enregistrements d'utilisateurs globaux en lecture seule. Vous devez ajouter les nouveaux utilisateurs dans le magasin d'utilisateurs externe, puis ajouter les droits CA Enterprise Log Manager aux enregistrements d'utilisateurs globaux.

Acceptation du magasin d'utilisateurs par défaut

Vous n'avez pas besoin de configurer le magasin d'utilisateurs si vous acceptez le magasin par défaut, à savoir le magasin de données interne. Cela s'applique s'il n'existe aucun magasin d'utilisateurs externe auquel faire référence.

Pour vérifier que le référentiel par défaut est configuré comme le magasin d'utilisateurs

1. Connectez-vous à un serveur CA Enterprise Log Manager en tant qu'utilisateur doté des droits Administrator ou avec le nom d'utilisateur EiamAdmin et le mot de passe associé.
2. Cliquez sur l'onglet Administration.

Si vous vous connectez en tant qu'utilisateur EiamAdmin, cet onglet s'affiche automatiquement.

3. Sélectionnez le sous-onglet Gestion des utilisateurs et des accès, puis cliquez sur le bouton Magasin d'utilisateurs dans le volet gauche.
La configuration du serveur EEM pour les utilisateurs globaux/groupes globaux s'affiche.
4. Vérifiez que l'option Stocker dans le magasin de données internes est sélectionnée.
5. Cliquez sur Enregistrer, puis sur Fermer.

Remarque : Lorsque le magasin d'utilisateurs par défaut est défini, vous pouvez créer de nouveaux utilisateurs, définir des mots de passe temporaires et établir des stratégies de mots de passe.

Informations complémentaires :

[Planification du magasin d'utilisateurs](#) (page 42)

Référence à un répertoire LDAP

Configurez le magasin d'utilisateurs comme une référence à un répertoire LDAP lorsque les détails des utilisateurs globaux sont stockés dans Microsoft Active Directory, Sun One ou Novell Directory.

Remarque : Les détails des applications sont stockés dans le référentiel par défaut. La référence à un magasin d'utilisateurs externe ne met pas à jour ce magasin.

Pour référencer un répertoire LDAP en tant que magasin d'utilisateurs

1. Connectez-vous à un serveur CA Enterprise Log Manager en tant qu'utilisateur doté des droits d'administrateur ou qu'utilisateur EiamAdmin.
2. Cliquez sur l'onglet Administration.
Si vous vous connectez en tant qu'utilisateur EiamAdmin, cet onglet s'affiche automatiquement.
3. Sélectionnez le sous-onglet Gestion des utilisateurs et des accès, puis cliquez sur Magasin d'utilisateurs dans le volet gauche.
La configuration du serveur CA EEM pour le magasin d'utilisateurs s'affiche.
4. Sélectionnez Référencer à partir d'un répertoire externe.
Les champs de la configuration LDAP s'affichent.

5. Renseignez ces champs en fonction de la feuille de calcul du répertoire externe.

Étudiez l'exemple ci-dessous pour la liaison vers les objets Active Directory, avec la chaîne de liaison ci-dessous.

Définissez objUser = Get Object ("LDAP://cn=Bob, cn=Users, ou=Sales, dc=MyDomain, dc=com"), où cn est le nom commun, ou est l'unité organisationnelle et dc est constitué de deux composants de domaine formant le nom DNS complet. Pour le DN utilisateur, vous pouvez entrer :

```
cn=Bob, cn=Users, ou=Sales, dc=MyDomain, dc=com.
```

6. Cliquez sur Enregistrer.

L'enregistrement de cette référence charge les informations des comptes d'utilisateur dans CA EEM. Vous pouvez alors accéder à ces enregistrements d'utilisateur comme s'il s'agissait d'utilisateurs globaux, puis ajouter des détails au niveau de l'application, comme le groupe d'utilisateurs de l'application et le nom du rôle d'utilisateur.

7. Examinez l'état affiché pour vérifier que la liaison vers le répertoire externe est effective et que les données sont chargées.

Si l'état affiche un avertissement, cliquez sur Actualiser l'état. Si l'état affiche une erreur, corrigez la configuration, cliquez sur Enregistrer et réitérez cette étape.

8. Cliquez sur Fermer.

Informations complémentaires :

[Planification du magasin d'utilisateurs](#) (page 42)

[Feuille de calcul du répertoire LDAP externe](#) (page 44)

Référence à CA SiteMinder comme magasin d'utilisateurs

Si vos comptes d'utilisateur sont déjà définis sur CA SiteMinder, référez ce répertoire externe lorsque vous configurez le magasin d'utilisateurs.

Pour référencer CA SiteMinder comme magasin d'utilisateurs

1. Connectez-vous à un serveur CA Enterprise Log Manager en tant qu'utilisateur doté des droits d'administrateur ou qu'utilisateur EiamAdmin.
2. Cliquez sur l'onglet Administration.

Si vous vous connectez en tant qu'utilisateur EiamAdmin, cet onglet s'affiche automatiquement.

3. Sélectionnez le sous-onglet Gestion des utilisateurs et des accès, puis cliquez sur le bouton Magasin d'utilisateurs dans le volet gauche.

La configuration du serveur CA EEM pour le magasin d'utilisateurs s'affiche.

4. Sélectionnez l'option Référencer à partir de CA SiteMinder.

Les champs spécifiques à CA SiteMinder s'affichent.

- a. Renseignez ces champs en fonction de la feuille de calcul SiteMinder.
- b. Pour afficher ou modifier les connexions et les ports utilisés par CA SiteMinder, cliquez sur les points de suspension pour afficher le panneau Attributs de connexion.

5. Cliquez sur Enregistrer.

L'enregistrement de cette référence charge les informations des comptes d'utilisateur dans CA EEM. Vous pouvez alors accéder à ces enregistrements d'utilisateur comme s'il s'agissait d'utilisateurs globaux, puis ajouter des détails au niveau de l'application, comme le groupe d'utilisateurs de l'application et le nom du rôle d'utilisateur.

6. Examinez l'état affiché pour vérifier que la liaison vers le répertoire externe est effective et que les données sont chargées.

Si l'état affiche un avertissement, cliquez sur Actualiser l'état. Si l'état affiche une erreur, corrigez la configuration, cliquez sur Enregistrer et réitérez cette étape.

7. Cliquez sur Fermer.

Informations complémentaires :

[Planification du magasin d'utilisateurs](#) (page 42)

[Feuille de calcul CA SiteMinder](#) (page 46)

Configuration des stratégies de mots de passe

Vous pouvez définir des stratégies de mots de passe pour vous assurer que les mots de passe créés par les utilisateurs pour eux-mêmes répondent aux normes établies et qu'ils sont modifiés selon la fréquence définie. Définissez des stratégies de mots de passe après avoir configuré le magasin d'utilisateurs interne. Seul l'utilisateur EiamAdmin ou un utilisateur disposant du rôle Administrator peut définir ou modifier des stratégies de mots de passe.

Remarque : Les stratégies de mots de passe CA Enterprise Log Manager ne s'appliquent pas aux comptes d'utilisateur créés dans un magasin d'utilisateurs externe.

Pour configurer des stratégies de mots de passe

1. Connectez-vous à un serveur CA Enterprise Log Manager en tant qu'utilisateur doté des droits Administrator ou qu'utilisateur EiamAdmin.
2. Cliquez sur l'onglet Administration.
Si vous vous connectez en tant qu'utilisateur EiamAdmin, cet onglet s'affiche automatiquement.
3. Sélectionnez le sous-onglet Gestion des utilisateurs et des accès, puis cliquez sur le bouton Stratégies de mots de passe dans le volet gauche.
Le panneau Stratégies de mots de passe s'affiche.
4. Spécifiez si vous souhaitez permettre les mots de passe identiques aux noms d'utilisateur.
5. Spécifiez si vous souhaitez appliquer des restrictions de longueur.
6. Spécifiez si vous souhaitez appliquer des stratégies sur le nombre maximum de caractères répétés ou sur le nombre minimum de caractères numériques.
7. Spécifiez des stratégies d'ancienneté et de réutilisation.
8. Vérifiez vos paramètres, puis cliquez sur Enregistrer.
9. Cliquez sur Fermer.

Les stratégies de mots de passe configurées s'appliquent à tous les utilisateurs CA Enterprise Log Manager.

Informations complémentaires :

[Planification de la stratégie de mots de passe](#) (page 47)

[Nom d'utilisateur comme mot de passe](#) (page 48)

[Ancienneté et réutilisation du mot de passe](#) (page 49)

[Longueur et format du mot de passe](#) (page 49)

Conservation des stratégies d'accès prédéfinies

Si vous prévoyez d'utiliser uniquement les groupes d'utilisateurs d'applications prédéfinis, ou rôles, avec les stratégies prédéfinies associées, il peut y avoir un petit risque de suppression ou de corruption des stratégies prédéfinies. Toutefois, si vos administrateurs prévoient de créer des rôles définis par l'utilisateur et des stratégies d'accès associées, les stratégies prédéfinies seront accessibles, modifiables et vulnérables aux modifications non souhaitées. Mieux vaut alors conserver une sauvegarde des stratégies prédéfinies d'origine, que vous pouvez restaurer le cas échéant.

Créez un fichier de sauvegarde contenant chaque type de stratégie prédéfinie à l'aide de la fonction Exporter. Vous pouvez copier ces fichiers sur un média externe ou les laisser sur le disque du serveur sur lequel l'exportation a été réalisée.

Remarque : Pour connaître les procédures de sauvegarde des stratégies prédéfinies, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Création du premier administrateur

Le premier utilisateur créé doit se voir affecter le rôle Administrator. Seuls les utilisateurs affichant le rôle Administrator peuvent effectuer la configuration. Vous pouvez affecter un rôle Administrator à un nouveau compte d'utilisateur que vous créez ou à un compte d'utilisateur existant, récupéré dans CA Enterprise Log Manager.

Utilisez le processus ci-dessous.

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur par défaut EiamAdmin.
2. Créez le premier administrateur.

La méthode utilisée pour créer le premier administrateur CA Enterprise Log Manager dépend de votre configuration de magasin d'utilisateurs.

- Si vous configurez CA Enterprise Log Manager pour qu'il utilise le magasin d'utilisateurs interne, vous créez un nouveau compte d'utilisateur avec le rôle Administrator.
- Si vous configurez CA Enterprise Log Manager pour qu'il utilise un magasin d'utilisateurs externe, vous utilisez un utilisateur LDAP existant pour le lier au répertoire. Une fois le lien avec un répertoire externe établi, vous récupérez, à partir du magasin d'utilisateurs externe, le compte de l'utilisateur auquel vous souhaitez affecter un rôle CA Enterprise Log Manager. Les comptes d'utilisateur provenant de magasins d'utilisateurs externes sont récupérés sous forme d'utilisateurs globaux. Vous ne pouvez pas modifier les informations des comptes d'utilisateur existants, mais vous pouvez ajouter un nouveau groupe d'utilisateurs d'applications (ou rôle) CAELM. Vous affectez le rôle Administrator au premier utilisateur.

Remarque : Vous ne pouvez pas créer de nouveaux utilisateurs à partir de CA Enterprise Log Manager si vous configurez un magasin d'utilisateurs externe.

3. Déconnectez-vous du serveur CA Enterprise Log Manager.
4. Reconnectez-vous au serveur CA Enterprise Log Manager avec les informations d'identification du nouveau compte d'utilisateur.

Vous êtes désormais prêt à effectuer les tâches de configuration.

Création d'un nouveau compte d'utilisateur

Vous pouvez créer un compte d'utilisateur pour chaque personne qui va utiliser CA Enterprise Log Manager. Vous fournissez les informations d'identification avec lesquelles l'utilisateur doit se connecter pour la première fois et vous spécifiez son rôle. Les trois rôles prédéfinis sont Administrator, Analyst et Auditor. Lorsqu'un nouvel utilisateur affichant un rôle Analyst ou Auditor se connecte, CA Enterprise Log Manager authentifie l'utilisateur grâce aux informations d'identification enregistrées et autorise l'utilisation de diverses fonctionnalités en fonction du rôle affecté.

Pour créer un utilisateur

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur par défaut EiamAdmin.
L'onglet Administration et le sous-onglet Gestion des utilisateurs et des accès s'affichent.
2. Cliquez sur Utilisateurs dans le volet gauche.
3. Cliquez sur Nouvel utilisateur, à gauche du dossier Utilisateurs.
L'écran des détails du nouvel utilisateur s'affiche du côté droit de la fenêtre.
4. Saisissez un nom d'utilisateur dans le champ Nom. Les noms d'utilisateurs ne sont pas sensibles à la casse.
5. Cliquez sur Ajouter les détails de l'utilisateur de l'application.
6. Sélectionnez le rôle associé aux tâches que doit effectuer cet utilisateur. Utilisez le contrôle de déplacement pour le déplacer vers la liste Groupes d'utilisateurs sélectionnés.
7. Indiquez des valeurs pour les champs restants dans l'écran selon vos besoins. Vous devez indiquer un mot de passe sensible à la casse avec une confirmation dans la zone du groupe d'authentification.
8. Cliquez sur Enregistrer, puis sur Fermer.

Informations complémentaires :

[Affectation d'un rôle à un utilisateur global](#) (page 148)

Affectation d'un rôle à un utilisateur global

Vous pouvez rechercher un compte d'utilisateur existant et affecter le groupe d'utilisateurs d'applications pour le rôle que l'individu doit endosser. Si vous faites référence à un magasin d'utilisateurs externe, la recherche renvoie les enregistrements globaux chargés depuis ce magasin d'utilisateurs. Si votre magasin d'utilisateurs configuré est le magasin d'utilisateurs CA Enterprise Log Manager, la recherche renvoie les enregistrements créés pour les utilisateurs dans CA Enterprise Log Manager.

Seuls les administrateurs peuvent modifier des comptes d'utilisateurs.

Pour affecter un rôle, ou groupe d'utilisateurs d'applications, à un utilisateur existant

1. Cliquez sur l'onglet Administration et sur le sous-onglet Gestion des utilisateurs et des accès.

2. Cliquez sur Utilisateurs dans le volet gauche.

Les volets Recherche d'utilisateurs et Utilisateurs apparaissent.

3. Sélectionnez Utilisateurs globaux, entrez des critères de recherche et cliquez sur OK.

Si la recherche porte sur les comptes d'utilisateurs chargés, le volet Utilisateurs affiche le chemin d'accès et les étiquettes de chemin d'accès reflètent le répertoire externe référencé.

Important : Entrez toujours des critères lors des recherches pour éviter d'afficher toutes les entrées d'un magasin d'utilisateurs externe.

4. Sélectionnez un utilisateur global n'ayant aucune appartenance à un groupe d'applications CA Enterprise Log Manager.

La page Utilisateur s'affiche avec le nom du dossier, les détails de l'utilisateur global et, le cas échéant, l'appartenance à un groupe global.

5. Cliquez sur Ajouter les détails de l'utilisateur de l'application.

Le volet des détails de l'utilisateur "CAELM" se développe.

6. Sélectionnez le groupe souhaité dans la liste des groupes d'utilisateurs disponibles et cliquez sur la flèche de droite.

Le groupe sélectionné apparaît dans la zone Groupes d'utilisateurs sélectionnés.

7. Cliquez sur Enregistrer.

8. Vérifiez l'ajout.
 - a. Dans le volet Recherche d'utilisateurs, cliquez sur Détails de l'utilisateur de l'application, puis sur OK.
 - b. Vérifiez que le nom du nouvel utilisateur de l'application apparaît bien dans les résultats affichés.
9. Cliquez sur Fermer.

Chapitre 5 : Configuration des services

Ce chapitre traite des sujets suivants :

[Sources d'événement et configurations](#) (page 151)

[Modification de configurations globales](#) (page 152)

[Utilisation des Paramètres et filtres globaux](#) (page 155)

[Configuration du magasin de journaux d'événements](#) (page 157)

[Configuration du service de corrélation](#) (page 184)

[Remarques sur le service d'incidents](#) (page 195)

[Remarques sur le serveur ODBC](#) (page 196)

[Remarques sur le serveur de rapports](#) (page 197)

[Configuration de l'abonnement](#) (page 198)

Sources d'événement et configurations

La plupart des réseaux disposent de périphériques Windows et de périphériques Syslog dont les journaux d'événements doivent être collectés, stockés, surveillés et audités. Votre réseau peut également disposer d'autres types de périphériques, notamment des applications, des bases de données, des lecteurs de badges, des unités biométriques ou des enregistreurs et iRecorders CA Audit. Les services, adaptateurs, agents et connecteurs CA Enterprise Log Manager représentent les configurations nécessaires pour se connecter à ces sources d'événement afin de recevoir des données d'événement.

Les services CA Enterprise Log Manager incluent les éléments ci-dessous pour les configurations et les paramètres.

- Configurations globales
- Paramètres et filtres globaux
- Service d'alertes
- Service de corrélation
- Paramètres du magasin de journaux d'événements

- Service d'incidents
- Paramètres du serveur ODBC
- Paramètres du serveur de rapports
- Service de tests de règles
- Configuration du service d'abonnement
- Panneau Etat du système

Les configurations des services peuvent être globales, c'est-à-dire qu'elles affectent tous les serveurs CA Enterprise Log Manager installés sous un seul nom d'instance d'application sur le serveur de gestion. Les configurations peuvent également être locales et n'affecter qu'un serveur sélectionné. Les configurations sont stockées dans le serveur de gestion, avec une copie locale sur le serveur CA Enterprise Log Manager de collecte. Ainsi, si le réseau perd sa connectivité ou si le serveur de gestion s'arrête pour une raison quelconque, la journalisation des événements continue sans interruption sur les serveurs de collecte.

Le panneau Etat du système contient des outils pour gérer les serveurs CA Enterprise Log Manager et leurs services, ainsi que pour collecter des informations à des fins d'assistance. Le manuel d'administration et l'aide en ligne contiennent des informations complémentaires sur le sujet.

Modification de configurations globales

Vous pouvez définir des configurations globales pour l'ensemble des services. Si vous essayez d'enregistrer des valeurs non comprises dans la plage autorisée, CA Enterprise Log Manager est défini par défaut sur la valeur minimale ou maximale, selon le cas. Plusieurs des paramètres sont interdépendants.

Pour modifier des paramètres globaux

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
La Liste de services s'affiche.
2. Cliquez sur Configuration globale dans la Liste de services.
Le volet de détails Configuration globale du service s'ouvre.

3. Vous pouvez changer les paramètres de configuration suivants.

Intervalle de mise à jour

Spécifie la fréquence, en secondes, à laquelle les composants du serveur appliquent les mises à jour de configuration.

Minimum : 30

Maximum : 86400

Délai d'expiration de la session

Spécifie la durée maximale d'une session inactive. Si l'actualisation automatique est activée, une session n'expire jamais.

Minimum : 10

Maximum : 600

Permettre l'actualisation automatique

Permet aux utilisateurs d'actualiser automatiquement les rapports ou les requêtes. Ce paramètre permet aux administrateurs de désactiver l'actualisation automatique de manière globale.

Fréquence d'actualisation automatique

Spécifie l'intervalle, en minutes, auquel les vues de rapport sont actualisées. Ce paramètre dépend de la sélection de Permettre l'actualisation automatique.

Minimum : 1

Maximum : 60

Activer l'actualisation automatique

Définit l'actualisation automatique dans l'ensemble des sessions. Par défaut, l'actualisation automatique n'est pas activée.

Pour afficher les alertes d'action, l'authentification est requise.

Empêche les auditeurs ou les produits tiers d'afficher les flux RSS des alertes d'action. Ce paramètre est activé par défaut.

Rapport par défaut

Spécifie le rapport par défaut.

Activer le lancement du rapport par défaut

Affiche le rapport par défaut lorsque vous cliquez sur le sous-onglet Rapports. Ce paramètre est activé par défaut.

4. Vous pouvez changer les paramètres de balise de rapport ou de requête suivants.

Masquer les balises de rapport

Empêche les balises spécifiées d'apparaître dans une liste de balises. Masquer les balises de rapport rationalise l'affichage des rapports disponibles.

Masquer les balises de requête

Vous permet de masquer les balises choisies. Les balises masquées n'apparaissent plus dans la liste de requêtes principale ou dans la liste de requêtes de planification d'alertes d'action. Masquer les balises de requête personnalise l'affichage des requêtes disponibles.

5. Vous pouvez modifier les paramètres de tableau de bord suivants.

Activer le lancement du tableau de bord par défaut

Affiche le tableau de bord par défaut lorsque vous cliquez sur l'onglet Requêtes et rapports. Ce paramètre est activé par défaut.

Tableau de bord par défaut

6. Vous pouvez changer les paramètres de profil suivants.

Activer le profil par défaut

Vous permet de définir le profil par défaut.

Profil par défaut

Spécifie le profil par défaut.

Masquer les profils

Vous permet de masquer les profils choisis. Lorsque l'interface s'actualise ou que l'intervalle de mise à jour expire, les profils masqués n'apparaissent plus. Masquer les profils personnalise l'affichage des profils disponibles.

Remarque : Cliquez sur Réinitialiser pour restaurer les dernières valeurs enregistrées. Vous pouvez réinitialiser un ou plusieurs changements jusqu'à leur enregistrement. Une fois ces changements enregistrés, réinitialisez-les un par un.

7. Cliquez sur Enregistrer.

Utilisation des Paramètres et filtres globaux

Vous pouvez définir les filtres et paramètres globaux lors de la configuration de votre serveur CA Enterprise Log Manager. Les paramètres globaux sont enregistrés pour la session en cours uniquement, ils ne persistent pas après votre déconnexion du serveur, sauf si vous sélectionnez l'option Utiliser par défaut.

Un *filtre rapide* global contrôle l'intervalle de temps initial suivant lequel générer des rapports, propose le filtrage du texte correspondant et vous permet d'utiliser des champs spécifiques et leurs valeurs pour modifier les données affichées dans un rapport.

Un *filtre avancé* global vous permet d'utiliser la syntaxe et les opérateurs SQL pour accroître la portée de vos données de rapport. Les paramètres globaux vous permettent de définir un fuseau horaire et d'utiliser des requêtes spéciales, qui récupèrent les données d'autres serveurs CA Enterprise Log Manager d'une fédération, mais aussi d'activer l'actualisation automatique des rapports en cours d'affichage.

Vous devez définir des filtres globaux qui pourront être utilisés dans plusieurs zones du rapport. En définissant des options limitant le filtre global, vous pouvez contrôler la quantité de données affichées dans un rapport. Vous trouverez ci-dessous les tâches initiales liées aux paramètres et filtres globaux.

- Configurer des filtres rapides globaux pour fournir une durée initiale qui modifie les rapports affichés depuis ce serveur CA Enterprise Log Manager.
- Sélectionner des requêtes fédérées dans l'onglet Paramètres pour afficher des données provenant des serveurs CA Enterprise Log Manager fédérés sous ce serveur.
- Décider de l'actualisation automatique ou non des rapports.
- Définir l'intervalle d'actualisation des données dans les rapports.

Remarque : La définition d'un filtre global trop restreint ou trop spécifique peut empêcher l'affichage des données dans certains rapports.

Vous trouverez davantage d'informations sur les filtres globaux et leur utilisation dans l'aide en ligne.

Sélection de l'utilisation des requêtes fédérées

Vous pouvez choisir d'exécuter des requêtes sur les données fédérées si vous le souhaitez. Si vous envisagez d'utiliser plusieurs serveurs CA Enterprise Log Manager sur un réseau fédéré, vous souhaitez peut-être sélectionner la case à cocher Utiliser les requêtes fédérées. Cette option vous permet de collecter des données d'événement pour les rapports depuis l'ensemble des serveurs CA Enterprise Log Manager fédérés à (agissant comme enfants de) ce serveur CA Enterprise Log Manager .

Vous pouvez également choisir de désactiver les requêtes fédérées pour une requête spécifique si vous souhaitez afficher uniquement les données du serveur CA Enterprise Log Manager actuel.

Pour définir l'utilisation des requêtes fédérées

1. Connectez-vous au serveur CA Enterprise Log Manager.
2. Cliquez sur le bouton Afficher/Modifier les filtres globaux.
Ce bouton se trouve à droite du nom du serveur CA Enterprise Log Manager actuel, juste au-dessus des onglets principaux.
3. Cliquez sur l'onglet Paramètres.
4. Indiquez si vous souhaitez utiliser des requêtes fédérées.

Si vous désactivez l'option de sélection des requêtes fédérées, les rapports affichés ne contiendront *pas* de données d'événement provenant des serveurs configurés comme étant les enfants de ce serveur.

Informations complémentaires :

[Configuration d'une fédération CA Enterprise Log Manager](#) (page 235)

[Configuration d'un serveur CA Enterprise Log Manager en tant que serveur enfant](#) (page 236)

Configuration de l'intervalle global de mise à jour

Vous pouvez définir l'intervalle selon lequel les services CA Enterprise Log Manager recherchent des changements de configuration. Après l'installation, la valeur par défaut est cinq minutes, exprimée en secondes. La définition de cette valeur sur des intervalles très longs peut entraîner un retard des changements de configuration nécessaires dans leur application.

Pour configurer l'intervalle de mise à jour

1. Connectez-vous au serveur CA Enterprise Log Manager et cliquez sur l'onglet Administration.
2. Cliquez sur l'onglet Services, puis sur le noeud du service Configuration globale.
3. Entrez une nouvelle valeur pour l'intervalle de mise à jour.
La valeur par défaut et recommandée est 300 secondes.

Configuration du magasin de journaux d'événements

Le magasin de journaux d'événements est la base de données propriétaire sous-jacente qui contient les journaux d'événements collectés. Les options de configuration définies par vos soins pour le service du magasin de journaux d'événements peuvent être globales ou locales et affecter le stockage et l'archivage d'événements pour les serveurs CA Enterprise Log Manager. Le processus de configuration du magasin de journaux d'événements suit les étapes ci-dessous.

- Comprendre le service du magasin de journaux d'événements
- Comprendre comment le magasin de journaux d'événements gère les fichiers d'archive
- Configurer les valeurs globales et locales du magasin de journaux d'événements

Cette étape inclut le paramétrage de la taille de la base de données, des valeurs de base pour la conservation des fichiers d'archive, des règles de récapitulation, des règles de suppression, des relations de fédération, des paramètres de corrélation, des vérifications de l'intégrité des données et des options d'archivage automatique.

CA Enterprise Log Manager ferme automatiquement les fichiers des bases de données actives et crée des fichiers d'archive lorsque les bases de données actives atteignent la capacité définie pour ce service. CA Enterprise Log Manager ouvre ensuite de nouveaux fichiers actifs pour poursuivre les opérations de journalisation des événements. Vous pouvez définir des options d'archivage automatique pour gérer ces fichiers, mais uniquement sous la forme d'une configuration locale pour chaque serveur CA Enterprise Log Manager.

A propos du service du magasin de journaux d'événements

Le service du magasin de journaux d'événements gère les interactions des bases de données, comme celles répertoriées ci-dessous.

- Insertion de nouveaux événements dans la base de données actuelle (chaude)
- Récupération d'événements provenant de bases de données fédérées locales et distantes pour les requêtes et les rapports
- Création de nouvelles bases de données lorsque la base de données actuelle est pleine
- Création de fichiers d'archive et suppression d'anciens fichiers d'archive
- Gestion du cache de requête d'archive
- Application des règles de récapitulation et de suppression sélectionnées
- Application des règles de transfert d'événement sélectionnées
- Définition des serveurs CA Enterprise Log Manager qui agissent comme des enfants fédérés pour ce serveur CA Enterprise Log Manager

A propos des fichiers d'archive

Le serveur CA Enterprise Log Manager crée automatiquement des fichiers de base de données compressée, appelés fichiers d'*archive*, lorsqu'une base de données chaude atteint le paramètre Nombre maximum de lignes spécifié dans le service du magasin de journaux d'événements. Les fichiers de base de données chaude ne sont pas compressés.

Lorsque vous configurez l'archivage automatique d'un serveur de collecte vers un serveur de rapports, les bases de données compressées du serveur de collecte sont supprimées après qu'elles ont été copiées sur le serveur de rapports. Le paramètre Nbre max. de jours d'archivage ne s'applique pas ici.

Lorsque vous configurez l'archivage automatique d'un serveur de rapports vers un serveur de stockage distant, les bases de données compressées du serveur de rapports ne sont pas supprimées après avoir été copiées sur le serveur de stockage distant. Ces bases de données tièdes sont plutôt conservées sur le serveur de rapports jusqu'à ce que la valeur Nbre max. de jours d'archivage soit atteinte. Ensuite, elles sont *supprimées*. Toutefois, un enregistrement de ces bases de données froides supprimées est conservé pour que vous puissiez effectuer des requêtes de détails sur la base de données d'archive, au cas où vous auriez besoin de cette information pour effectuer une restauration.

Lorsque vous déterminez le paramètre Nbre max. de jours d'archivage, tenez compte de votre espace disque disponible sur le serveur de rapports. Votre configuration de l'espace disque d'archivage définit le seuil. Si l'espace disque disponible passe en dessous du pourcentage défini, les données des journaux d'événements sont supprimées pour libérer de l'espace, même si le Nbre max. de jours d'archivage n'est pas écoulé pour ces données.

Si vous ne configurez pas l'archivage automatique d'un serveur de rapports vers un serveur de stockage distant, vous devez sauvegarder manuellement les bases de données compressées et déplacer manuellement la copie vers un emplacement de stockage distant selon une fréquence supérieure au Nbre max. de jours d'archivage configuré. Sans quoi vous risquez de perdre des données. Nous vous recommandons de sauvegarder quotidiennement les fichiers d'archive, pour éviter tout risque de perte de données et conserver l'espace disque approprié. Le service du magasin de journaux d'événements gère son propre cache interne pour les requêtes sur les bases de données archivées, afin d'améliorer les performances lors de l'exécution de requêtes répétées ou très vastes.

Le *Manuel d'administration CA Enterprise Log Manager* contient davantage d'informations sur l'utilisation des fichiers d'archive.

Informations complémentaires :

[Exemple : Archivage automatique sur trois serveurs](#) (page 175)

A propos de l'archivage automatique

La gestion des magasins d'événements stockés nécessite une manipulation soigneuse des sauvegardes et des fichiers restaurés. La configuration du service du magasin de journaux d'événements constitue une position centrale pour configurer et régler la taille et la conservation de la base de données interne, et pour définir les options d'archivage automatique. CA Enterprise Log Manager fournit les scripts ci-dessous pour vous permettre d'effectuer ces tâches.

- backup-ca-elm.sh
- restore-ca-elm.sh
- monitor-backup-ca-elm.sh

Remarque : L'utilisation de ces scripts suppose que vous avez établi une authentification non interactive entre les deux serveurs à l'aide de clés RSA.

Les scripts *backup* et *restore* se servent de l'utilitaire LMArchive pour simplifier la copie de bases de données tièdes depuis et vers les hôtes distants. Ces scripts mettent automatiquement à jour les fichiers de catalogue adéquats lorsque les tâches s'achèvent. Vous pouvez faire une copie vers des serveurs distants ou vers d'autres serveurs CA Enterprise Log Manager. Si l'hôte distant auquel vous envoyez des fichiers est un serveur CA Enterprise Log Manager, les scripts mettent également à jour automatiquement les fichiers de catalogue sur le serveur de réception. Les scripts suppriment également les fichiers d'archive de l'ordinateur local, pour éviter la duplication dans les rapports fédérés. Cela permet de garantir la disponibilité des données pour les requêtes et les rapports. Le stockage en dehors du système est appelé stockage sauvegardé. Vous pouvez restaurer les fichiers déplacés vers le stockage sauvegardé pour effectuer des requêtes et des rapports.

Le script *monitor* exécute automatiquement le script backup à l'aide des paramètres spécifiés dans la partie archivage automatique de la configuration du service du magasin de journaux d'événements.

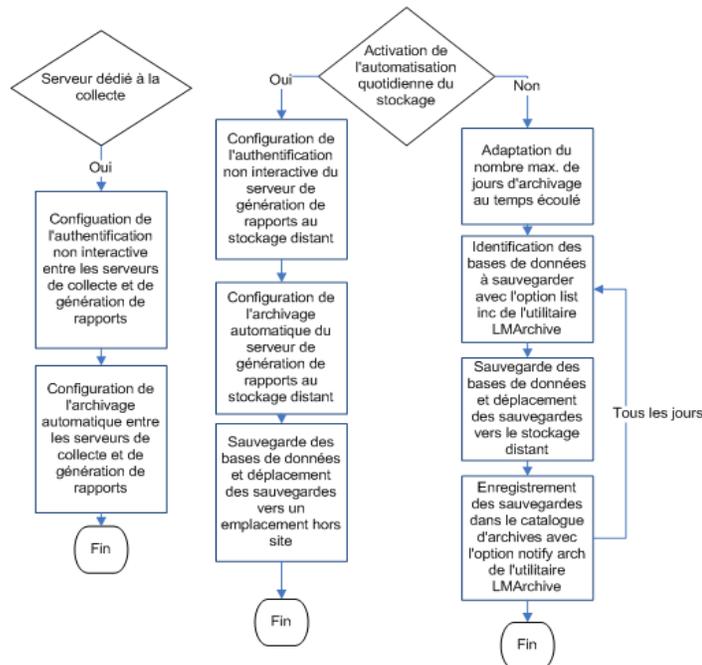
Informations complémentaires :

[Exemple : Archivage automatique sur trois serveurs](#) (page 175)

Organigramme de stratégie de sauvegarde et de déplacement de base de données

Vous pouvez effectuer la collecte d'événements et la génération de rapports sur chaque serveur CA Enterprise Log Manager ou vous pouvez dédier un serveur différent pour chaque type d'opération. Si vous dédiez des serveurs à la collecte, vous devez automatiser les déplacements des serveurs de collecte par heure vers un serveur de génération de rapports. Dans le cas contraire, cette configuration n'est pas applicable. Si vous n'avez pas de rôles de serveur dédiés, il vous faut lire les références "à partir des rapports vers le stockage distant" de l'organigramme comme "à partir d'un serveur CA Enterprise Log Manager non-dédié vers le stockage distant".

Une stratégie de sauvegarde suppose deux copies de chaque base de données: L'une d'elle est considérée comme la sauvegarde. Vous pouvez réaliser cet objectif avec ou sans l'archivage automatique vers un serveur de stockage distant. La stratégie de sauvegarde avec archivage automatique suppose que les bases de données originales sont situées sur le serveur de stockage distant et les sauvegardes dans un emplacement hors site. La stratégie de sauvegarde sans archivage automatique suppose que les bases de données originales sont situées sur le serveur CA Enterprise Log Manager et les sauvegardes sur serveur de stockage distant. Le stockage des bases de données originales sur le serveur CA Enterprise Log Manager où elles ont initialement été archivées dépend de l'espace disponible pour le stockage à long terme et des stratégies de stockage. Si ces critères sont satisfaits, la décision vous appartient.



Configuration de l'authentification non interactive pour l'archivage automatique

Vous pouvez configurer l'archivage automatique entre serveurs ayant des rôles différents. Par exemple :

- A partir d'un ou plusieurs serveurs de collecte vers un unique serveur de génération de rapports.
- A partir d'un ou plusieurs serveurs de génération de rapports vers un unique serveur de stockage distant.

Avant de configurer l'archivage automatique d'un serveur vers un autre, configurez l'authentification *ssh* non interactive du serveur source vers le serveur de destination. *Non interactive* signifie qu'un serveur peut déplacer des fichiers vers un autre serveur sans nécessiter de mot de passe.

- Si vous disposez uniquement de trois serveurs, un serveur de collecte, un serveur de génération de rapports, et un serveur de stockage distant, configurez l'authentification non interactive deux fois :
 - A partir du serveur de collecte vers le serveur de génération de rapports.
 - A partir du serveur de génération de rapports vers le serveur de stockage distant.
- Si vous disposez de six serveurs avec quatre serveurs de collecte, un serveur de génération de rapports et un serveur de stockage distant, configurez l'authentification non interactive cinq fois :
 - A partir du serveur de collecte 1 vers le serveur de génération de rapports.
 - A partir du serveur de collecte 2 vers le serveur de génération de rapports.
 - A partir du serveur de collecte 3 vers le serveur de génération de rapports.
 - A partir du serveur de collecte 4 vers le serveur de génération de rapports.
 - A partir du serveur de génération de rapports vers le serveur de stockage distant.

La configuration de l'authentification ssh non interactive entre deux serveurs requiert des paires de clé RSA, une clé privée et une clé publique. Copiez la première clé publique que vous générez sur le serveur de destination en tant que `authorized_keys`. Lorsque vous configurez plusieurs instances d'authentification non interactive sur le même serveur de génération de rapports de destination, copiez les clés publiques supplémentaires portant des noms de fichier uniques pour éviter d'écraser l'original `authorized_keys`. Puis, concaténez ces noms de fichier à `authorized_keys`. Par exemple, vous pouvez ajouter `authorized_keys_ELM-C2` et `authorized_keys_ELM-C3` au fichier `authorized_keys` d'ELM-C1.

Exemple : Configuration de l'authentification non interactive pour la topologie en étoile

L'existence de l'authentification non interactive entre deux serveurs est une condition préalable à l'archivage automatique de la source vers le serveur de destination. Un scénario commun pour configurer l'authentification non interactive consiste à mettre en place un serveur de génération de rapports/de gestion commun pour les serveurs sources dédiés à la collecte. Cet exemple présuppose une fédération CA Enterprise Log Manager de taille moyenne avec un serveur de génération de rapports/de gestion (concentrateur), quatre serveurs de collecte (branches) et un serveur de stockage distant. Les noms des serveurs pour chaque rôle de serveur sont les suivants :

- Serveur de génération de rapports/de gestion CA Enterprise Log Manager : ELM-RPT
- Serveurs de collecte CA Enterprise Log Manager : ELM-C1, ELM-C2, ELM-C3, ELM-C4
- Serveur de stockage distant : RSS

Les procédures pour activer l'authentification non interactive pour la fédération CA Enterprise Log Manager sont les suivantes :

1. A partir du premier serveur de collecte, générez une paire de clé RSA caelmservice, puis copiez la clé publique comme `authorized_keys` dans le répertoire `/tmp` sur le serveur de génération de rapports de destination.
2. A partir de chaque serveur de collecte supplémentaire, générez une paire de clé RSA et copiez la clé publique comme `authorized_keys_n`, le `n` permettant d'identifier la source.
3. A partir du répertoire `/tmp` du serveur de génération de rapports, concaténez le contenu des fichiers de clé publique à l'original `authorized_keys`. Créez un répertoire `.ssh` et modifiez les droits de propriété du répertoire sur `caelmservice`, déplacez `authorized_keys` dans le répertoire `.ssh`, puis définissez les droits de propriété du fichier clé et les autorisations obligatoires.
4. Vérifiez que l'authentification non interactive existe entre chaque serveur de collecte et le serveur de génération de rapports.
5. A partir du serveur de stockage distant, créez une structure de répertoires pour le répertoire `.ssh`, la valeur par défaut étant `/opt/CA/LogManager`. Créez un répertoire `.ssh` sur la destination, modifiez les droits de propriété par `caelmservice`.

6. A partir du serveur de génération de rapports, générez une paire de clé RSA caelmservice, puis copiez la clé publique comme `authorized_keys` dans le répertoire `/tmp` sur le serveur de stockage distant.
7. A partir du serveur de stockage distant, déplacez `authorized_keys` de `/tmp` dans le répertoire `.ssh`, puis remplacez les droits de propriété du fichier clé sur `caelmservice` et définissez les autorisations obligatoires.
8. Vérifiez que l'authentification non interactive existe entre le serveur de génération de rapports et le serveur de stockage distant.

Configuration des clés pour la première paire génération de rapports-collection

La configuration de l'authentification non interactive pour une topologie en étoile commence par la génération d'une paire de clé publique/clé privée RSA sur un serveur de collecte et par la copie de la clé publique sur son serveur de génération de rapports. Copiez le fichier de clé publique nommée `authorized_keys`. Partons du principe que cette clé est la première clé publique copiée sur le serveur de génération de rapports spécifié.

Pour générer une paire de clés RSA sur le serveur de collecte et copiez la clé publique sur le serveur de génération de rapports :

1. Connectez-vous au serveur ELM-C1 via ssh en tant qu'utilisateur `caelmadmin`.
2. Basculez sur le compte d'utilisateur `root`.
`su -`
3. Basculez sur le compte d'utilisateur `caelmservice`.
`su - caelmservice`
4. Générez la paire de clés RSA à l'aide de la commande ci-dessous.
`ssh-keygen -t rsa`
5. Pour accepter la valeur par défaut lorsque les invites suivantes s'affichent, appuyez sur Entrée :
 - Indiquez le fichier dans lequel enregistrer la clé (`/opt/CA/LogManager/.ssh/id_rsa`) :
 - Saisissez la phrase secrète (laissez le champ vide si aucune phrase secrète n'a été définie) :
 - Confirmez la phrase secrète :

6. Remplacez les répertoires par /opt/CA/LogManager.
7. Modifiez les autorisations du répertoire .ssh à l'aide de la commande ci-dessous.

```
chmod 755 .ssh
```

8. Accédez au fichier .ssh, dans lequel la clé id_rsa.pub est enregistrée.

```
cd .ssh
```

9. Copiez le fichier id_rsa.pub sur ELM-RPT, le serveur CA Enterprise Log Manager de destination à l'aide de la commande ci-dessous.

```
scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys
```

Le fichier authorized_keys est créé sur le serveur de génération de rapports avec le contenu de la clé publique.

Configuration des clés pour les paires génération de rapports-collection supplémentaires

La deuxième étape de configuration de l'authentification non interactive pour une topologie en étoile est la génération d'une paire de clés RSA sur chaque serveur de collecte supplémentaire et sa copie dans le répertoire /tmp du serveur commun de génération de rapports comme authorized_keys_n, la lettre n indiquant le serveur de collecte source.

Pour générer une paire de clés RSA sur les serveurs de collecte supplémentaires et copier la clé publique sur un serveur commun de génération de rapports :

1. Connectez-vous au deuxième serveur de collecte ELM-C2 au moyen du ssh en tant que caelmadmin.
2. Basculez sur le compte d'utilisateur root.
3. Basculez sur le compte d'utilisateur caelmservice.

```
su - caelmservice
```

4. Générez la paire de clés RSA à l'aide de la commande ci-dessous.

```
ssh-keygen -t rsa
```

5. Pour accepter la valeur par défaut lorsque les invites suivantes s'affichent, appuyez sur Entrée :

- Indiquez le fichier dans lequel enregistrer la clé (/opt/CA/LogManager/.ssh/id_rsa) :
- Saisissez la phrase secrète (laissez le champ vide si aucune phrase secrète n'a été définie) :
- Confirmez la phrase secrète :

6. Accédez au répertoire /opt/CA/LogManager.
7. Modifiez les autorisations du répertoire .ssh à l'aide de la commande ci-dessous.

```
chmod 755 .ssh
```

8. Accédez au fichier .ssh, dans lequel la clé id_rsa.pub est enregistrée.
9. Copiez le fichier id_rsa.pub sur ELM-RPT, le serveur CA Enterprise Log Manager de destination à l'aide de la commande ci-dessous.

```
scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C2
```

Le fichier authorized_keys_ELM-C2 est créé sur le serveur de génération de rapports avec le contenu de la clé publique.

10. Entrez yes (oui) suivi du mot de passe de caelmadmin pour ELM-RPT.
11. Entrez exit (quitter).
12. Répétez les étapes 1 à 11 de cette procédure pour les serveurs de collecte ELM-C3. Pour l'étape 9, saisissez la valeur suivante :

```
scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C3
```

13. Répétez les étapes 1 à 11 de cette procédure pour les serveurs de collecte ELM-C4. Pour l'étape 9, saisissez la valeur suivante :

```
scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C4
```

Création d'un fichier de clé publique unique sur le serveur de génération de rapports et définition des droits de propriété du fichier

Jusqu'ici dans notre scénario, nous avons généré des paires de clés sur chaque serveur de collecte et copié les clés publiques sur le serveur de génération de rapports en tant que fichiers nommés :

- authorized_keys
- authorized_keys_ELM-C2
- authorized_keys_ELM-C3
- authorized_keys_ELM-C4

La troisième étape consiste à concaténer ces fichiers et à déplacer le fichier de clé publique RSA obtenu dans le répertoire approprié, puis à définir caelmservice en tant que propriétaire du répertoire et du fichier.

Pour créer un fichier de clé publique concaténé dans un emplacement approprié sur le serveur de génération de rapports et définir les droits de propriété du fichier :

1. Connectez-vous au serveur de génération de rapports CA Enterprise Log Manager via ssh en tant qu'utilisateur caelmadmin.
2. Basculez sur le compte d'utilisateur root.
3. Remplacez les répertoires dans le dossier CA Enterprise Log Manager par :

```
cd /opt/CA/LogManager
```
4. Créez le dossier .ssh.

```
mkdir .ssh
```
5. Modifiez les droits de propriété du nouveau dossier sur le groupe et l'utilisateur caelmservice.

```
chown caelmservice:caelmservice .ssh
```
6. Remplacez les répertoires par /tmp.
7. Ajoutez le contenu des clés publiques des serveurs de collecte ELM-C2, ELM-C3 et ELM-C4 au fichier authorized_keys qui contient la clé publique d'ELM-C1.

```
cat authorized_keys_ELM-C2 >> authorized_keys
cat authorized_keys_ELM-C3 >> authorized_keys
cat authorized_keys_ELM-C4 >> authorized_keys
```

8. Remplacez les répertoires par /opt/CA/LogManager/.ssh.
9. Copiez le fichier authorized_keys du dossier /tmp vers le dossier actuel .ssh :

```
cp /tmp/authorized_keys .
```

10. Modifiez la propriété du fichier authorized_keys pour l'octroyer au compte caelmservice.

```
chown caelmservice:caelmservice authorized_keys
```

11. Modifiez les autorisations de ce fichier :

```
chmod 755 authorized_keys
```

Le chiffre 755 fait référence à un accès en lecture et exécution pour tous les utilisateurs et à un accès en lecture, exécution et écriture pour le propriétaire du fichier.

Vous achevez ainsi la configuration de l'authentification sans mot de passe entre les serveurs de collecte et le serveur de génération de rapports.

Validation de l'authentification non interactive entre les serveurs de collecte et de génération de rapports

Vous pouvez valider la configuration de l'authentification non interactive entre les serveurs source et de destination des deux phases de l'archivage automatique.

Pour valider la configuration entre les serveurs de collecte et de rapports

1. Connectez-vous au serveur de collecte ELM-C1; via ssh en tant que caelmsadmin.
2. Basculez sur le compte d'utilisateur root.
3. Basculez sur le compte d'utilisateur caelmservice.

```
su - caelmservice
```

4. Entrez la commande suivante.

```
ssh caelmservice@ELM-RPT
```

La connexion à ELM-RPT sans saisie de phrase secrète confirme l'authentification non interactive entre le ELM-C1 et ELM-RPT.

5. Connectez-vous à ELM-C2 et répétez l'opération.
6. Connectez-vous à ELM-C3 et répétez l'opération.
7. Connectez-vous à ELM-C4 et répétez l'opération.

Création d'une structure de répertoires avec des droits de propriété sur le serveur de stockage distant

Cette procédure suppose que le serveur de stockage distant n'est pas un serveur CA Enterprise Log Manager et que vous devez créer de nouveaux utilisateurs, un groupe et une structure de répertoires reflétant ceux d'un serveur CA Enterprise Log Manager. Vous devez effectuer cette procédure avant d'envoyer la clé du serveur de génération de rapports, car vous utilisez le compte caelmadmin créé pour communiquer avec le serveur de génération de rapports.

Pour créer une structure de fichier et définir les droits de propriété du fichier sur le serveur de stockage distant :

1. Connectez-vous au serveur de stockage distant (RSS); via ssh en tant qu'utilisateur root.
2. Créez un nouvel utilisateur appelé caelmadmin.
3. Créez un groupe appelé caelmservice, puis créez un nouvel utilisateur appelé caelmservice.
4. Créez le répertoire qui servira d'emplacement distant, celui par défaut étant /opter/CA/LogManager.

Remarque : Pour utiliser un répertoire différent, indiquez-le lorsque vous configurez l'emplacement distant pour l'archivage automatique.

5. Remplacez le répertoire de base de caelmservice par /opter/CA/LogManager ou par le répertoire d'emplacement distant prévu. Le répertoire par défaut est utilisé dans l'exemple suivant :

```
usermod -d /opt/CA/LogManager caelmservice
```

6. Définissez les autorisations du fichier pour caelmservice. Le répertoire Emplacement distant par défaut est utilisé dans l'exemple suivant :

```
chown -R caelmservice:caelmservice /opt/CA/LogManager
```

7. Remplacez les répertoires par /opter/CA/LogManager ou par l'emplacement distant.
8. Créez le dossier .ssh.
9. Remplacez le propriétaire du dossier .ssh par le groupe et l'utilisateur caelmservice.

```
chown caelmservice:caelmservice .ssh
```

10. Déconnectez-vous du serveur de stockage distant.

Configuration des clés pour la paire Génération de rapports-Stockage distant

Après avoir configuré et validé l'authentification non interactive de tous les serveurs de collecte vers le serveur de génération de rapports, vous devez configurer et valider l'authentification non interactive du serveur de génération de rapports vers le serveur de stockage distant.

Dans l'exemple, la première étape de la configuration passe par la génération d'une nouvelle paire de clé RSA sur le serveur de génération de rapports, ELM-RPT, puis par la copie de la clé publique en tant que `authorized_keys` dans el répertoire `/tmp` du serveur de stockage distant (RSS).

Pour générer une paire de clé RSA sur le serveur de génération de rapports et la copier sur le serveur de stockage distant :

1. Connectez-vous au serveur de génération de rapports en tant qu'utilisateur `caelmadmin`.
2. Basculez sur le compte d'utilisateur `root`.
3. Basculez sur le compte d'utilisateur `caelmservice`.

```
su - caelmservice
```

4. Générez la paire de clés RSA à l'aide de la commande ci-dessous.

```
ssh-keygen -t rsa
```

5. Pour accepter la valeur par défaut lorsque les invites suivantes s'affichent, appuyez sur Entrée :

- Indiquez le fichier dans lequel enregistrer la clé (`/opt/CA/LogManager/.ssh/id_rsa`) :
- Saisissez la phrase secrète (laissez le champ vide si aucune phrase secrète n'a été définie) :
- Confirmez la phrase secrète :

6. Remplacez les répertoires par `/opt/CA/LogManager`.
7. Modifiez les autorisations du répertoire `.ssh` à l'aide de la commande ci-dessous.

```
chmod 755 .ssh
```

8. Naviguez jusqu'au dossier `.ssh`.

9. Copiez le fichier `id_rsa.pub` sur RSS, le serveur de stockage distant de destination à l'aide de la commande ci-dessous.

```
scp id_rsa.pub caelmadmin@RSS:/tmp/authorized_keys
```

Le fichier `authorized_keys` est créé dans le répertoire `/tmp` du serveur de génération de rapports avec le contenu de la clé publique.

Définition des droits de propriété de fichier de clé sur le serveur de stockage distant

Vous pouvez définir les droits de propriété et les autorisations du fichier de clé sur un serveur de stockage distant si vous avez généré une paire de clés sur le serveur de génération de rapports et si vous avez copié la clé publique sur ce serveur de stockage distant.

Pour déplacer le fichier de clé publique vers le bon emplacement sur le serveur de stockage distant et définir la propriété du fichier

1. Connectez-vous au serveur de stockage distant en tant qu'utilisateur `caelmadmin`.
2. Basculez sur le compte d'utilisateur `root`.
3. Remplacez les répertoires par `/opt/CA/LogManager/.ssh`.
4. Copiez le fichier `authorized_keys` du répertoire `/tmp` vers le répertoire `.ssh` actuel :

```
cp /tmp/authorized_keys .
```

5. Modifiez les droits de propriété du fichier `authorized_keys` à l'aide de la commande ci-dessous.

```
chown caelmservice:caelmservice authorized_keys
```

6. Modifiez les autorisations du fichier `authorized_keys` :

```
chmod 755 authorized_keys
```

L'authentification non interactive est désormais configurée entre un serveur de génération de rapports CA Enterprise Log Manager et l'hôte distant utilisé pour le stockage.

Validation de l'authentification non interactive entre les serveurs de génération de rapports et de stockage

Vérifiez que l'authentification non interactive existe entre le serveur de génération de rapports et le serveur de stockage distant. Dans l'exemple, le serveur de stockage distant est nommé RSS.

Pour valider l'authentification non interactive entre le serveur de génération de rapports CA Enterprise Log Manager et le serveur de stockage :

1. Connectez-vous au serveur de génération de rapports en tant qu'utilisateur root.
2. Basculez sur le compte d'utilisateur caelmservice.
3. Entrez la commande suivante.

```
su - caelmservice
```

```
ssh caelmservice@RSS
```

Vous êtes connecté au serveur de stockage distant sans avoir à saisir de phrase secrète.

Exemple : Configuration de l'authentification non interactive au niveau de trois serveurs

Le scénario le plus simple pour configurer l'authentification non interactive, une condition préalable à l'archivage automatique, est basé sur deux serveurs CA Enterprise Log Manager, un serveur de collecte et un serveur de génération de rapports/de gestion et un système de stockage distant sur un serveur UNIX ou Linux. Cet exemple suppose que les trois serveurs préparés pour l'archivage automatique sont :

- NY-Collecte-ELM
- NY-Rapports-ELM
- NY-Serv-Stockage

Les procédures pour activer l'authentification non interactive sont les suivantes :

1. A partir du serveur NY-Collecte-ELM, générez la paire de clés RSA comme caelmservice, puis copiez la clé publique de cette paire comme authorized_keys dans le répertoire /tmp sur NY-Rapports-ELM.
2. Créez un répertoire .ssh sur NY-Rapports-ELM, modifiez les droits de propriété sur caelmservice, déplacez le fichier authorized_keys du répertoire /tmp vers le répertoire .ssh, puis définissez les droits de propriété du fichier clé sur caelmservice avec les autorisations obligatoires.
3. Validez l'authentification non interactive de NY-Collecte-ELM vers NY-Rapports-ELM.
4. A partir du serveur NY-Rapports-ELM, générez la paire de clés RSA comme caelmservice, puis copiez la clé publique de cette paire comme authorized_keys dans le répertoire /tmp sur NY-Serv-Stockage.
5. Dans le serveur NY-Serv-Stockage, crée la structure de répertoires /opter/CA/LogManager. A partir de ce chemin d'accès, créez un répertoire .ssh , modifiez les droits de propriété sur caelmservice, déplacez authorized_keys dans ce répertoire et définissez les droits de propriété du fichier clé sur caelmservice avec les autorisations obligatoires.
6. Validez l'authentification non interactive de NY-Rapports-ELM vers NY-Serv-Stockage.

Les détails pour ces étapes sont similaires à ceux du scénario de topologie en étoile. Pour un scénario à trois serveurs, vous pouvez ignorer l'étape 2 sur des paires génération de rapports/collecte supplémentaires et ignorer les instructions de l'étape 3 sur la concaténation des fichiers dans authorized_keys.

Exemple : Archivage automatique sur trois serveurs

Dans une architecture collecte-génération de rapports, vous devez configurer l'archivage automatique entre le serveur de collecte et un serveur de rapports. Cette configuration automatise le déplacement d'une base de données tiède, contenant les données de journaux d'événements collectés et ajustés, vers le serveur de rapports sur lequel vous pouvez effectuer la génération de rapports. Il est recommandé de planifier cet archivage automatique toutes les heures, plutôt qu'une fois par jour, afin d'éviter de longs transferts quotidiens. Choisissez une planification basée sur votre charge et indiquez si vous souhaitez regrouper le traitement en une fois ou le répartir sur la journée. Lorsque la copie des bases de données s'effectue via un archivage automatique à partir d'un serveur de collecte vers son serveur de rapports, les bases sont supprimées du serveur de collecte.

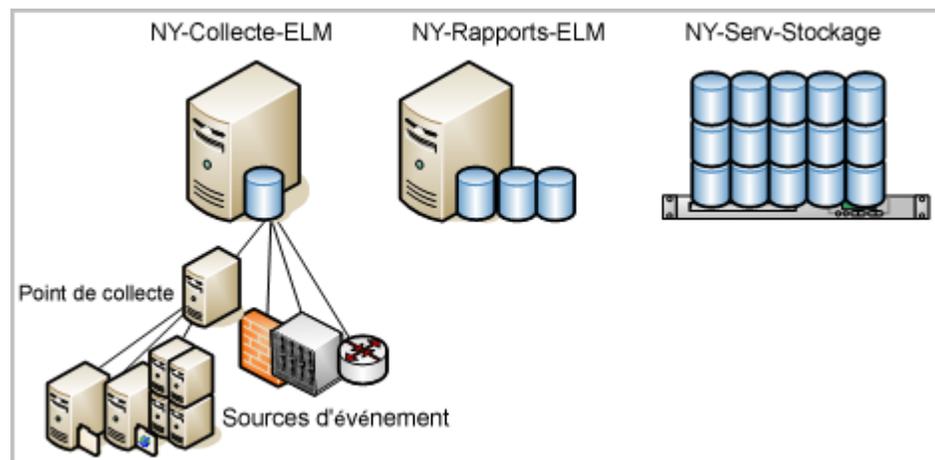
Après avoir identifié un serveur local disposant d'un espace de stockage suffisant, vous pouvez configurer l'archivage automatique du serveur de rapports vers ce serveur de stockage distant. Lorsque la copie des bases de données s'effectue via l'archivage automatique, à partir d'un serveur de rapports vers un serveur de stockage distant, les bases restent intactes sur le serveur de rapports jusqu'à ce que le délai défini par le paramètre Nbre max. de jours d'archivage soit écoulé. A ce moment seulement elles sont supprimées. L'avantage de cette phase d'archivage automatique est qu'elle évite la perte des bases de données archivées si celles-ci ne sont pas déplacées manuellement jusqu'à l'emplacement de stockage à long terme avant leur suppression automatique.

Remarque : Avant de configurer un serveur distant pour recevoir les bases de données archivées automatiquement, vous devez créer une structure de répertoires sur le serveur de destination, identique à celle existant sur le serveur CA Enterprise Log Manager source, puis affecter des droits de propriétés et des autorisations pour l'authentification. Pour plus de détails, consultez la section "Configuration d'une authentification non interactive", dans le *Manuel d'implémentation*. Veillez à bien suivre les instructions décrites dans la section "Définition de la propriété du fichier de clé sur un hôte distant".

Dans le cadre du présent scénario, imaginons que vous êtes administrateur CA Enterprise Log Manager d'un centre de données situé à New York et doté d'un réseau de serveurs CA Enterprise Log Manager, chacun possédant un rôle dédié, plus un serveur distant disposant d'une capacité de stockage importante. Les noms des serveurs utilisés pour l'archivage automatique sont les suivants.

- NY-Collecte-ELM
- NY-Rapports-ELM
- NY-Serv-Stockage

Remarque : Cet exemple suppose l'existence d'un serveur de gestion dédié à l'administration du système de serveurs CA Enterprise Log Manager. Ce serveur n'est pas décrit ici car il n'a pas de fonction directe dans la procédure d'archivage automatique.



Pour configurer l'archivage automatique entre un serveur de collecte et un serveur de rapports, puis entre ce dernier et un serveur de stockage distant, basez-vous sur l'exemple suivant.

1. Sélectionnez l'onglet Administration, puis le sous-onglet Collecte de journaux.
2. Développez le dossier Magasin de journaux d'événements, puis sélectionnez un serveur de collecte.



3. Indiquez une récurrence d'archivage automatique toutes les heures, avec le serveur de rapports comme destination. Entrez les informations d'identification d'un utilisateur CA Enterprise Log Manager doté d'un rôle d'administrateur. Si vous utilisez des stratégies personnalisées, cet utilisateur doit disposer de droits de modification sur les ressources de base de données, qui lui donnent la possibilité de supprimer la base de données archivée.



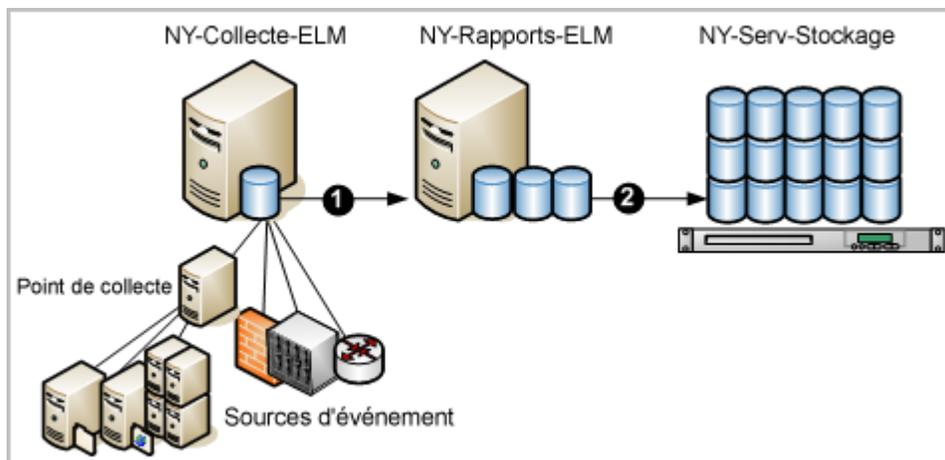
4. Dans la Liste de services, sélectionnez le serveur de rapports.



- Indiquez une récurrence d'archivage automatique tous les jours, avec un serveur distant comme destination de stockage. Entrez les informations d'identification d'un compte d'utilisateur doté d'un rôle d'administrateur. Vous pouvez également créer une stratégie d'accès CALM avec l'action de modification sur les ressources de base de données et affecter un utilisateur comme identité. Dans ce cas, entrez les informations d'identification d'un utilisateur disposant de peu de droits.



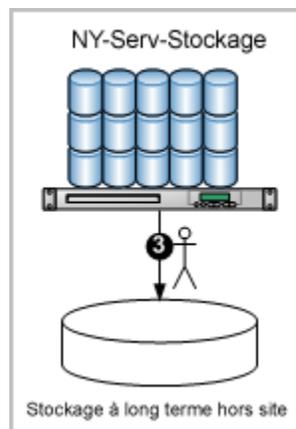
Les numéros figurant sur le diagramme suivant représentent deux configurations d'archivage automatique : une entre le serveur de collecte et le serveur de rapports et une autre entre le serveur de rapports et un serveur distant du réseau.



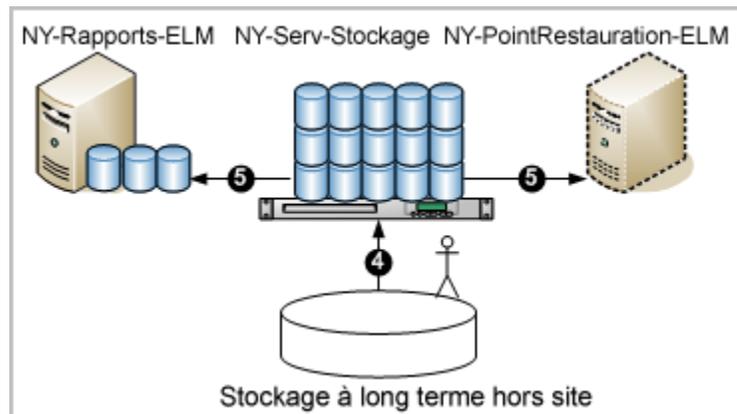
Dans une telle configuration, la procédure automatique fonctionne comme suit.

1. NY-Collecte-ELM, serveur de collecte CA Enterprise Log Manager, collecte et ajuste les événements et les intègre à la base de données chaude. Lorsque la base de données chaude atteint le nombre d'enregistrements configuré, elle est compressée. L'archivage automatique étant planifié toutes les heures, le système copie les bases de données tièdes une fois par heure et les transfère sur le serveur de rapports CA Enterprise Log Manager, NY-Rapports-ELM. Les bases de données tièdes sont supprimées du serveur NY-Collecte-ELM lors du déplacement.
2. NY-Rapports-ELM conserve les bases de données pouvant faire l'objet de requêtes tant que le délai défini par le paramètre Nbre max. de jours d'archivage n'est pas écoulé. L'archivage automatique étant planifié tous les jours, le système déplace quotidiennement les bases de données tièdes et les transfère sur NY-Serv-Stockage en tant que bases de données froides. Ces dernières peuvent être conservées sur le serveur de stockage pendant une longue période.
3. Pour conserver les bases de données froides pendant le nombre d'années requis, transférez-les depuis NY-Serv-Stockage sur le réseau jusqu'à un système de stockage à long terme hors site.

La fonction de l'archivage est de garder les journaux d'événements à disposition à des fins de restauration. Les bases de données froides peuvent être restaurées si nécessaire, afin d'étudier des événements consignés dans les journaux. Le déplacement manuel des bases de données archivées, entre le serveur de stockage sur site et le système de stockage à long terme hors site, est illustré dans le schéma suivant.



4. Imaginez une situation où il serait nécessaire d'étudier des journaux sauvegardés et stockés hors site. Pour identifier le nom de la base de données archivée à restaurer, faites une recherche dans le catalogue d'archive local sur NY-Rapports-ELM. Pour ce faire, cliquez sur l'onglet Administration, sélectionnez Requête de catalogue d'archive dans l'Explorateur de collecte de journaux, puis cliquez sur Requête.
5. Récupérez la base de données archivée identifiée dans le stockage hors site. Copiez-la dans le répertoire /opt/CA/LogManager/data/archive, sur le serveur de stockage NY-Serv-Stockage. Modifiez ensuite la propriété du répertoire d'archivage en sélectionnant l'utilisateur caelmservice.
6. Restaurez la base de données sur son serveur de rapports d'origine ou à un point de restauration dédié à l'étude des journaux contenus dans les bases de données restaurées, en procédant comme suit.
 - Si vous restaurez la base sur NY-Rapports-ELM, exécutez le script restore-ca-elm.sh à partir de NY-Rapports-ELM, en spécifiant NY-Serv-Stockage comme hôte distant.
 - Si vous restaurez la base sur NY-PointRestauration-ELM, exécutez le script restore-ca-elm.sh à partir de NY-PointRestauration-ELM en spécifiant NY-Serv-Stockage comme hôte distant.



Remarque : Vous pouvez désormais créer des requêtes et des rapports sur les données restaurées.

Informations complémentaires :

[A propos de l'archivage automatique](#) (page 159)

[A propos des fichiers d'archive](#) (page 158)

[Paramètres du magasin de journaux d'événements dans l'environnement de base](#) (page 181)

[Exemple : Carte de fédération pour une grande entreprise](#) (page 37)

Paramètres du magasin de journaux d'événements dans l'environnement de base

Dans un environnement où des serveurs CA Enterprise Log Manager distincts assument les rôles de serveur de collecte et de serveur de rapports, vous devriez configurer individuellement les magasins de journaux d'événements comme des configurations locales. Si vous choisissez également d'utiliser le serveur de rapports pour gérer le trafic de basculement, vous souhaitez peut-être définir une valeur plus élevée pour le champ Nombre maximum de lignes que celle affichée dans la table. Si vous utilisez votre serveur de gestion comme serveur de rapports, n'oubliez pas que le serveur de gestion lui-même génère certaines informations d'événement sous la forme d'événements d'autosurveillance.

Remarque : Vous devez configurer chaque paire de serveurs participant à l'archivage automatique pour l'authentification non interactive, pour que la configuration de l'archivage automatique fonctionne correctement.

La table suivante est un exemple de paramétrage de base. Le serveur CA Enterprise Log Manager de collecte s'appelle CollSrvr-1. Le serveur CA Enterprise Log Manager de rapports s'appelle RptSrvr-1. Pour cet exemple, un serveur de stockage distant appelé RemoteStore-1 stocke les fichiers de base de données froides, situés dans le répertoire /CA-ELM_cold_storage.

Magasin de journaux d'événements	Valeurs du serveur de collecte	Valeurs du serveur de rapports
Nombre maximum de lignes	2 000 000 (par défaut)	Non applicable pour l'archivage automatique
Nbre max. de jours d'archivage	1 (non applicable pour l'archivage automatique)	30 (applicable pour l'archivage automatique et lorsque celui-ci n'est pas configuré)
Espace disque d'archivage	10	10
Exporter la stratégie	24	72
Port de service sécurisé	17001	17001
<i>Options d'archivage automatique</i>		
Activé	Oui	Oui
Type de sauvegarde	Incrémentiel	Incrémentiel
Fréquence	Toutes les heures	Tous les jours

Magasin de journaux d'événements	Valeurs du serveur de collecte	Valeurs du serveur de rapports
Heure de début	0	23
Utilisateur EEM	<Administrateur_CA Enterprise Log Manager>	<Administrateur_CA Enterprise Log Manager>
Mot de passe EEM	<mot_passe>	<mot_passe>
Serveur distant	RptSrvr-1	RemoteStore-1
Utilisateur distant	caelmservice	user_X
Emplacement distant	/opt/CA/LogManager	/CA-ELM_cold_storage
Serveur CA-ELM distant	Oui	Non

Les options d'archivage automatique de cet exemple déplacent les fichiers d'archive (fichiers de base de données tièdes) du serveur de collecte au serveur de rapports toutes les heures. Cela permet de libérer de l'espace disque pour les événements entrants. Les deux serveurs utilisent une sauvegarde incrémentielle pour ne pas avoir à déplacer des volumes importants de données en une fois. Lorsqu'une base de données tiède est déplacée vers le serveur de rapports, elle est automatiquement supprimée du serveur de collecte.

Remarque : La valeur 0 pour l'Heure de début n'a aucun effet lorsque la fréquence de sauvegarde est paramétrée sur Toutes les heures.

Pour l'Utilisateur EEM et le Mot de passe EEM, vous spécifiez les informations d'identifications d'un utilisateur CA Enterprise Log Manager doté du rôle Administrator prédéfini ou d'un rôle personnalisé, associé à une stratégie personnalisée offrant la possibilité d'effectuer l'action Modifier sur la ressource de la base de données.

Pour le serveur de rapports, spécifiez /opt/CA/LogManager comme Emplacement distant et caelmservice comme Utilisateur distant en cas d'archivage automatique du serveur de rapports vers le serveur de stockage distant. Vous créez ce chemin et cet utilisateur lorsque vous configurez une authentification non interactive entre ces serveurs.

Les options d'archivage automatique de cet exemple déplacent les fichiers d'archive du serveur de rapports vers le serveur de stockage distant tous les jours à partir de 23 h 00. Lorsqu'une base de données est déplacée vers le stockage sauvegardé sur le serveur distant, elle est conservée sur le serveur de rapports pendant le Nbre max. de jours d'archivage.

Si l'archivage automatique n'est pas activé, les bases de données tièdes sont conservées en fonction des seuils configurés pour le Nbre max. de jours d'archivage et l'Espace disque d'archivage, au premier des deux termes échu. Les bases de données archivées peuvent être conservées sur le serveur de rapports pendant 30 jours avant d'être supprimées, sauf si l'espace disque devient inférieur à 10 %. Dans ce cas, le serveur de rapports génère un événement d'autosurveillance et supprime les bases de données les plus anciennes jusqu'à ce que l'espace disque disponible soit supérieur à 10 %. Vous pouvez créer une alerte pour vous avertir de cette situation par courriel ou par flux RSS.

Lorsqu'une base de données est restaurée d'un serveur de stockage distant vers son serveur de rapports d'origine, elle est conservée pendant 3 jours (72 heures).

Vous trouverez plus d'informations sur chacun de ces champs et sur leurs valeurs dans l'aide en ligne.

Définition des options des magasins de journaux d'événements

La boîte de dialogue de configuration Magasin de journaux d'événements vous permet de définir des options globales pour tous les serveurs CA Enterprise Log Manager. Vous pouvez également cliquer sur la flèche en regard de l'entrée pour développer le noeud Magasin de journaux d'événements. Vous affichez ainsi les serveurs CA Enterprise Log Manager individuels de votre réseau. En cliquant sur les noms de ces serveurs, vous pouvez définir des options de configuration locales spécifiques à chaque serveur si vous le souhaitez.

Les utilisateurs dotés du rôle Administrator peuvent configurer n'importe quel serveur CA Enterprise Log Manager à partir de n'importe quel autre serveur CA Enterprise Log Manager.

Pour définir les options des magasins de journaux d'événements

1. Connectez-vous au serveur CA Enterprise Log Manager et sélectionnez l'onglet Administration.

Le sous-onglet Collecte de journaux s'affiche par défaut.

2. Cliquez sur le sous-onglet Services.

3. Sélectionnez l'entrée Magasin de journaux d'événements.

Les options par défaut offrent une bonne configuration de départ pour un réseau de taille moyenne doté d'un débit modéré.

Vous trouverez d'autres informations sur chaque champ dans l'aide en ligne.

Remarque : Les tables Enfants de fédération de serveurs et Archivage automatique s'affichent uniquement lorsque vous affichez les options locales d'un serveur CA Enterprise Log Manager individuel.

Configuration du service de corrélation

Le service de corrélation contrôle le nombre de règles de corrélation et leur application dans votre environnement. Lors de la configuration du service de corrélation, prenez en compte les éléments suivants :

- Déploiement prévu ou non d'un serveur de corrélation dédié
- Noms et les emplacements des serveurs de collecte qui fournissent des événements pour la corrélation
- Types et noms spécifiques des règles de corrélation que vous voulez appliquer dans votre environnement
- Destinations des notifications créées pour votre environnement

Application de règles de corrélation et de notifications d'incidents

Vous devez appliquer des règles de corrélation à votre environnement. Lorsque vous appliquez des règles de corrélation, vous pouvez également associer des destinations de notification pour chaque règle.

Pour appliquer des règles de corrélation et définir des destinations de notification :

1. Cliquez sur Administration, puis sur le sous-onglet Services et développez le noeud Service de corrélation.
2. Sélectionnez le serveur CA Enterprise Log Manager sur lequel vous souhaitez appliquer les règles de corrélation.
Les informations du serveur de corrélations s'affichent dans le volet droit.
3. Cliquez sur Ajouter.
Une boîte de dialogue de règle et de version s'affiche.
4. Activez la case à cocher située à côté de la catégorie de règle ou de la règle à appliquer. Vous pouvez sélectionner l'intégralité des dossiers de catégorie, des règles individuelles ou les deux.
5. Sélectionnez la version de règle dont vous avez besoin pour chaque règle à appliquer.
6. (Facultatif) Sélectionnez une destination de notification pour chacune des règles à appliquer. Si vous ne sélectionnez aucune destination, aucune notification automatique ne sera générée avec la règle. Vous pouvez néanmoins définir manuellement une notification pour les incidents générés par une règle.
7. Sélectionnez les serveurs de collecte pour router les événements pour la corrélation dans la liste des serveurs disponibles. Vous devez sélectionner tous les serveurs auxquels vous voulez envoyer des événements pour la corrélation. Si aucun serveur n'est sélectionné, aucun événement ne sera envoyé pour la corrélation.
8. Cliquez sur OK ou sur Appliquer

Utilisation de règles de corrélation prédéfinies

CA Enterprise Log Manager fournit un grand nombre de règles de corrélation prédéfinies pour une utilisation dans votre environnement, organisées par type ou condition de réglementation. Par exemple, dans le dossier de règles de corrélation de l'interface de la bibliothèque, un dossier intitulé PCI apparaît contenant les règles pour plusieurs conditions PCI. Un dossier intitulé Identité est également créé. Il contient les règles générales relatives à l'autorisation et à l'authentification.

Il existe trois types principaux de règles pouvant être incluses dans chacune des catégories. Cette rubrique propose un exemple de sélection et d'application de chaque type.

Exemple : sélection et application d'une règle simple

Les règles de corrélation simples détectent la présence d'un état ou d'une occurrence. Par exemple, vous pouvez appliquer une règle vous informant sur les activités de création de compte en dehors des heures de bureau habituelles. Avant d'appliquer une règle, créez les destinations de notification dont vous avez besoin pour votre environnement.

Pour sélectionner et appliquer la règle Création de comptes en dehors des heures habituelles de bureau :

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Bibliothèque et développez le dossier Règles de corrélation.
2. Développez le dossier PCI, puis le dossier Condition 8 et sélectionnez la règle Création de comptes en dehors des heures habituelles de bureau.

Les détails de la règle s'affichent dans le volet droit.

3. Vérifiez les informations de la règle et vérifiez qu'elle s'adapte à votre environnement. Si tel est le cas, les filtres définissent l'action de création de compte et définissent les heures de bureau habituelles par heure et jour de la semaine.
4. (Facultatif) Cliquez sur Modifier en haut du volet pour modifier les paramètres de filtre, si nécessaire. Par exemple, vous pouvez changer les heures de travail habituelles et les ajuster aux spécifications régionales.

L'assistant de gestion des règles s'ouvre et affiche les informations détaillées de la règle.

5. Ajoutez tous les détails de notification nécessaires dans le l'assistant de gestion des règles. Les détails de notification fournissent le contenu du message délivré aux destinations de notification.

6. Après avoir préparé la règle, cliquez sur Enregistrer et fermer dans l'assistant. Lorsque vous modifiez et enregistrez une règle de corrélation prédéfinie, CA Enterprise Log Manager crée automatiquement une nouvelle version, en conservant la version originale.
7. Cliquez sur le sous-onglet Services, puis développez le noeud Service de corrélation.
8. Sélectionnez le serveur sur lequel vous voulez appliquer la règle. Si vous avez identifié un serveur de corrélation, sélectionnez-le.
9. Cliquez sur Appliquer dans la zone Configuration de la règle et sélectionnez la nouvelle version de la règle Création de comptes en dehors des heures habituelles de bureau, ainsi que la destination de notification que vous voulez associer.
10. Cliquez sur OK pour fermer la boîte de dialogue et activez la règle.

Exemple : sélection et application d'une règle de comptabilisation

Les règles de corrélation de comptabilisation identifient un ensemble d'états ou d'occurrences identiques. Par exemple, vous pouvez appliquer une règle qui vous informe lorsqu'au moins cinq échecs de connexion se produisent pour un compte d'administrateur. Avant d'appliquer une règle, créez les destinations de notification dont vous avez besoin pour votre environnement.

Pour sélectionner et appliquer la règle 5 échecs de connexion par compte d'administrateur :

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Bibliothèque et développez le dossier Règles de corrélation.
2. Développez le dossier Gestion des menaces, puis le dossier Activité suspecte des compte et des connexions et sélectionnez la règle 5 échecs de connexion par compte d'administrateur.

Les détails de la règle s'affichent dans le volet droit.

3. Vérifiez les informations de la règle et vérifiez qu'elle s'adapte à votre environnement. Dans ce cas, les filtres définissent un compte d'administrateur en tant que nom d'utilisateur appartenant à la liste à clés Administrateurs et ils définissent le seuil sur 5 événements en 60 minutes.
4. (Facultatif) Cliquez sur Modifier en haut du volet pour modifier les paramètres de filtre, si nécessaire. Par exemple, vous pouvez modifier et définir la limite d'heure sur 3 événements en 30 minutes.

L'assistant de gestion des règles s'ouvre et affiche les informations détaillées de la règle.

5. Ajoutez tous les détails de notification nécessaires dans le l'assistant de gestion des règles. Les détails de notification fournissent le contenu du message délivré aux destinations de notification.
6. Après avoir préparé la règle, cliquez sur Enregistrer et fermer dans l'assistant. Lorsque vous modifiez et enregistrez une règle de corrélation prédéfinie, CA Enterprise Log Manager crée automatiquement une nouvelle version, en conservant la version originale.
7. Cliquez sur le sous-onglet Services, puis développez le noeud Service de corrélation.
8. Sélectionnez le serveur sur lequel vous voulez appliquer la règle. Si vous avez identifié un serveur de corrélation, sélectionnez-le.
9. Cliquez sur Appliquer dans la zone Configuration de la règle et sélectionnez la nouvelle version de la règle 5 échecs de connexion par le compte d'administrateur, ainsi que la destination de notification que vous voulez associer.
10. Cliquez sur OK pour fermer la boîte de dialogue et activez la règle.

Exemple : sélection et application d'une règle de transition d'état

Les règles de corrélation de transition d'état identifient une série d'états ou occurrences à tour de rôle. Par exemple, vous pouvez appliquer une règle qui vous informe en cas d'échecs de connexion suivis d'une connexion réussie pour un même compte d'utilisateur. Avant d'appliquer une règle, créez les destinations de notification dont vous avez besoin pour votre environnement.

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Bibliothèque et développez le dossier Règles de corrélation.
2. Développez le dossier Identité, puis le dossier Authentification et sélectionnez la règle Echecs de connexion suivis d'une connexion réussie.
Les détails de la règle s'affichent dans le volet droit.
3. Vérifiez les informations de la règle et vérifiez qu'elle s'adapte à votre environnement. Dans ce cas, le volet de détails affiche les deux états suivis par la règle. Le premier état correspond à cinq échecs de connexions ou plus pour un même compte d'utilisateur ou une même identité. Le deuxième état correspond à une connexion réussie pour un utilisateur ou une identité.
4. (Facultatif) Cliquez sur Modifier en haut du volet pour modifier les paramètres d'état, si nécessaire.
L'assistant de gestion des règles s'ouvre et affiche les deux états qui composent la règle.
5. Double-cliquez sur l'état que vous souhaitez modifier.

L'assistant de définition d'états apparaît et affiche les détails de l'état.

6. Modifiez l'état sélectionné et cliquez sur Enregistrer et fermer pour ouvrir de nouveau l'assistant de gestion des règles. Par exemple, le premier état vérifie la présence de 5 échecs de connexion en 10 minutes. Vous pouvez modifier le seuil d'échecs de connexions, l'heure ou les deux.
7. Ajoutez tous les détails de notification nécessaires dans le l'assistant de gestion des règles. Les détails de notification fournissent le contenu du message délivré aux destinations de notification.
8. Après avoir préparé la règle, cliquez sur Enregistrer et fermer dans l'assistant. Lorsque vous modifiez et enregistrez une règle de corrélation prédéfinie, CA Enterprise Log Manager crée automatiquement une nouvelle version, en conservant la version originale.
9. Cliquez sur le sous-onglet Services, puis développez le noeud Service de corrélation.
10. Sélectionnez le serveur sur lequel vous voulez appliquer la règle. Si vous avez identifié un serveur de corrélation, sélectionnez-le.
11. Cliquez sur Appliquer dans la zone Configuration de la règle et sélectionnez la nouvelle version de la règle Echecs de connexion suivis d'une connexion réussie, ainsi que la destination de notification que vous voulez associer.
12. Cliquez sur OK pour fermer la boîte de dialogue et activez la règle.

Informations complémentaires :

[Application de règles de corrélation et de notifications d'incidents](#) (page 185)

Définition des serveurs de collecte

Vous pouvez définir des serveurs de collecte pour router les événements pour la corrélation dans un environnement multiserveur. La définition de serveurs de collecte permet d'administrer et d'exécuter les règles de corrélation sur un serveur (de corrélation dédié ou avec des rôles partagés). Vous pouvez alors afficher des incidents à partir de tous les serveurs de collecte sélectionnés.

Pour définir des serveurs de collecte :

1. Cliquez sur Administration, puis sur le sous-onglet Services et développez le noeud Service de corrélation.
2. Sélectionnez le serveur CA Enterprise Log Manager vers lequel vous voulez router les événements pour la corrélation. Si vous utilisez un serveur de corrélation dédié, sélectionnez-le.

Les informations du serveur de corrélations s'affichent dans le volet droit.

3. Pour sélectionner les serveurs que vous voulez, utilisez le contrôle de déplacement de serveurs de collecte. Vérifiez que tous les serveurs qui collectent des événements pour la corrélation apparaissent dans la colonne Sélectionné(s).

Conception et application des notifications d'incidents

Vous pouvez configurer des notifications pour les règles de corrélation. Les notifications permettent de transférer des informations clés sur les incidents détectés au personnel spécifié ou de créer des tickets pour le centre de services de CA IT PAM automatiquement.

Utilisez le processus suivant pour concevoir et déclencher des notifications dans votre environnement :

1. Préparez et créez des destinations de notification.
2. Sélectionnez les règles de corrélation prédéfinies ou créez des règles personnalisées pour les utiliser dans votre environnement.
3. Ajoutez les détails de notification aux règles pour lesquelles vous souhaitez définir des notifications.
4. Appliquez les règles de corrélation aux serveurs CA Enterprise Log Manager et affectez les destinations de notification.

Informations complémentaires :

[Création d'une destination de notification](#) (page 191)

[Application de règles de corrélation et de notifications d'incidents](#) (page 185)

Création d'une destination de notification

Vous pouvez créer des objets de destination de notification pour les utiliser dans les règles de corrélation. Les destinations permettent d'appliquer des paramètres de livraison communs à plusieurs règles. Si nécessaire, vous pouvez affecter une destination à plusieurs règles. Vous pouvez les affecter pendant l'application de la règle de corrélation ou après la création d'un incident.

Vous créez un objet de destination de notification en suivant la méthode suivante :

1. Ouvrez l'assistant de destinations de notification et définissez un nom de destination et une description.
2. Définissez les paramètres pour les types de destination souhaités :
 - a. Messagerie électronique
 - b. Processus CA IT PAM
 - c. interruptions SNMP

Un objet de destination de notification peut présenter plusieurs types de notification.

Informations complémentaires :

[Ouverture de l'assistant de destinations de notification](#) (page 191)

[Définition des destinations de courriel](#) (page 192)

[Définition des destination de processus](#) (page 193)

[Définition des destinations SNMP](#) (page 194)

Ouverture de l'assistant de destinations de notification

Pour créer une destination de notification, ouvrez l'assistant.

Pour ouvrir l'assistant de destinations de notification :

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Bibliothèque et ouvrez le dossier Destinations de notification.
2. Cliquez sur Nouvelle notification.

L'assistant de gestion des notifications s'ouvre.

Informations complémentaires :

[Définition des destinations de courriel](#) (page 192)

[Définition des destination de processus](#) (page 193)

[Définition des destinations SNMP](#) (page 194)

Définition des destinations de courriel

Vous pouvez définir des destinations de courriels pour les notifications afin de notifier au personnel concerné les incidents selon leur rôle ou leur responsabilité.

Pour définir des destinations de courriel :

1. Ouvrez l'assistant de gestion des destinations de notification.
2. Définissez les détails d'identification et passez à l'étape Notifications.
3. Cliquez sur l'onglet Courriel et sélectionnez Activer les notifications par courriel.
4. Entrez au moins une adresse électronique de destinataire. Vous pouvez entrer plusieurs adresses en les séparant par des virgules.
5. (Facultatif) Entrez l'adresse électronique de l'expéditeur.
6. Si nécessaire, ajoutez d'autres destinations ou cliquez sur Enregistrer et fermer.

Définition des destination de processus

Vous pouvez définir un processus IT PAM en tant que destination de notification. La notification transfère les informations sur les incidents CA Enterprise Log Manager à CA Service Desk ou aux applications tierces au moyen d'IT PAM. Définissez une destination de processus en identifiant un processus IT PAM valide. Définissez les informations d'incidents qui formeront les paramètres de processus au moyen des détails de notification.

Pour plus d'informations sur les processus IT PAM, consultez le *Manuel d'administration de CA Enterprise Log Manager*.

Pour définir des destinations de processus :

1. Ouvrez l'assistant de gestion des destinations de notification, définissez les détails d'identification et passez à l'étape Notifications.
2. Cliquez sur l'onglet Processus et sélectionnez Activer l'automatisation des processus.
3. Entrez le nom d'un processus IT PAM auquel vous voulez transférer les informations de l'incident, par exemple :
`/CA_ELM/EventAlertOutput`
4. Si nécessaire, ajoutez d'autres destinations ou cliquez sur Enregistrer et fermer.

Définition des destinations SNMP

Vous pouvez définir des destinations SNMP qui vous permettront d'utiliser des interruptions SNMP pour envoyer les informations des incidents à des systèmes de gestion de tierce partie. Pour plus d'informations sur les interruptions SNMP, consultez le *Manuel d'administration de CA Enterprise Log Manager*.

Pour définir des destinations SNMP :

1. Ouvrez l'assistant de gestion des destinations de notification, définissez les détails d'identification et passez à l'étape Notifications.
2. Cliquez sur l'onglet SNMP et sélectionnez Activer l'interruption SNMP.
3. Pour envoyer l'alerte à l'aide de SNMP v3, sélectionnez SNMP v3 (facultatif). La version par défaut est SNMP v2.
4. (Facultatif) Si vous sélectionnez SNMP v3, cliquez sur le bouton Fonctionnalités de sécurité de la version 3 pour définir l'authentification ou le chiffrement dans la boîte de dialogue Paramètres de sécurité.
5. Entrez les informations du serveur de destination et du port de destination pour identifier la cible des événements transmis via SNMP.
6. (Facultatif) Sélectionnez une autre ligne Serveur de destination/Port de destination et entrez une autre paire de valeurs de serveur/port.
7. Si nécessaire, ajoutez d'autres destinations ou cliquez sur Enregistrer et fermer.

Remarques sur le service d'incidents

Vous pouvez contrôler la manière dont le service d'incidents stocke les événements et crée les incidents pour un serveur CA Enterprise Log Manager sélectionné. Vous pouvez définir les valeurs suivantes :

Période d'expiration

Spécifie le nombre de jours de conservation des incidents dans la base de données d'incidents. Si la valeur est définie sur 0, les événements ne seront jamais supprimés. Les incidents expirés ne sont pas affichés.

Valeurs de limite de génération d'incidents

Indique la fréquence à laquelle une règle de corrélation unique peut créer des incidents, pour vous permettre de réduire les incidents multiples superflus. Pour limiter la génération d'incidents, les différentes versions d'une règle sont considérées comme des règles à part. Si vous avez appliqué plusieurs versions de règle à l'environnement, une limite sera fixée pour chaque règle. Les valeurs de limite incluent :

Activé

Indique si les limites de génération d'incidents sont appliquées.

Nombre

Définit une limite de nombre d'incidents générés par une règle unique. Cette valeur utilise la valeur définie pour les heures, si cette valeur est supérieure 0. Si ces nombres sont atteints, le service d'incidents applique la limite définie pour la Durée du blocage. Si vous avez défini le nombre sur 3 et que la période est définie sur 10, la limite s'appliquera dès qu'une règle aura générée plus de 3 incidents en 10 secondes.

Heure

Définit une limite en secondes pour les incidents générés par une règle unique. Cette valeur utilise la valeur définie pour le nombre, si cette valeur est supérieure 0. Si ces nombres sont atteints, le service d'incidents applique la limite définie pour la Durée du blocage. Si vous avez défini le nombre sur 3 et que la période est définie sur 10, la limite s'appliquera dès qu'une règle aura générée plus de 3 incidents en 10 secondes.

Durée du blocage

Spécifie un intervalle en secondes après le blocage de la règle qui ne peut plus créer d'incidents. Lorsque cette limite est atteinte, la règle ne crée plus d'incidents jusqu'à expiration du délai.

Remarques sur le serveur ODBC

Vous pouvez installer un client ODBC ou un client JDBC pour accéder au magasin de journaux d'événements CA Enterprise Log Manager à partir d'une application externe telle que SAP BusinessObjects Crystal Reports.

Vous pouvez effectuer les tâches suivantes depuis cette zone de configuration.

- Activez ou désactivez l'accès d'ODBC et de JDBC au magasin de journaux d'événements.
- Configurez le port de service utilisé pour les communications entre le client ODBC ou JDBC et le serveur CA Enterprise Log Manager.
- Spécifiez si les communications entre le client ODBC ou JDBC et le serveur CA Enterprise Log Manager sont cryptées.

Les descriptions des champs sont les suivantes.

Activer le service

Indique si les clients ODBC et JDBC peuvent accéder aux données dans le magasin de journaux d'événements. Sélectionnez cette case à cocher pour activer l'accès externe aux événements. Désactivez la case pour désactiver l'accès externe.

Le service ODBC n'est actuellement pas compatible avec FIPS. Désactivez cette case à cocher pour empêcher l'accès d'ODBC et de JDBC en cas d'exécution en mode FIPS. Tout accès non conforme aux données de l'événement sera bloqué. Pour désactiver les services ODBC et JDBC pour des opérations en mode FIPS, définissez cette valeur pour *chacun* des serveurs dans une fédération.

Port d'écoute du serveur

Permet de spécifier le numéro de port utilisé par les services ODBC ou JDBC. La valeur par défaut est 17002. Le serveur CA Enterprise Log Manager refuse les tentatives de connexion lorsqu'une valeur différente est spécifiée dans la source de données Windows ou dans la chaîne URL JDBC.

Chiffrement (SSL)

Indique si le chiffrement doit être utilisé pour les communications entre le client ODBC et le serveur CA Enterprise Log Manager. Le serveur CA Enterprise Log Manager refuse les tentatives de connexion lorsque la valeur correspondante dans la source de données Windows ou dans l'URL JDBC est différente de ce paramètre.

Délai d'expiration de la session (en minutes)

Spécifie le nombre de minutes pendant lequel une session inactive reste ouverte avant d'être automatiquement fermée.

Niveau de journal

Définit le type et le niveau de détail enregistrés dans le fichier journal. La liste déroulante est classée dans l'ordre croissant du niveau de détail.

Appliquer à tous les enregistreurs

Détermine si le paramètre Niveau de journal écrase tous les paramètres de journal issus du fichier des propriétés du journal. Ce réglage s'applique uniquement lorsque le paramètre Niveau de journal est inférieur (plus détaillé) au paramètre par défaut.

Remarques sur le serveur de rapports

Le serveur de rapports contrôle l'administration des rapports diffusés de manière automatique, leur aspect au format PDF, ainsi que la conservation des alertes d'action et des rapports. Vous pouvez effectuer les tâches suivantes depuis la zone de configuration du serveur de rapports.

- Contrôler le nom et le logo de l'entreprise, les polices et d'autres paramètres des rapports au format PDF dans la zone Configurations des rapports.
- Définir le nombre total d'alertes d'action conservées et le nombre de jours pendant lequel elles sont conservées dans la zone Conservation d'alerte.

Nombre maximum d'alertes d'action

Définit le nombre maximal d'alertes d'action conservées par le serveur de rapports en vue de leur examen.

Minimum : 50

Maximum : 1000

Durée de conservation des alertes d'action

Définit le nombre de jours maximal pendant lequel les alertes d'action sont conservées.

Minimum : 1

Maximum : 30

- Définir la stratégie de conservation pour chaque type de récurrence de rapport planifié dans la zone Conservation de rapport.

- Déterminer si l'utilitaire de conservation doit rechercher les rapports à supprimer automatiquement sur la base de ces stratégies, et si oui à quelle fréquence. Par exemple, si l'utilitaire de conservation de rapport fonctionne quotidiennement, il supprime chaque jour les rapports qui dépassent l'ancienneté spécifiée.

Configuration de l'abonnement

Après avoir préparé votre architecture d'abonnement, vous pouvez configurer votre environnement CA Enterprise Log Manager pour implémenter les mises à jour d'abonnement.

Vous trouverez ci-après une présentation du processus de configuration de l'abonnement. Pour plus d'informations sur chaque étape, consultez les procédures associées.

1. En utilisant votre architecture d'abonnement comme référence, configurez chaque serveur en tant que proxy ou client d'abonnement. Le cas échéant, spécifiez un ou plusieurs proxys comme proxys hors ligne. Spécifiez chaque serveur comme proxy ou client au niveau local.
2. Configurez des listes de proxys pour les mises à jour de client et de contenu. Vous pouvez spécifier une liste de proxys pour des mises à jour de client au niveau global pour l'ensemble de votre environnement, ou définir des listes de proxys locaux pour chaque serveur. Pour les mises à jour de contenu, vous pouvez spécifier une seule liste de proxys au niveau global.
3. Sélectionnez les modules à télécharger. Vous pouvez sélectionner des modules au niveau global, ou au niveau local pour chacun des serveurs.
4. Définissez votre planification d'abonnement. Vous pouvez définir une planification au niveau global, ou au niveau local pour chacun des serveurs.

Informations complémentaires :

[Configuration d'un proxy d'abonnement en ligne](#) (page 199)

[Configuration d'un proxy d'abonnement hors ligne](#) (page 200)

[Configuration d'un client d'abonnement](#) (page 201)

[Configuration des listes de proxys](#) (page 202)

[Sélection de modules d'abonnement en ligne](#) (page 205)

[Téléchargement et sélection de modules d'abonnement hors ligne](#) (page 207)

[Définition d'une planification d'abonnement](#) (page 209)

Configuration d'un proxy d'abonnement en ligne

Un proxy d'abonnement en ligne contacte le serveur d'abonnement de CA pour télécharger les plus récentes mises à jour de CA Enterprise Log Manager, puis il les distribue vers des clients d'abonnement à tour de rôle.

Si aucun autre proxy n'est configuré ou disponible, le *proxy d'abonnement en ligne par défaut* télécharge les mises à jour vers des clients d'abonnement. Après l'installation, le premier serveur CA Enterprise Log Manager installé est automatiquement défini comme proxy d'abonnement par défaut. Toutefois, vous pouvez spécifier un proxy en ligne comme proxy d'abonnement par défaut. Vous pouvez configurer le proxy d'abonnement par défaut uniquement au niveau global.

Pour configurer un proxy d'abonnement en ligne

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Service d'abonnement.

La fenêtre Configuration globale du service d'abonnement s'affiche.

Remarque : Pour spécifier un proxy d'abonnement par défaut différent de celui configuré dans l'installation, cliquez sur Administration et introduisez le nom de serveur dans le champ Proxy d'abonnement par défaut.

3. Dans la Liste Services, développez le service d'abonnement et sélectionnez le serveur à configurer.

La Configuration du service d'abonnement s'affiche pour le serveur CA Enterprise Log Manager sélectionné.

4. Cliquez sur l'onglet Administration.
5. Désactivez la case à cocher Proxy d'abonnement et sélectionnez Proxy d'abonnement en ligne.
6. Confirmez que l'URL du flux RSS pour les mises à jour d'abonnement est correcte. Si vous voulez que ce proxy utilise un flux RSS différent du paramètre global, basculez vers la configuration locale et entrez l'URL du flux RSS correcte.
7. Si ce serveur doit contacter le serveur d'abonnement CA via un serveur proxy HTTP différent du serveur hérité, passez en configuration locale et configurez le proxy HTTP de votre choix.
8. Cliquez sur Enregistrer.

Informations complémentaires :

[Configuration de l'abonnement](#) (page 198)

Configuration d'un proxy d'abonnement hors ligne

Un proxy d'abonnement hors ligne fournit des mises à jour de CA Enterprise Log Manager à ses clients sans se connecter à Internet. Cette configuration permet d'isoler certains ou l'ensemble des serveurs CA Enterprise Log Manager d'Internet.

Avant d'effectuer une mise à jour d'abonnement hors ligne, copiez manuellement les fichiers de mise à jour hors ligne à partir d'un site FTP de CA vers un proxy hors ligne, à l'aide d'un média physique ou via l'utilitaire scp, inclus dans CA Enterprise Log Manager. Copiez les fichiers de mise à jour vers l'emplacement suivant : /opt/CA/LogManager/data/subscription/offline.

Les clients d'abonnement de serveurs proxys hors ligne sont conçus pour recevoir automatiquement toutes les mises à jour manuellement installées sur le proxy hors ligne, quels que soient les modules sélectionnés pour un client au niveau local. Ainsi, dans un environnement d'abonnement mixte dans lequel vous avez configuré à la fois des proxys en ligne et hors ligne, n'incluez aucun proxy hors ligne dans la liste de proxys pour un client d'abonnement en ligne. Dans le cas contraire, le client d'abonnement en ligne recevra automatiquement toutes les mises à jour manuellement installées sur le serveur proxy hors ligne, au lieu des modules sélectionnés pour ce client.

Pour configurer un proxy d'abonnement hors ligne

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Développez le service d'abonnement et sélectionnez le serveur à configurer.
La Configuration du service d'abonnement s'affiche pour le serveur CA Enterprise Log Manager sélectionné.
3. Cliquez sur l'onglet Administration.
4. Désactivez la case à cocher Proxy d'abonnement et sélectionnez Proxy d'abonnement hors ligne.
5. Dans la liste déroulante Fichier, sélectionnez le fichier .zip contenant les fichiers d'abonnement hors ligne que vous voulez installer.

Remarque : Pour appliquer cette procédure, vous devez avoir copié le package d'abonnement hors ligne vers l'emplacement correct sur ce serveur. Si ce n'est pas le cas, une invite s'affichera.

6. Cliquez sur Enregistrer.

Informations complémentaires :

[Configuration de l'abonnement](#) (page 198)

Configuration d'un client d'abonnement

Les clients d'abonnement téléchargent les mises à jour de CA Enterprise Log Manager les plus récentes à partir des proxys d'abonnement. Après la récupération de mises à jour, le client installe les composants téléchargés.

Par défaut, tous les serveurs CA Enterprise Log Manager non configurés en tant que proxys d'abonnement sont des clients d'abonnement. Il n'est pas nécessaire de configurer un serveur au niveau local en tant que client, excepté si vous voulez remplacer des paramètres d'abonnement que vous avez définis au niveau global.

Un client d'abonnement ne peut pas récupérer les mises à jour à partir d'un proxy d'abonnement avant que celui-ci ait lui-même téléchargé et installé ces mises à jour. Un client tente de récupérer des mises à jour à partir de chaque serveur figurant sur sa liste de proxys configurés, l'un après l'autre. Si aucun proxy n'a terminé l'installation des mises à jour demandées par le client, celui-ci renouvelle la demande toutes les 5 minutes jusqu'à ce que l'installation de la mise à jour soit terminée. Si le client ne peut pas télécharger les mises à jour après une heure de tentatives, la mise à jour est annulée et le client renouvellera la demande de mise à jour à la date planifiée suivante. Tout au long de ce processus, des messages s'affichent dans le journal d'événements d'autosurveillance, informant de l'état de la mise à jour.

Pour configurer un client d'abonnement

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Développez le service d'abonnement et sélectionnez le serveur à configurer.
La Configuration du service d'abonnement s'affiche pour le serveur CA Enterprise Log Manager sélectionné.
3. Identifiez le serveur sélectionné en tant que client en désactivant la case à cocher Proxy d'abonnement.
4. Les clients d'abonnement contactent les proxys d'abonnement via le réseau interne, il n'est donc pas nécessaire de configurer des paramètres de proxy HTTPS locaux pour un serveur client.
5. Cliquez sur Enregistrer.

Informations complémentaires :

[Configuration de l'abonnement](#) (page 198)

Configuration des listes de proxys

Si vous configurez plusieurs proxys d'abonnement pour votre environnement, vous pouvez configurer des listes de proxys pour des mises à jour de client. Si un proxy spécifique n'est pas disponible lors de la demande de mises à jour par un client, celui-ci contacte chaque proxy figurant sur sa liste de proxys, jusqu'à ce qu'il parvienne à les télécharger. Vous pouvez configurer une liste de proxys pour obtenir des mises à jour de client au niveau global pour l'ensemble de votre environnement CA Enterprise Log Manager, ou au niveau local pour des clients d'abonnement spécifiques.

Si vous disposez de plusieurs proxys d'abonnement, vous pouvez également configurer une liste de proxys pour obtenir des mises à jour de contenu. Il s'agit de serveurs qui reçoivent des mises à jour de contenu, tels que des requêtes, des rapports et des règles de corrélation, puis qui les distribuent au serveur de gestion sur lequel elles seront stockées et utilisée par CA Enterprise Log Manager. Vous pouvez configurer une liste de proxys pour obtenir des mises à jour de contenu uniquement au niveau global.

Les listes de proxys permettent d'assurer que les mises à jour d'abonnement soient récupérées et distribuées en temps voulu. Même dans un environnement CA Enterprise Log Manager de petite taille, il est recommandé de configurer au moins un proxy de sauvegarde pour les mises à jour de client et de contenu, au cas où le proxy principal deviendrait indisponible.

Pour configurer une liste de proxys :

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Service d'abonnement.

La Configuration globale du service d'abonnement s'affiche.

3. Effectuez l'une des opérations suivantes :

- Pour spécifier une liste de proxys globaux pour l'ensemble de l'environnement CA Enterprise Log Manager, cliquez sur l'onglet Administration.

ou

- Pour spécifier une liste de proxys locaux pour un client d'abonnement spécifique, cliquez sur le nom du serveur, puis accédez à l'onglet Administration et passez en configuration locale.

4. Ajoutez les serveurs proxys de votre choix aux listes de proxys.

Important : Dans un environnement d'abonnement mixte, dans lequel vous avez configuré à la fois des proxys d'abonnement en ligne et hors ligne, n'incluez aucun proxy hors ligne dans la liste de proxys pour un client d'abonnement en ligne. Dans le cas contraire, le client d'abonnement en ligne recevra automatiquement toutes les mises à jour manuellement installées sur le serveur proxy hors ligne, au lieu des modules sélectionnés.

5. Cliquez sur Enregistrer.

Informations complémentaires :

[Configuration de l'abonnement](#) (page 198)

Modules à télécharger

Les mises à jour sont mises en package dans *des modules*, téléchargés via le serveur d'abonnement CA. Vous pouvez accéder à la liste des modules disponibles via l'URL d'un flux RSS fournie par CA, ou dans le cas d'un abonnement hors ligne, via un site FTP de CA. CA détermine le contenu de chaque module.

Le tableau suivant décrit chaque module, sa fonction et la fréquence à laquelle CA met à disposition des mises à jour.

Type de module	Description	Fréquence
Contenu	Met à jour la liste de requêtes, la liste de rapports et les règles de corrélation avec le nouveau contenu. Le serveur proxy de mise à jour du contenu envoie automatiquement ce contenu au niveau du référentiel du serveur de gestion.	Tous les mois

Type de module	Description	Fréquence
Intégrations	Met à jour les connecteurs lorsque vous exécutez l'Assistant d'abonnement et sélectionnez les mises à jour de connecteur.	Tous les mois
Système d'exploitation	Met à jour le système d'exploitation installé sur chaque serveur CA Enterprise Log Manager.	Régulièrement
Agents	Met à jour les agents lorsque vous exécutez l'Assistant d'abonnement et sélectionnez les mises à jour d'agent.	Régulièrement
Service Pack du gestionnaire de journaux	Met à jour le produit CA Enterprise Log Manager sur chaque serveur avec le service Pack indiqué.	Trimestrielle
Version du gestionnaire de journaux	Met à niveau le produit CA Enterprise Log Manager sur chaque système vers la version indiquée.	Régulièrement

Vous pouvez sélectionner la liste des modules à télécharger pour votre environnement CA Enterprise Log Manager au niveau global. Chaque proxy d'abonnement et serveur client hérite de ces paramètres globaux. Vous pouvez également remplacer les paramètres globaux en configurant une liste locale de modules à télécharger pour un serveur CA Enterprise Log Manager particulier.

Remarque : Un proxy d'abonnement ne peut pas distribuer un module vers un client que le proxy n'a pas lui-même installé. Lors de la sélection des modules pour un proxy d'abonnement, incluez au moins tous les modules sélectionnés pour les clients du proxy.

Vous pouvez effectuer les mises à jour dans l'environnement CA Enterprise Log Manager à l'aide de l'une des méthodes suivantes (ou des deux) :

1. Mise à jour automatique : sélectionnez des modules en avance, puis spécifiez une planification pour le téléchargement. Le service d'abonnement télécharge et installe automatiquement les modules sélectionnés, selon la planification spécifiée.
2. Mise à jour manuelle : sélectionnez des modules lorsque vous en avez besoin, à l'aide de la fonctionnalité Mettre à jour du service d'abonnement pour télécharger et pour installer ces modules à un moment déterminé.

Les modules de contenu, d'intégration, de système d'exploitation et d'agent étant régulièrement mis à jour, il est recommandé de définir une planification d'abonnement pour télécharger ces modules automatiquement au moins une fois par mois. Les mises à jour du service Pack et de la version du gestionnaire de journaux sont moins fréquentes et peuvent requérir des vérifications et une planification supplémentaires avant de les appliquer à votre environnement de CA Enterprise Log Manager. Si nécessaire, vous pouvez télécharger ces types de mises à jour manuellement.

Dès que de nouveaux modules sont disponibles, ils s'affichent dans le flux RSS d'abonnement, ou dans le cas d'un abonnement hors ligne, sur le site FTP d'abonnement hors ligne de CA. Les modules disponibles pour le téléchargement varient en fonction du cycle de mise à jour ; vérifiez donc la liste des modules disponibles pour vous assurer que tous les modules requis sont sélectionnés. Vous pouvez également visiter le site du support CA à l'adresse www.ca.com/worldwide pour connaître la date de disponibilité des nouveaux services Packs et versions du gestionnaire de journaux.

Informations complémentaires :

[Sélection de modules d'abonnement en ligne](#) (page 205)

[Téléchargement et sélection de modules d'abonnement hors ligne](#) (page 207)

[Planification des mises à jour d'abonnement](#) (page 54)

[Configuration de l'abonnement](#) (page 198)

Sélection de modules d'abonnement en ligne

Les mises à jour d'abonnement de CA Enterprise Log Manager actuellement disponibles sont répertoriées dans le flux RSS fourni par CA. L'URL du flux RSS est fournie par défaut dans l'onglet Administration du service d'abonnement lors de l'installation.

Dès que les nouveaux modules sont disponibles, ils apparaissent dans le flux RSS d'abonnement. Surveillez régulièrement la liste des modules disponibles pour vérifier que tous les modules nécessaires sont sélectionnés. Vous pouvez également visiter le site du support CA à l'adresse www.ca.com/worldwide pour connaître la date de disponibilité des nouveaux services Packs et versions du gestionnaire de journaux.

Pour sélectionner les modules à télécharger :

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Service d'abonnement.

La Configuration globale du service d'abonnement s'affiche.

3. Effectuez l'une des opérations suivantes :
 - Pour sélectionner des modules à télécharger au niveau global pour l'ensemble de l'environnement CA Enterprise Log Manager, cliquez sur l'onglet Administration.

ou

 - Pour sélectionner des modules à télécharger au niveau local pour un serveur spécifique, cliquez sur le nom du serveur, puis sur l'onglet Administration. Définissez la configuration locale dans la section Modules sélectionnés pour le téléchargement.

4. Confirmez que l'adresse RSS affichée dans le champ URL du flux RSS est correcte, ou pour configurer une adresse RSS personnalisée pour un serveur spécifique, basculez vers la configuration locale et entrez l'URL du flux RSS.
5. Cliquez sur Parcourir.

La boîte de dialogue Modules disponibles pour le téléchargement s'affiche.
6. Sélectionnez les modules à télécharger.

Remarque : Pour recevoir de nouvelles mises à jour de CA dès leur disponibilité, sélectionnez des modules mensuels et périodiques et définissez la planification d'abonnement pour télécharger les modules automatiquement au moins une fois par mois. Les mises à jour de Service Packs et de versions sont moins fréquentes et requièrent un examen supplémentaire et une planification préalable à leur application à l'environnement de CA Enterprise Log Manager. Si nécessaire, vous pouvez télécharger ces types de mises à jour manuellement.

Remarque : Les clients ne peuvent pas télécharger de modules non téléchargés par leur proxy. Veillez à ce que les modules sélectionnés pour un proxy d'abonnement incluent au minimum tous les modules sélectionnés dans les listes de téléchargement des clients de ce proxy.
7. Cliquez sur OK.

La boîte de dialogue Modules disponibles pour le téléchargement se ferme et les modules que vous avez sélectionnés s'affichent dans la liste Modules sélectionnés pour le téléchargement.
8. Cliquez sur Enregistrer.

Informations complémentaires :

[Configuration de l'abonnement](#) (page 198)

[Modules à télécharger](#) (page 203)

Téléchargement et sélection de modules d'abonnement hors ligne

Les fichiers de mise à jour d'abonnement hors ligne sont disponibles sur le site FTP d'abonnement hors ligne de CA, sous forme de fichiers .zip. Lorsque de nouveaux modules sont disponibles, ils apparaissent sur le site FTP. Surveillez régulièrement la liste de modules disponibles afin de télécharger les plus récentes mises à jour. Vous pouvez également visiter le site du support CA à l'adresse www.ca.com/worldwide pour connaître la date de disponibilité des nouveaux services Packs et versions du gestionnaire de journaux.

Pour pouvoir sélectionner des modules à télécharger pour des proxys d'abonnement hors ligne, téléchargez le package de fichiers de mise à jour hors ligne à partir du site FTP de CA et copiez-le manuellement vers vos proxys hors ligne. Vous pourrez alors sélectionner les modules à télécharger et à installer. En revanche, les clients d'abonnement hors ligne reçoivent automatiquement toutes les mises à jour, qui sont installées manuellement sur leur proxy hors ligne, quels que soient les modules sélectionnés pour le client au niveau local.

Pour télécharger et sélectionner des modules d'abonnement hors ligne :

1. Sur un système disposant d'un accès Internet ou FTP, accédez au site d'abonnement hors ligne FTP :

```
ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription
```

L'index de répertoires contient un dossier pour chaque version majeure de CA Enterprise Log Manager.

2. Téléchargez le fichier .zip correspondant à la mise à jour que vous voulez effectuer.

Remarque : Le dossier de la version r12.5 de CA Enterprise Log Manager contient un sous-dossier ainsi qu'un fichier .zip. Le sous-dossier contient des modules de mise à niveau à partir d'une version antérieure à la version r12.5. Le fichier .zip contient les modules permettant d'effectuer des mises à jour de routine et régulières vers la version r12.5. Si vous utilisez l'abonnement hors ligne pour la mise à niveau à partir d'une version antérieure à r12.5, reportez-vous à la section Mise à niveau vers CA Enterprise Log Manager des *Notes de parution*. Si vous effectuez une mise à jour de routine, sélectionnez le fichier .zip.

3. A l'aide d'un média physique (par exemple, un disque) ou de l'utilitaire scp, copiez manuellement le fichier .zip vers l'emplacement du fichier suivant sur vos proxys hors ligne :

/opt/CA/LogManager/data/subscription/offline.

4. Connectez-vous à un système dans votre environnement CA Enterprise Log Manager.
5. Cliquez sur l'onglet Administration et le sous-onglet Services.
6. Développez le service d'abonnement et sélectionnez le serveur proxy hors ligne à configurer.

La fenêtre de configuration du service d'abonnement s'affiche pour le serveur CA Enterprise Log Manager sélectionné.

Remarque : Les clients d'abonnement hors ligne reçoivent automatiquement tous les modules, qui sont manuellement installés sur leur proxy hors ligne. Le contenu du serveur proxy contrôle les mises à jour reçues par le client d'abonnement. Les modules sélectionnés au niveau local pour un client hors ligne n'ont aucun impact.

7. Cliquez sur l'onglet Administration.
8. Dans la liste déroulante Fichier, sélectionnez le fichier .zip de mise à jour hors ligne que vous avez copié vers le serveur, puis cliquez sur Parcourir.
La boîte de dialogue Modules disponibles pour le téléchargement s'affiche.
9. Sélectionnez les modules à télécharger.
10. Cliquez sur OK.

La boîte de dialogue Modules disponibles pour le téléchargement se ferme et les modules que vous avez sélectionnés s'affichent dans la liste Modules sélectionnés pour le téléchargement.

11. Cliquez sur Enregistrer.

Les clients d'abonnement hors ligne peuvent désormais télécharger automatiquement ces modules en fonction de la planification d'abonnement définie, ou à la demande lors du lancement d'une mise à jour manuelle.

12. (facultatif) Cliquez sur Mettre à jour.

Le serveur proxy hors ligne effectue lui-même sa mise à jour avec les modules sélectionnés.

Remarque : Même si vous pouvez autoriser la mise à jour par le proxy hors ligne en fonction de la planification de l'abonnement définie, il est recommandé d'effectuer une mise à jour manuelle lors du transfert de nouveaux fichiers. Cela permet d'assurer que les mises à jour sont disponibles lorsque les clients d'abonnement hors ligne en font la demande.

Informations complémentaires :

[Configuration de l'abonnement](#) (page 198)

[Modules à télécharger](#) (page 203)

Définition d'une planification d'abonnement

Vous pouvez définir une planification d'abonnement pour déterminer la date et la fréquence des mises à jour automatiques qui seront effectuées par le service d'abonnement. Vous pouvez définir une planification d'abonnement au niveau global, pour l'ensemble de votre environnement CA Enterprise Log Manager, ou définir une planification personnalisée pour des proxys d'abonnement et des clients particuliers.

Pour configurer une planification d'abonnement :

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Service d'abonnement.

La Configuration globale du service d'abonnement s'affiche.

3. Effectuez l'une des opérations suivantes :
 - Pour spécifier une planification d'abonnement globale pour l'ensemble de l'environnement CA Enterprise Log Manager, cliquez sur l'onglet Administration.

ou

 - Pour spécifier une planification d'abonnement locale pour un serveur spécifique, cliquez sur le nom du serveur, puis accédez à l'onglet Administration et passez en configuration locale.

4. Définissez la planification d'abonnement. Sélectionnez le fuseau horaire et une heure de début pour les mises à jour, puis spécifiez la fréquence de mise à jour souhaitée.

Informations complémentaires :

[Configuration de l'abonnement](#) (page 198)

Chapitre 6 : Configuration de la collecte d'événements

Ce chapitre traite des sujets suivants :

[Installation d'agents](#) (page 211)

[Utilisation de l'Explorateur d'agent](#) (page 212)

[Configuration de l'agent par défaut](#) (page 213)

[Exemple : Activation de la collecte directe à l'aide du détecteur ODBCLogSensor](#) (page 216)

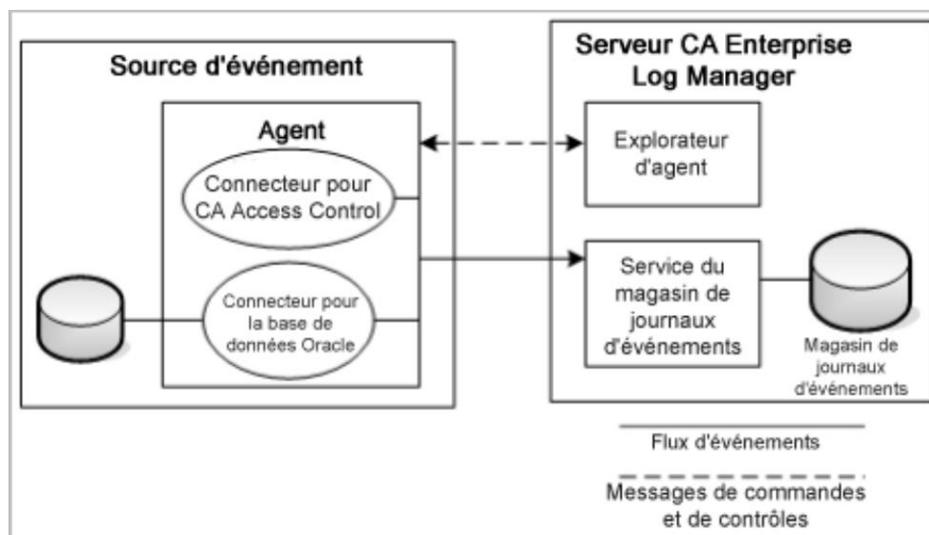
[Exemple : Activation de la collecte directe à l'aide du détecteur](#)

[WinRMLinuxLogSensor](#) (page 223)

[Affichage et contrôle de l'état d'un agent ou d'un connecteur](#) (page 229)

Installation d'agents

Grâce aux installations distinctes pour des plates-formes spécifiques, les agents CA Enterprise Log Manager apportent la couche transport qui permet de transmettre les événements des sources d'événement au magasin de journaux d'événements du serveur CA Enterprise Log Manager. Les agents utilisent des connecteurs pour collecter des journaux d'événements provenant de différentes sources d'événement. Le diagramme qui suit illustre les interactions entre les agents et le serveur CA Enterprise Log Manager.



Après avoir installé un agent sur une source d'événement, vous pouvez configurer un ou plusieurs connecteurs pour collecter des événements provenant de sources d'événement telles que des unités, des applications, des systèmes d'exploitation et des bases de données. Les exemples du diagramme incluent des connecteurs pour CA Access Control et une base de données Oracle. En général, vous installez un seul agent par serveur hôte ou source d'événement, mais vous pouvez configurer plusieurs types de connecteurs sur cet agent. Vous pouvez utiliser l'Explorateur d'agent, qui fait partie du serveur CA Enterprise Log Manager, pour contrôler les agents ainsi que pour configurer et contrôler des connecteurs sur un agent. L'Explorateur d'agent vous permet également de créer des groupes d'agents, pour simplifier la gestion et le contrôle.

Vous fondez votre configuration d'un connecteur sur une intégration ou sur un écouteur, qui sont des modèles pouvant comprendre des fichiers d'accès aux données, d'analyse de message et de mappage de données. CA Enterprise Log Manager propose un certain nombre d'intégrations prêtes à l'emploi pour les sources d'événement courantes.

Vous trouverez plus d'informations et les procédures d'installation des agents dans le *Manuel d'installation des agents CA Enterprise Log Manager*.

Informations complémentaires :

[Affichage et contrôle de l'état d'un agent ou d'un connecteur](#) (page 229)

Utilisation de l'Explorateur d'agent

Juste après l'installation d'un serveur CA Enterprise Log Manager, un agent par défaut s'affiche dans l'Explorateur d'agent. Cet agent est installé en même temps que le serveur CA Enterprise Log Manager et vous l'utilisez pour la collecte directe d'événements Syslog.

L'Explorateur d'agent suit et répertorie les agents lorsque vous les installez sur votre réseau ; il constitue également une place centrale pour la configuration, les commandes et le contrôle des agents et des connecteurs. Les agents s'enregistrent auprès du serveur CA Enterprise Log Manager spécifié lorsque vous les démarrez pour la première fois. Après cet enregistrement, le nom de l'agent s'affiche dans l'Explorateur d'agent et vous pouvez configurer un connecteur pour commencer la collecte des journaux d'événements. Les connecteurs collectent les journaux d'événements et les envoient au serveur CA Enterprise Log Manager. Un agent peut contrôler plusieurs connecteurs.

L'utilisation de l'Explorateur d'agent pour installer, configurer et contrôler des connecteurs et des agents implique les étapes de base ci-après.

1. Téléchargez les fichiers binaires de l'agent.
2. Créez un ou plusieurs groupes d'agents (facultatif).
3. Créez et configurez un connecteur, notamment en créant ou en appliquant des règles de suppression et de récapitulation.
4. Affichez l'état des agents ou des connecteurs.

Reportez-vous au *Manuel d'administration CA Enterprise Log Manager* pour plus d'informations sur la création et l'utilisation des groupes d'agents et des connecteurs, ainsi que sur l'application de règles de suppression aux agents.

Informations complémentaires :

[A propos des agents](#) (page 66)

[A propos des groupes d'agents](#) (page 67)

[A propos des détecteurs de journaux](#) (page 69)

[Effets des règles de suppression](#) (page 71)

Configuration de l'agent par défaut

L'installation de CA Enterprise Log Manager crée sur le serveur CA Enterprise Log Manager un agent par défaut dotés de deux connecteurs prêts à l'emploi, un connecteur Syslog et un connecteur Linux_local. Le connecteur Syslog permet de collecter les événements Syslog transmis au serveur CA Enterprise Log Manager. Le connecteur Linux_local permet de collecter les événements au niveau du système d'exploitation à partir du serveur physique CA Enterprise Log Manager ou d'un fichier Syslog.

Dans l'environnement de base comprenant deux serveurs, configurez un ou plusieurs connecteurs Syslog sur le serveur de collecte pour recevoir des événements.

Le processus d'utilisation de l'agent par défaut inclut les étapes ci-dessous.

1. Examinez les intégrations et écouteurs Syslog (facultatif).
2. Créez un connecteur Syslog.
3. Vérifiez que le serveur CA Enterprise Log Manager reçoit les événements Syslog.

Examen des intégrations et écouteurs Syslog

Vous pouvez examiner les intégrations et écouteurs Syslog par défaut avant de créer un connecteur. Les écouteurs sont pour l'essentiel un modèle pour vos connecteurs Syslog qui utilisent des intégrations spécifiques fournies comme du contenu prêt à l'emploi avec votre serveur CA Enterprise Log Manager.

Pour examiner les intégrations Syslog

1. Connectez-vous à CA Enterprise Log Manager et accédez à l'onglet Administration.
2. Cliquez sur le sous-onglet Bibliothèque et développez le noeud Bibliothèque d'ajustement d'événement.
3. Développez le noeud Intégrations et le noeud Abonnement.
4. Sélectionnez une intégration dont le nom se termine par ..._Syslog.

Les détails de l'intégration s'affichent dans la fenêtre de droite. Vous pouvez examiner les fichiers d'analyse de message et de mappage de données utilisés par l'intégration, ainsi que d'autres détails, comme la version et les listes de règles de suppression et de récapitulation.

Pour examiner un écouteur Syslog

1. Développez le noeud Ecouteurs et le noeud Abonnement.
2. Sélectionnez l'écouteur Syslog.

Les détails de l'écouteur par défaut s'affichent dans la fenêtre de droite. Vous pouvez examiner les détails comme les versions, les règles de suppression et de récapitulation, les ports par défaut sur lesquels écouter, la liste des hôtes fiables et le fuseau horaire de l'écouteur.

Création d'un connecteur Syslog pour l'agent par défaut

Vous pouvez créer un connecteur Syslog pour recevoir les événements Syslog à l'aide de l'agent par défaut sur le serveur CA Enterprise Log Manager.

Pour créer un connecteur Syslog pour l'agent par défaut

1. Connectez-vous à CA Enterprise Log Manager et accédez à l'onglet Administration.
2. Développez l'Explorateur d'agent et un groupe d'agents.

L'agent par défaut est automatiquement installé dans le groupe d'agents par défaut. Vous pouvez déplacer cet agent vers un autre groupe.

3. Sélectionnez le nom de l'agent.
L'agent par défaut porte le même nom que celui attribué au serveur CA Enterprise Log Manager lors de l'installation.
4. Cliquez sur Créer un connecteur pour ouvrir l'assistant du connecteur.
5. Cliquez sur l'option Ecouteurs et indiquez un nom pour ce connecteur.
6. Appliquez les règles de suppression et de récapitulation selon vos besoins, dans les deuxièmes et troisièmes pages de l'assistant.
7. Sélectionnez une ou plusieurs intégrations Syslog ciblées dans la liste Disponible(s) pour les utiliser avec ce connecteur, puis déplacez-les dans la liste Sélectionné(e)(s).
8. Paramétrez les valeurs des ports UDP et TCP si vous n'utilisez pas les paramètres par défaut, puis fournissez une liste d'hôtes fiables si votre implémentation les utilise.

Remarque : Lorsqu'un agent CA Enterprise Log Manager ne s'exécute pas en tant que root, il ne peut pas ouvrir de port en deçà de 1024. C'est pourquoi le connecteur Syslog par défaut utilise le port UDP 40514. L'installation applique une règle de pare-feu au serveur CA Enterprise Log Manager pour rediriger le trafic du port 514 vers le port 40514.

9. Sélectionnez un fuseau horaire.
10. Cliquez sur Enregistrer, puis sur Fermer pour terminer la création du connecteur.

Le connecteur commence à collecter les événements Syslog correspondant aux intégrations sélectionnées sur les ports spécifiés.

Vérification de la réception des événements Syslog par le serveur CA Enterprise Log Manager

Vous pouvez vérifier que le connecteur de l'agent par défaut collecte les événements Syslog grâce à la procédure ci-dessous.

Pour vérifier la réception d'événements Syslog

1. Connectez-vous à CA Enterprise Log Manager et accédez à l'onglet Requêtes et rapports.

2. Sélectionnez l'onglet des requêtes du système et ouvrez la requête Détail de tous les événements du système.

Vous devez visualiser les événements répertoriés pour l'agent par défaut, si vous avez configuré correctement le connecteur et si la source d'événement envoie activement des événements.

Exemple : Activation de la collecte directe à l'aide du détecteur ODBCLogSensor

Vous pouvez activer la collecte directe des événements générés par des bases de données spécifiques et les produits CA à l'aide du détecteur ODBCLogSensor. Pour y parvenir, créez un connecteur sur l'agent par défaut basé sur une intégration qui utilise le détecteur ODBCLogSensor. De nombreuses intégrations utilisent ce détecteur, par exemple, CA_Federation_Manager, CAIdentityManager, Oracle10g, Oracle9i et MS_SQL_Server_2005.

Vous trouverez ci-dessous une liste partielle des produits qui génèrent des événements pouvant être collectés directement par l'agent par défaut sur un serveur CA Enterprise Log Manager. Un connecteur unique est utilisé pour chaque produit ; chaque connecteur utilise le détecteur ODBCLogSensor.

- CA Federation Manager
- CA SiteMinder
- CA Identity Manager
- Oracle 9i et 10g
- Microsoft SQL Server 2005

Pour obtenir une liste complète, consultez la [Matrice d'intégration de produits](#) sur le support en ligne.

Cet exemple décrit l'activation de la collecte directe des événements à partir d'une base de données Microsoft SQL Server. Le connecteur déployé sur l'agent par défaut est fondé sur l'intégration MS_SQL_Server_2005. Dans cet exemple, la base de données SQL Server se trouve sur un serveur ODBC. Le connecteur déployé dans l'agent CA Enterprise Log Manager collecte des événements à partir de la table MSSQL_TRACE. Une partie de l'activation de la collecte d'événements à partir d'une base de données Microsoft SQL Server consiste à diriger des événements sélectionnés vers cette table de trace. Vous trouverez des instructions explicites pour y parvenir dans le *manuel du connecteur CA pour Microsoft SQL Server*.

Pour configurer la source d'événement Microsoft SQL Server :

1. Cliquez sur l'onglet Administration et le sous-onglet Bibliothèque.
2. Développez Bibliothèque d'ajustement d'événement, Intégrations, Abonnement, puis sélectionnez MS_SQL_Server_2005.

La fenêtre Afficher les détails de l'intégration indique le nom du détecteur, à savoir ODBCLogSensor. Windows et Linux sont les deux plateformes prises en charge.

3. Cliquez sur le lien Aide de la fenêtre Afficher les détails de l'intégration WinRM.

Le manuel du connecteur pour Microsoft SQL Server s'affiche.

4. Consultez les sections concernant les éléments prérequis et la configuration de Microsoft SQL Server pour de plus amples instructions.

Pour configurer la source d'événement et vérifier la journalisation :

1. Rassemblez les informations suivantes : l'adresse IP du serveur ODBC, le nom de la base de données, le nom d'utilisateur et le mot de passe de l'administrateur requis pour la connexion au serveur, ainsi que les informations de connexion de l'utilisateur à faibles privilèges utilisé pour l'authentification SQL Server (il s'agit de l'utilisateur défini ayant un accès en lecture seule à la table de trace).
2. Connectez-vous au serveur ODBC en utilisant le nom d'utilisateur et le mot de passe de l'administrateur.
3. Assurez la connectivité via TCP/IP, tel que spécifié dans le *manuel du connecteur pour Microsoft SQL Server*.
4. Configurez le serveur SQL et vérifiez que les événements sont dirigés vers la table de trace, tel que spécifié dans le *manuel du connecteur pour Microsoft SQL Server*.

Remarque : Conservez le nom de la base de données sur laquelle vous avez créé la table de trace. Vous devez spécifier ce nom de base de données dans la chaîne de connexion. Par exemple : master.

Pour créer un connecteur sur l'agent par défaut afin de récupérer des événements générés par une base de données SQL Server sur un serveur ODBC :

1. Sélectionnez l'onglet Administration, puis le sous-onglet Collecte de journaux.
2. Développez Explorateur d'agent, puis le groupe d'agents qui contient l'agent par défaut CA Enterprise Log Manager.
3. Sélectionnez un agent par défaut, c'est-à-dire, un agent portant le nom d'un serveur CA Enterprise Log Manager.
D'autres connecteurs peuvent être déployés sur l'agent par défaut.
4. Cliquez sur Créer un connecteur.



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

5. Dans la liste déroulante Intégration, sélectionnez l'intégration MS_SQL_Server_2005.

Cette sélection renseigne le champ Nom du connecteur avec la valeur MS_SQL_Server_2005_Connecteur.

6. Remplacez le nom par défaut par un autre permettant d'identifier le connecteur plus facilement (facultatif). Pensez à fournir un nom unique si vous surveillez plusieurs bases de données SQL Server ayant le même agent.



7. Cliquez sur Appliquer les règles de suppression et sélectionnez les règles associées aux événements pris en charge (facultatif).

Par exemple, sélectionnez MSSQL_2005_Authorization 12.0.44.12.

8. Cliquez sur l'étape Configuration du connecteur, puis cliquez sur le lien Aide.

Les Instructions incluent les éléments requis pour la configuration des détecteurs CA Enterprise Log Manager pour Windows et Linux.

9. Consultez les étapes pour Linux, la plateforme de l'agent par défaut, puis configurez la Chaîne de connexion et les autres champs, tel que spécifié.
 - a. Saisissez la chaîne de connexion comme indiqué à la section Configuration des détecteurs--Linux, l'adresse étant le nom d'hôte ou l'adresse IP de la source d'événement et la base de données étant la base de données SQL Server sous laquelle MSSQLSERVER_TRACE est créée.

DSN=SQLServer Wire
Protocol;Address=Adresse_IP,port;Database=nom_base_de_données

- b. Indique le nom de l'utilisateur disposant de droits d'accès en lecture seule à la collecte des événements. L'utilisateur doit posséder les rôles db_datareader et public pour disposer d'un accès en lecture seule.
- c. Saisissez le mot de passe du nom d'utilisateur spécifié.
- d. Spécifiez le fuseau horaire de la base de données, avec un décalage par rapport à l'heure GMT.

Remarque : Sur un serveur Windows, ces informations apparaissent dans l'onglet Fuseau horaire des propriétés Date et heure. Ouvrez l'horloge dans la barre d'état système.

- e. Sélectionnez ou désactivez Lecture à partir du début, si vous voulez que le détecteur de journaux lise ou non les événements à partir du début de la base de données.

Voici un exemple partiel :

Configuration des détecteurs

• Chaîne de connexion: DSN=SQLServer Wire Protocol;Address=172.24.36.107,1433;Database=master

• Nom de l'utilisateur: ELMsqagent

• Mot de passe: *****

Signe pour le décalage horaire: +

Heures de décalage horaire: 0

Minutes de décalage horaire: 0

• Nom du journal d'événements: MS_SQL_Server

• Mise à jour du taux d'ancrage: 10

• Intervalle d'interrogation: 10

• Nombre maximum d'événements par seconde: 1000

Lecture à partir du début

10. Cliquez sur Enregistrer et fermer.

Le nouveau nom du connecteur s'affiche sous l'agent dans l'Explorateur d'agent.



11. Cliquez sur MS_SQL_Server_2005_Connector pour afficher les détails de l'état.

Au début, l'état indique Configuration en attente. Attendez jusqu'à ce que l'état affiche Exécution en cours.

Connecteur	Agent	Groupe d'agents	Plate-forme	Intégration	Etat
MS_SQL_Server_2005_コネクター	ca-elm	Default Agent Group	Linux_X86_32	MS_SQL_Server_2005	Exécution en cours

12. Sélectionnez le connecteur et cliquez sur Exécution en cours pour afficher les détails de la collecte d'événements.

Remarque : Vous pouvez également exécuter un rapport pour afficher des données à partir de cette base de données.

Pour vérifier que l'agent par défaut collecte des événements à partir de la source d'événement cible :

1. Sélectionnez l'onglet Requête et rapports. Le sous-onglet Requête s'affiche.
2. Développez Invites dans la Liste de requêtes, puis sélectionnez Connecteur.
3. Saisissez le nom du connecteur, puis cliquez sur OK.

Les événements collectés s'affichent. Les deux premiers événements sont des événements internes. Les événements suivants sont ceux collectés à partir de la table de trace MS SQL que vous avez configurée.

Remarque : Si les événements attendus ne s'affichent pas, cliquez sur Paramètres et filtres globaux dans la barre d'outils principale, paramétrez la Période sur Aucune limite, puis enregistrez le paramètre.

4. Sélectionnez Afficher les événements bruts et examinez la chaîne de résultat des deux premiers événements (facultatif). La chaîne de résultat apparaît dans l'événement brut. Les valeurs suivantes indiquent que le démarrage a abouti.
 - result_string=ODBCSource initiated successfully - MSSQL_TRACE
 - result_string=<nom du connecteur> Connector Started Successfully

Exemple : Activation de la collecte directe à l'aide du détecteur WinRMLinuxLogSensor

Vous pouvez activer la collecte directe d'événements générés par des applications Windows ou le système d'exploitation Windows Server 2008 à l'aide du détecteur WinRMLinuxLogSensor. Pour y parvenir, créez un connecteur sur l'agent par défaut basé sur une intégration qui utilise le détecteur WinRMLinuxLogSensor. De nombreuses intégrations utilisent ce détecteur, par exemple, Active_Directory_Certificate_Services, Forefront_Security_for_Exchange_Server, Hyper-V, MS_OCS et WinRM. L'application et le système d'exploitation Microsoft Windows qui génèrent des événements pouvant être récupérés via le détecteur WinRMLinuxLogSensor sont ceux pour lesquels la fonction Gestion à distance de Windows a été activée.

Vous trouverez ci-dessous une liste partielle des produits qui génèrent des événements pouvant être collectés directement par l'agent par défaut sur un serveur CA Enterprise Log Manager. Un connecteur unique est utilisé pour chaque produit ; chaque connecteur utilise le détecteur WinRMLinuxLogSensor.

- Services de certificat Microsoft Active Directory
- Microsoft Forefront Security pour Exchange Server
- Microsoft Forefront Security pour SharePoint Server
- Microsoft Hyper-V Server 2008
- Microsoft Office Communication Server
- Microsoft Windows Server 2008

Pour obtenir une liste complète, consultez la [Matrice d'intégration de produits](#) sur le support en ligne.

Cet exemple décrit l'activation de la collecte directe des événements à l'aide d'un connecteur fondé sur l'intégration WinRM. Quand un tel connecteur est déployé, il collecte des événements à partir d'une source d'événement du système d'exploitation Windows Server 2008. La collecte débute après la configuration des sources d'événement afin de consigner les événements dans la Visionneuse d'événements Windows et d'activer la fonction Gestion à distance de Windows sur le serveur, tel que spécifié dans le manuel du connecteur associé à cette intégration.

Pour configurer la source d'événements Windows Server 2008 :

1. Cliquez sur l'onglet Administration et le sous-onglet Bibliothèque.
2. Développez Bibliothèque d'ajustement d'événement, Intégrations, Abonnement, puis sélectionnez WinRM.

La fenêtre Afficher les détails des intégrations indique le nom du détecteur, à savoir WinRMLinuxLogSensor. Windows et Linux sont les deux plateformes prises en charge.

3. Cliquez sur le lien Aide de la fenêtre Afficher les détails de l'intégration WinRM.

Le manuel du connecteur pour Microsoft Windows Server 2008--WinRM s'affiche.

Pour configurer la source d'événement et vérifier la journalisation :

1. Connectez-vous à l'hôte cible muni d'un système d'exploitation Windows Server 2008.
2. Suivez les instructions figurant dans le *manuel du connecteur CA pour Microsoft Windows Server 2008* pour vous assurer de l'affichage des événements dans la Visionneuse d'événements Windows et de l'activation de la fonction Gestion à distance de Windows sur le serveur cible.

Remarque : Une partie de ce processus consiste à créer le nom d'utilisateur et le mot de passe que vous devez saisir lors de la configuration du connecteur. Ces informations de connexion permettent l'authentification requise pour établir une connectivité entre la source d'événement et CA Enterprise Log Manager.

3. Vérifiez la journalisation.
 - a. Ouvrez eventvwr dans la boîte de dialogue Exécuter.
La visionneuse d'événements apparaît.
 - b. Développez Journaux Windows et cliquez sur Sécurité.

Une fenêtre semblable à la suivante s'affiche et indique que la journalisation est en cours.



Pour activer la collecte directe d'événements à partir de sources d'événement Windows :

1. Sélectionnez l'onglet Administration, puis le sous-onglet Collecte de journaux.
2. Dans l'Explorateur de collecte de journaux, développez Explorateur d'agent, ainsi que le groupe d'agents contenant l'agent par défaut CA Enterprise Log Manager.
3. Sélectionnez un agent par défaut, c'est-à-dire, un agent portant le nom d'un serveur CA Enterprise Log Manager.

D'autres connecteurs peuvent être déployés sur l'agent par défaut.

4. Cliquez sur Créer un connecteur.



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

5. Sélectionnez une intégration qui utilise le détecteur de journaux WinRM dans la liste déroulante Intégration.

Par exemple, WinRM.



Cette sélection renseigne le champ Nom du connecteur par WinRM_Connecteur

6. Cliquez sur Appliquer les règles de suppression et sélectionnez les règles associées à des événements pris en charge (facultatif).
7. Cliquez sur l'étape Configuration du connecteur, puis cliquez sur le lien Aide.

Les instructions incluent la configuration des détecteurs CA Enterprise Log Manager--WinRM.

[5.0 Configuration des détecteurs CA Enterprise Log Manager - WinRM](#)

[5.1 Paramètre fixe](#)

8. Suivez les instructions du manuel du connecteur pour configurer le détecteur. Saisissez l'adresse IP, plutôt que le nom d'hôte, de l'hôte sur lequel vous avez configuré Gestion à distance de Windows. Le nom d'utilisateur et le mot de passe saisis correspondent aux informations de connexion ajoutées lors de la configuration de la Gestion à distance de Windows.

Voici un exemple.

Configuration du connecteur

Indiquez les informations de configuration.

Configurations enregistrées: Sélectionner la configuration

Configuration des détecteurs

- Nom de l'ordinateur: 172.24.36.107
- Port: 80
- Nom de l'utilisateur: ELMagent
- Mot de passe: *****
- Nom du journal d'événements: NT-Security
- Intervalle d'interrogation: 10
- Mise à jour du taux d'ancrage: 10
- Lecture à partir du début

Nom de la source: Security

Nom du canal (ou du journal): Security

9. Cliquez sur Enregistrer et fermer.
10. Le nouveau nom du connecteur s'affiche sous l'agent dans l'Explorateur d'agent.



11. Cliquez sur WinRM_Connector pour afficher les détails de l'état.

Au début, l'état indique Configuration en attente. Attendez jusqu'à ce que l'état affiche Exécution en cours.

Détails de l'état					
Redémarrer Démarrer Arrêter					
Connecteur	Agent	Groupe d'agents	Plate-forme	Intégration	Etat
WinRM_Connetto	ca-elm	Default Agent Group	Linux_X86_32	WinRM	Exécution en cours

12. Cliquez sur Exécution en cours pour obtenir des données, telles que les EPS (événements par seconde).

Etat: Pourcentage de l'UC: 0.0
Utilisation de la mémoire en Mo: 19.2
Moyenne d'événements par seconde: 0
Nombre d'événements filtrés: 0

Pour vérifier que l'agent par défaut collecte des événements à partir de la source d'événement cible :

1. Sélectionnez l'onglet Requêtes et rapports. Le sous-onglet Requêtes s'affiche.
2. Développez Invites dans la Liste de requêtes, puis sélectionnez Connecteur.
3. Saisissez le nom du connecteur, puis cliquez sur OK.
4. Visualisez les événements collectés.

Affichage et contrôle de l'état d'un agent ou d'un connecteur

Dans votre environnement, vous pouvez surveiller l'état d'agents ou de connecteurs, redémarrer les agents, ou encore démarrer, arrêter et redémarrer les connecteurs, le cas échéant.

Vous pouvez afficher les agents ou les connecteurs des différents niveaux de la hiérarchie de dossiers de l'Explorateur d'agent. Chaque niveau restreint l'affichage disponible en conséquence.

- Depuis le dossier Explorateur d'agent, vous pouvez afficher tous les agents ou connecteurs affectés au serveur CA Enterprise Log Manager actuel.
- Depuis le dossier d'un groupe d'agents spécifique, vous pouvez afficher les agents et connecteurs affectés à ce groupe d'agents.
- Depuis un agent spécifique, vous pouvez afficher cet agent uniquement et les connecteurs qui lui sont affectés.

Vous pouvez déterminer le mode FIPS ou non-FIPS d'un agent à partir de ces trois niveaux.

Pour afficher l'état d'un agent ou d'un connecteur

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Collecte de journaux.
La liste du dossier Collecte de journaux s'affiche.
2. Sélectionnez le dossier de l'Explorateur d'agent.
Les boutons de gestion des agents s'affichent dans le volet Détails.
3. Cliquez sur Etat et commande .
Le panneau d'état s'affiche.
4. Sélectionnez Agents ou Connecteurs.
Le panneau de recherche d'agents ou de connecteurs s'affiche.

5. Sélectionnez les critères de recherche de mise à jour d'agent ou de connecteur (facultatif). Si vous n'entrez aucun terme de recherche, toutes les mises à jour disponibles s'affichent. Vous pouvez sélectionner un ou plusieurs critères ci-dessous pour restreindre votre recherche.

- Groupe d'agents : renvoie uniquement les agents et les connecteurs affectés au groupe sélectionné.
- Plate-forme : renvoie uniquement les agents et les connecteurs s'exécutant sur le système d'exploitation sélectionné.
- Schéma de nom de l'agent : renvoie uniquement les agents et les connecteurs contenant le schéma spécifié.
- Intégration (connecteurs uniquement) : renvoie uniquement les connecteurs qui utilisent l'intégration sélectionnée.

6. Cliquez sur Afficher l'état.

Le graphique de détails qui s'affiche indique les agents ou les connecteurs correspondant à votre recherche. Par exemple :

Total : 10 Exécution en cours : 8 En attente : 1 Arrêté : 1 Aucune réponse : 0

7. Cliquez sur l'état pour afficher les détails dans le volet Etat, au bas du graphique (facultatif).

Remarque : Vous pouvez cliquer sur le bouton A la demande d'un agent ou d'un connecteur pour actualiser l'affichage de l'état.

8. Si vous affichez des connecteurs, sélectionnez l'un d'entre eux et cliquez sur Redémarrer, Démarrer ou Arrêter (facultatif). Si vous affichez des agents, sélectionnez n'importe quel agent et cliquez sur Redémarrer.

Chapitre 7 : Création de fédérations

Ce chapitre traite des sujets suivants :

[Requêtes et rapports dans un environnement fédéré](#) (page 231)

[Fédérations hiérarchiques](#) (page 232)

[Fédérations maillées](#) (page 234)

[Configuration d'une fédération CA Enterprise Log Manager](#) (page 235)

Requêtes et rapports dans un environnement fédéré

Un seul serveur CA Enterprise Log Manager renvoie les données de sa base de données interne d'événements pour répondre aux requêtes et renseigner les rapports. Si vous disposez d'une fédération de serveurs CA Enterprise Log Manager, vous pouvez contrôler la manière dont les requêtes et les rapports renvoient des informations d'événements en fonction de la configuration des relations de votre fédération. Vous pouvez également conserver les résultats des requêtes provenant des serveurs seuls en désactivant le paramètre global Utiliser les requêtes fédérées.

Le paramètre global Utiliser les requêtes fédérées est activé par défaut. Il permet d'envoyer les requêtes d'un serveur CA Enterprise Log Manager parent à tous les serveurs CA Enterprise Log Manager enfants. Chaque serveur CA Enterprise Log Manager enfant effectue des requêtes sur le magasin de journaux d'événements actif et sur le catalogue d'archive, ainsi que sur l'ensemble de ses serveurs CA Enterprise Log Manager enfants. Chaque serveur CA Enterprise Log Manager enfant crée ensuite un seul jeu de résultats à envoyer au serveur CA Enterprise Log Manager parent à l'origine de la requête. Pour permettre les configurations maillées, CA Enterprise Log Manager dispose d'une protection intégrée contre les requêtes circulaires.

Une implémentation classique de CA Enterprise Log Manager en entreprise comporte un à cinq serveurs. Une implémentation dans une grande entreprise peut comprendre dix serveurs et plus. La façon dont vous configurez votre fédération contrôle la quantité d'informations visibles par le serveur CA Enterprise Log Manager à l'origine de la requête. Le type de requête le plus simple provient du serveur CA Enterprise Log Manager principal et renvoie des informations provenant de tous les serveurs enfants configurés en dessous de celui-ci.

Lorsque vous effectuez une requête sur la fédération à partir d'un serveur enfant, les résultats affichés dépendent de la configuration de votre fédération. Dans une fédération *hiérarchique*, tous les serveurs configurés comme les enfants d'un serveur renvoient les résultats des requêtes à ce serveur. Dans une fédération *maillée*, tous les serveurs interconnectés renvoient les données au serveur à l'origine de la requête.

Fédérations hiérarchiques

Les *fédérations hiérarchiques* utilisent une structure pyramidale descendante pour diffuser largement les charges de collecte d'événements. Cette structure est similaire à un organigramme. Il n'existe aucun nombre défini de niveaux à créer, vous pouvez créer les niveaux qui correspondent le mieux à vos besoins professionnels.

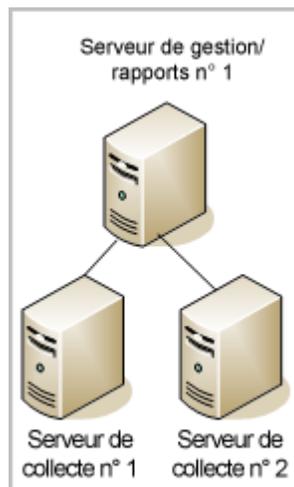
Dans une fédération hiérarchique, vous pouvez vous connecter à n'importe quel serveur CA Enterprise Log Manager pour afficher des rapports sur ses données d'événements et sur les données provenant de ses serveurs enfants. La portée des données auxquelles vous pouvez accéder est limitée en fonction de votre position de départ dans la hiérarchie. Si vous commencez au milieu de la hiérarchie, vous pouvez seulement consulter les données de ce serveur, ainsi que celles de tous ses serveurs enfants. Plus vous montez dans une fédération hiérarchique, plus la portée des données réseau est importante. Au plus haut niveau, vous avez accès aux données de l'ensemble du déploiement.

Les fédérations hiérarchiques sont utiles pour les déploiements régionaux, par exemple. Supposons que vous souhaitiez que les ressources locales puissent accéder aux données d'événement au sein d'une certaine hiérarchie (ou branche) du réseau, mais pas aux données d'événement dans d'autres branches parallèles. Vous pouvez créer une fédération hiérarchique avec plusieurs branches parallèles pour contenir les données de chaque région. Chaque branche peut transmettre des rapports à un serveur CA Enterprise Log Manager de gestion situé dans les bureaux du siège, pour afficher tous les rapports de journaux d'événements de manière descendante.

Exemple de fédération hiérarchique

Dans la carte de fédération illustrée par le diagramme ci-après, le réseau utilise le serveur CA Enterprise Log Manager de gestion comme serveur de rapports et plusieurs serveurs de collecte dans une configuration similaire à un organigramme. Le serveur de gestion/rapports agit comme un serveur CA Enterprise Log Manager parent et dispose de fonctions d'authentification, d'autorisation et de gestion majeure des utilisateurs, ainsi que de fonctions de génération de rapports liées à la gestion des requêtes, rapports et alertes. Dans cet exemple, les serveurs de collecte sont les enfants du serveur de gestion/rapports n° 1. Vous pouvez organiser d'autres niveaux dans la hiérarchie. Toutefois, il ne peut y avoir plusieurs serveurs de gestion. Les niveaux supplémentaires sont composés de serveurs de rapports à l'état de parents des serveurs de collecte.

Pour illustrer ce style de fédération, le serveur de gestion/rapports n° 1 pourrait être situé dans vos bureaux du siège et les serveurs de collecte pourraient se trouver dans des bureaux régionaux ou de branches, représentés par les serveurs de collecte n° 1 et 2. Chaque branche pourrait obtenir des informations sur ses propres données, mais pas les données de l'autre branche. A partir du serveur de collecte n° 1, vous pouvez par exemple effectuer une requête et générer des rapports sur les données de ce serveur uniquement. Par contre, à partir du serveur de gestion/rapports n° 1, vous pouvez effectuer des requêtes et générer des rapports sur les données provenant de ce serveur, mais également des serveurs de collecte n° 1 et 2.



Dans une fédération hiérarchique, chaque serveur CA Enterprise Log Manager peut avoir un ou plusieurs enfants, mais un seul parent. Vous configurez ce type de fédération selon une approche descendante, en commençant par le serveur de gestion. Vous accédez ensuite à chaque couche inférieure pour configurer les serveurs enfants de rapports et de collecte. L'aspect essentiel de la configuration d'une fédération consiste à réaliser au préalable une carte des serveurs et des relations souhaitées. Ensuite, vous pouvez configurer un serveur CA Enterprise Log Manager comme serveur enfant, afin d'implémenter les relations entre eux.

Fédérations maillées

Une *fédération maillée* est similaire à une fédération hiérarchique car elle peut afficher des niveaux. La principale différence repose sur la configuration des connexions entre les serveurs. Une fédération maillée peut permettre à n'importe quel serveur CA Enterprise Log Manager sur le réseau d'effectuer des requêtes et de générer des rapports sur les données de tous les autres serveurs CA Enterprise Log Manager. Les capacités de génération de rapport dépendent des relations créées entre les serveurs.

Par exemple, dans une fédération maillée, les serveurs peuvent être interconnectés uniquement au sein d'une branche verticale. Cela signifie que tous les serveurs CA Enterprise Log Manager de cette branche peuvent avoir accès à tous les autres serveurs CA Enterprise Log Manager de la même branche. Cette situation est en opposition directe avec celle d'un serveur CA Enterprise Log Manager d'une fédération hiérarchique, qui peut produire des rapports uniquement sur les serveurs hiérarchiquement inférieurs.

Dans une formation en anneau ou en étoile, chaque serveur CA Enterprise Log Manager est configuré pour être l'enfant de tous les autres serveurs. Lorsque vous demandez des données de rapports à partir d'un serveur CA Enterprise Log Manager, vous affichez les données de tous les serveurs CA Enterprise Log Manager du réseau.

La fédération maillée affecte plusieurs serveurs CA Enterprise Log Manager comme serveurs principaux et elle utilise les serveurs en fédération sans tenir compte de leur position sur le réseau. Les serveurs configurés *comme* enfants sont également configurés pour afficher les enfants de la même branche ou d'autres branches fédérées à ces serveurs. Par exemple, si vous disposez de deux serveurs CA Enterprise Log Manager, A et B, vous pouvez créer une fédération maillée en désignant B comme l'enfant de A *et* A comme l'enfant de B. Il s'agit de la configuration attendue lorsque vous utilisez plusieurs serveurs de gestion.

Exemple de fédération maillée

Etudiez l'illustration suivante d'une fédération totalement maillée.

Dans la fédération maillée illustrée dans ce diagramme, quatre serveurs de collecte sont fédérés les uns aux autres ainsi qu'aux deux serveurs de rapports. Chaque serveur est à la fois un parent et un enfant pour chaque autre serveur de la fédération.

Ce déploiement présente un avantage potentiel par rapport à la fédération hiérarchique stricte : vous pouvez accéder aux données depuis n'importe quel point du maillage et obtenir des résultats depuis tous les autres serveurs CA Enterprise Log Manager de ce maillage, sans tenir compte d'une hiérarchie.

Vous pouvez associer les fédérations maillées et hiérarchiques pour atteindre la configuration qui répond à vos besoins. Par exemple, une configuration maillée au sein d'une seule branche peut s'avérer très utile pour les déploiements globaux. Vous pouvez obtenir une présentation globale des données à partir des serveurs parents de rapports, tout en conservant des clusters régionaux (branches) ayant accès à leurs propres données uniquement.

Configuration d'une fédération CA Enterprise Log Manager

Chaque serveur CA Enterprise Log Manager ajouté à une fédération doit faire référence au même nom d'instance d'application sur le serveur de gestion. Ainsi, le serveur de gestion peut stocker et gérer l'ensemble des configurations, comme des configurations globales.

Vous pouvez configurer la fédération à tout moment, mais il vaut mieux le faire avant de commencer à planifier des rapports si vous souhaitez des rapports consolidés.

La configuration d'une fédération implique les activités répertoriées ci-dessous.

1. Créez une carte de fédération.
2. Installez le premier serveur CA Enterprise Log Manager, à savoir le serveur de gestion.

3. Installez un ou plusieurs serveurs supplémentaires.
4. Configurez les relations parents/enfants. Par exemple, commencez par sélectionner les enfants de fédération de serveurs du serveur de gestion à partir des paramètres des magasins de journaux d'événements pour ce serveur.

Ce premier groupe de serveurs enfants forme la deuxième couche, ou niveau, de la fédération si vous configurez une fédération hiérarchique.

5. Affichez le graphique de fédération pour vérifier que la structure entre les serveurs pour les niveaux parents et enfants est configurée selon vos souhaits.

Configuration d'un serveur CA Enterprise Log Manager en tant que serveur enfant

La configuration d'un serveur CA Enterprise Log Manager en tant qu'enfant d'un autre serveur constitue l'étape essentielle de la création d'une fédération. Utilisez la procédure suivante pour ajouter des serveurs à votre fédération à tout moment. Vous devez installer tous les serveurs CA Enterprise Log Manager que vous souhaitez fédérer sous le même nom d'instance d'application enregistré avant d'effectuer cette partie de la configuration. Lorsque vous installez chaque nouveau serveur, son nom s'affiche dans la liste des serveurs disponibles pour la fédération. Vous pouvez effectuer cette procédure autant de fois que nécessaire pour créer la structure fédérée souhaitée.

Pour configurer un serveur CA Enterprise Log Manager en tant que serveur enfant

1. Connectez-vous à n'importe quel serveur CA Enterprise Log Manager enregistré sous le même nom d'instance d'application que les autres dans la fédération que vous envisagez.
2. Cliquez sur l'onglet Administration et sélectionnez le sous-onglet Services.
3. Développez le dossier du service Magasin de journaux d'événements, puis sélectionnez le nom de serveur pour le serveur CA Enterprise Log Manager parent.
4. Faites défiler vers le bas jusqu'à la liste Enfants de fédération de serveurs.
5. Sélectionnez un ou plusieurs noms de serveur à configurer comme enfants du serveur parent dans la liste Disponible(s).
6. Utilisez les boutons fléchés pour déplacer vos sélections vers la liste Serveurs sélectionnés.

Les serveurs CA Enterprise Log Manager sélectionnés et déplacés dans la liste sont désormais des enfants fédérés du serveur parent.

Informations complémentaires :

[Sélection de l'utilisation des requêtes fédérées](#) (page 156)

Affichage du graphique de fédération et du contrôleur de l'état du serveur

Vous pouvez afficher un graphique représentant les serveurs CA Enterprise Log Manager de votre environnement, leurs relations de fédération et leur état. Le graphique de fédération vous permet d'afficher la structure de fédération actuelle et de visualiser l'état de chaque serveur. Vous pouvez également sélectionner le serveur local interrogé au cours de cette session en le définissant comme serveur parent.

Pour afficher le graphique de fédération, cliquez sur Afficher le graphique de fédération et le contrôleur de l'état, en haut de l'écran : 

La fenêtre qui s'affiche montre un graphique de tous les hôtes de magasins d'événements enregistrés auprès du serveur de gestion actuel.

- Les magasins d'événements avec des enfants de fédération de serveurs s'affichent en bleu clair, avec des lignes de connexion noires matérialisant la relation de fédération.
- Les magasins d'événements sans enfant de fédération de serveurs s'affichent en vert clair.

Vous avez la possibilité de sélectionner un serveur local à des fins de requête.

Vous pouvez également visualiser l'état de tous les serveurs affichés. Cliquez sur un serveur du graphique de fédération pour afficher diverses informations d'état.

- Pourcentage d'utilisation de l'UC
- Pourcentage d'utilisation de la mémoire disponible
- Pourcentage d'utilisation de l'espace disque disponible
- Événements reçus par seconde
- Graphique principal de l'état du magasin de journaux d'événements

Informations complémentaires :

[Exemple : Carte de fédération pour une PME](#) (page 39)

[Exemple : Carte de fédération pour une grande entreprise](#) (page 37)

Chapitre 8 : Utilisation de la bibliothèque d'ajustement d'événement

Ce chapitre traite des sujets suivants :

- [A propos de la bibliothèque d'ajustement d'événement](#) (page 239)
- [Prise en charge de nouvelles sources d'événement avec la bibliothèque d'ajustement d'événement](#) (page 240)
- [Fichiers de mappage et d'analyse](#) (page 240)

A propos de la bibliothèque d'ajustement d'événement

La bibliothèque d'ajustement d'événement fournit les outils permettant de créer de nouveaux fichiers d'analyse et de mappage, ou encore de modifier des copies de fichiers pour prendre en charge de nouvelles unités, applications, etc. La bibliothèque comprend les options ci-dessous.

- Intégrations
- Ecouteurs
- Fichiers de mappage et d'analyse
- Règles de suppression et de récapitulation

Les règles de suppression empêchent la collecte des données ou l'insertion des données dans le magasin de journaux d'événements. Les règles de récapitulation vous permettent de cumuler des événements afin de réduire le nombre d'insertions de types d'événements ou d'actions similaires. Il s'agit de la partie de la bibliothèque la plus fréquemment utilisée, car les règles de suppression et de récapitulation peuvent permettre de régler les performances du réseau et de la base de données.

Vous pouvez utiliser la zone des intégrations pour afficher les intégrations prédéfinies et créer de nouvelles intégrations pour vos unités, applications, bases de données ou fichiers personnalisés ou propriétaires. Vous trouverez plus d'informations dans le *Manuel d'administration CA Enterprise Log Manager* et dans l'aide en ligne.

Prise en charge de nouvelles sources d'événement avec la bibliothèque d'ajustement d'événement

Pour prendre en charge un périphérique, une application, une base de données ou toute autre source d'événement qui n'est pas encore prise en charge, utilisez les Assistants de fichier de mappage et d'analyse ainsi que l'Assistant d'intégration pour créer les composants nécessaires.

Ce processus comprend les grandes étapes suivantes.

1. Création de fichiers d'analyse pour collecter les données d'événement sous forme de paires nom-valeur
2. Création de fichiers de mappage pour mapper les paires nom-valeur vers la grammaire commune aux événements
3. Création de nouvelles intégrations et de nouveaux écouteurs pour collecter les données de votre source d'événement

Les intégrations, les fichiers d'analyse et de mappage ainsi que les règles de suppression et de récapitulation sont évoqués plus précisément dans le *Manuel d'administration CA Enterprise Log Manager* et dans l'aide en ligne.

Fichiers de mappage et d'analyse

Lors du fonctionnement, CA Enterprise Log Manager lit les événements entrants et les répartit en sections au cours d'une action appelée *analyse*. Il s'agit de fichiers d'analyse de message distincts pour différents systèmes d'exploitation, unités, applications et bases de données. Une fois les événements entrants analysés par paires nom-valeur, les données traversent un module de *mappage* qui place les données d'événement dans les champs de la base de données.

Le module de mappage utilise des fichiers de mappage de données créés pour des sources d'événement spécifiques, similaires aux fichiers d'analyse de message. Le schéma de base de données est la grammaire commune aux événements, l'une des fonctions centrales de CA Enterprise Log Manager.

Réunis, l'analyse et le mappage constituent le moyen de normaliser les données et de les stocker dans une base de données commune, quel que soit le type d'événement ou le format de message.

L'Assistant d'intégration et certains modules d'adaptateurs CA impliquent que vous configuriez les fichiers de mappage et d'analyse qui décrivent le mieux les genres de données d'événement écoutées par un connecteur ou un adaptateur. Dans les panneaux de configuration où apparaissent ces contrôles, l'ordre des fichiers d'analyse de message doit refléter le nombre relatif d'événements reçus du même type. L'ordre des fichiers de mappage des données doit également refléter la quantité d'événements reçus en provenance d'une source donnée.

Par exemple, si le module de l'écouteur Syslog pour un serveur CA Enterprise Log Manager spécifique reçoit principalement des événements du pare-feu Cisco PIX, vous devez placer les fichiers CiscoPIXFW.XMPS et CiscoPIXFW.DMS en premier dans leurs listes respectives.

Annexe A : Remarques pour les utilisateurs de CA Audit

Ce chapitre traite des sujets suivants :

[Présentation des différences entre les architectures](#) (page 243)

[Configuration d'adaptateurs CA](#) (page 251)

[Envoi d'événements CA Audit à CA Enterprise Log Manager](#) (page 256)

[Quand importer des événements](#) (page 261)

[Importation des données d'une table SEOSDATA](#) (page 263)

Présentation des différences entre les architectures

Lorsque vous planifiez l'utilisation conjointe de CA Audit et de CA Enterprise Log Manager, vous devez au préalable comprendre les différences entre les architectures et leurs effets sur la structure de votre réseau.

CA Enterprise Log Manager utilise un magasin de journaux d'événements intégré et dispose d'un Explorateur d'agent pour configurer et gérer les agents. La nouvelle technologie, associée à une grammaire commune aux événements, permet un débit d'événements plus rapide vers le stockage, tout en prenant en charge un plus grand nombre de sources d'événement. Grâce à la grammaire commune aux événements, CA Enterprise Log Manager peut normaliser les événements provenant de nombreuses sources d'événement différentes pour obtenir un seul schéma de base de données.

CA Enterprise Log Manager s'intègre à CA Audit jusqu'à un certain niveau mais, du fait de sa conception, n'est pas complètement intéropérable. CA Enterprise Log Manager est une infrastructure de serveur nouvelle et distincte, qui peut fonctionner en parallèle de CA Audit, en tenant compte des phénomènes ci-dessous en matière de gestion d'événements.

CA Enterprise Log Manager peut...

Recevoir des journaux d'événements envoyés par des clients CA Audit et des iRecorders utilisant des écouteurs configurables.

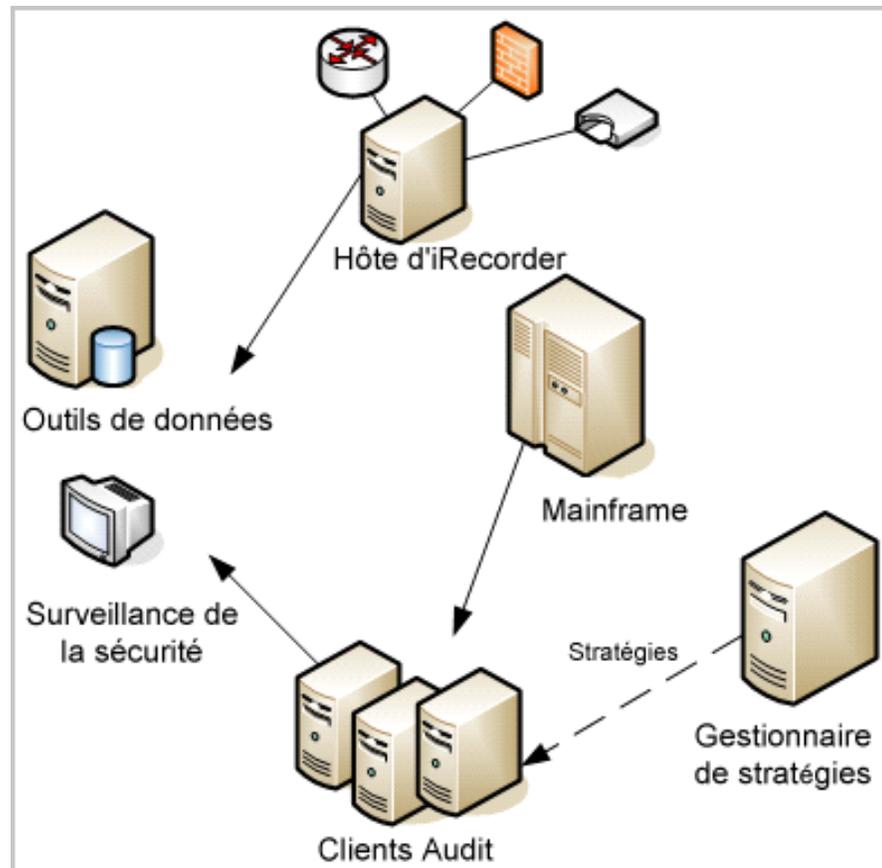
CA Enterprise Log Manager ne peut pas...

Accéder directement aux journaux d'événements stockés dans la base de données du collecteur CA Audit.

CA Enterprise Log Manager peut...	CA Enterprise Log Manager ne peut <i>pas</i>...
Proposer un utilitaire pour importer les données des journaux d'événements stockées dans la base de données du collecteur CA Audit (table SEOSDATA).	
Utiliser des agents pour envoyer des journaux d'événements à la seule infrastructure du serveur CA Enterprise Log Manager.	
Autoriser les agents CA Enterprise Log Manager et les clients CA Audit dotés d'iRecorders à fonctionner sur le même hôte physique.	Autoriser les agents CA Enterprise Log Manager et les clients CA Audit dotés d'iRecorders sur le même hôte à accéder simultanément aux mêmes sources de journaux.
Utiliser son Explorateur d'agent intégré pour gérer uniquement des agents CA Enterprise Log Manager. Lors du fonctionnement côte à côte des deux systèmes, CA Audit utilise son gestionnaire de stratégies uniquement pour gérer les clients CA Audit.	
	Migrer les données CA Audit contenues dans les collecteurs de tables, les modèles de rapports ou les rapports personnalisés, les stratégies d'alerte, les stratégies de collecte/filtrage ou encore les stratégies de contrôle d'accès basées sur des rôles.

Architecture CA Audit

L'illustration qui suit montre une implémentation CA Audit simplifiée.



Dans certains déploiements de CA Audit en entreprise, les données d'événement sont stockées par le service du collecteur dans une base de données relationnelle qui s'exécute sur le serveur d'outils de données. Un administrateur de base de données surveille et entretient cette base de données, il travaille également avec un administrateur système pour mettre en place les stratégies adéquates afin de collecter les événements souhaités et d'exclure les événements inutiles.

Sur ce diagramme, les lignes pleines représentent les événements transmis par les clients CA Audit, l'enregistreur et les hôtes iRecorder au serveur d'outils de données ou, dans certains cas, à une console facultative de surveillance de la sécurité. Une ligne pointillée représente le flux de contrôle entre le serveur du gestionnaire de stratégies et les clients utilisant des stratégies.

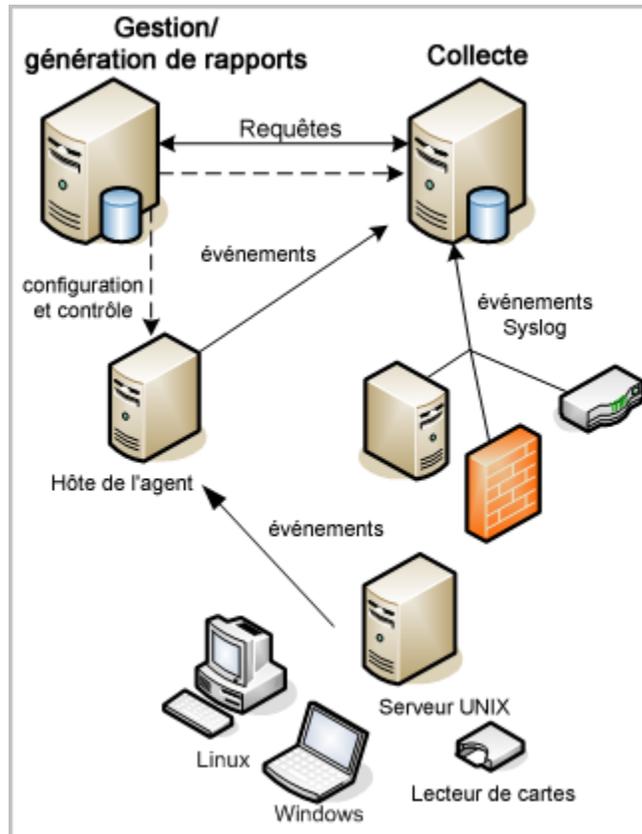
Le serveur d'outils de données dispose d'utilitaires de base pour la génération de rapports, la visualisation et le stockage d'événements. La création et la conservation des requêtes et rapports personnalisés, qui constituent la norme des implémentations d'entreprise, sont des opérations qui prennent du temps.

Cette topologie de réseau permet la collecte de divers types d'événements provenant de différentes unités, applications et bases de données. Vous disposez du stockage central des événements collectés, qui fait généralement partie (ou est géré par) le serveur d'outils de données, qui produit également certains rapports.

Toutefois, vous devez disposer de capacités supplémentaires pour échelonner votre solution afin de gérer rapidement les volumes croissants d'événements. Vous devez générer des rapports attestant de la conformité avec diverses réglementations fédérales et internationales. Vous devez également pouvoir retrouver rapidement et facilement ces rapports.

Architecture CA Enterprise Log Manager

L'illustration ci-dessous représente une implémentation CA Enterprise Log Manager de base, comprenant deux serveurs.



Un système CA Enterprise Log Manager peut comprendre un ou plusieurs serveurs et le premier serveur installé est le serveur de gestion. Un système ne peut comprendre qu'un seul serveur de gestion, mais vous pouvez avoir plusieurs systèmes. Le serveur de gestion conserve le contenu et la configuration de tous les serveurs CA Enterprise Log Manager et il effectue l'autorisation et l'authentification des utilisateurs.

Dans une implémentation de base comprenant deux serveurs, le serveur de gestion assume également le rôle de serveur de rapports. Un serveur de rapports reçoit les événements ajustés d'un ou plusieurs serveurs de collecte. Le serveur de rapports gère les requêtes et rapports à la demande, ainsi que les alertes et rapports planifiés. Le serveur de collecte ajuste les événements collectés.

Chaque serveur CA Enterprise Log Manager dispose de sa propre base de données interne de magasin de journaux d'événements. Le magasin de journaux d'événements est une base de données propriétaire qui utilise la compression pour améliorer la capacité de stockage et pour autoriser les requêtes sur les fichiers des bases de données actives, les fichiers marqués pour archivage et les fichiers dégivrés. Aucun package SGBD relationnel n'est nécessaire pour le stockage d'événements.

Le serveur CA Enterprise Log Manager de collecte peut recevoir directement les événements à l'aide de son agent par défaut ou à partir d'un agent se trouvant sur la source d'événement. Les agents peuvent également se trouver sur un hôte qui agit en tant que collecteur pour d'autres sources d'événement sur le réseau, comme un concentrateur VPN ou un hôte de routeur.

Sur ce diagramme, les lignes pleines représentent les flux d'événements depuis les sources d'événement vers les agents, puis vers le serveur de collecte et enfin vers le rôle de rapports du serveur de gestion/rapports. Les lignes pointillées représentent le trafic de configuration et de contrôle entre les serveurs CA Enterprise Log Manager, ainsi qu'entre le rôle de gestion du serveur de gestion/rapports et les agents. Sur le réseau, vous pouvez utiliser un serveur CA Enterprise Log Manager pour contrôler n'importe quel agent, si, lors de l'installation, les serveurs CA Enterprise Log Manager ont bien été enregistrés auprès du serveur de gestion avec le même nom d'instance d'application.

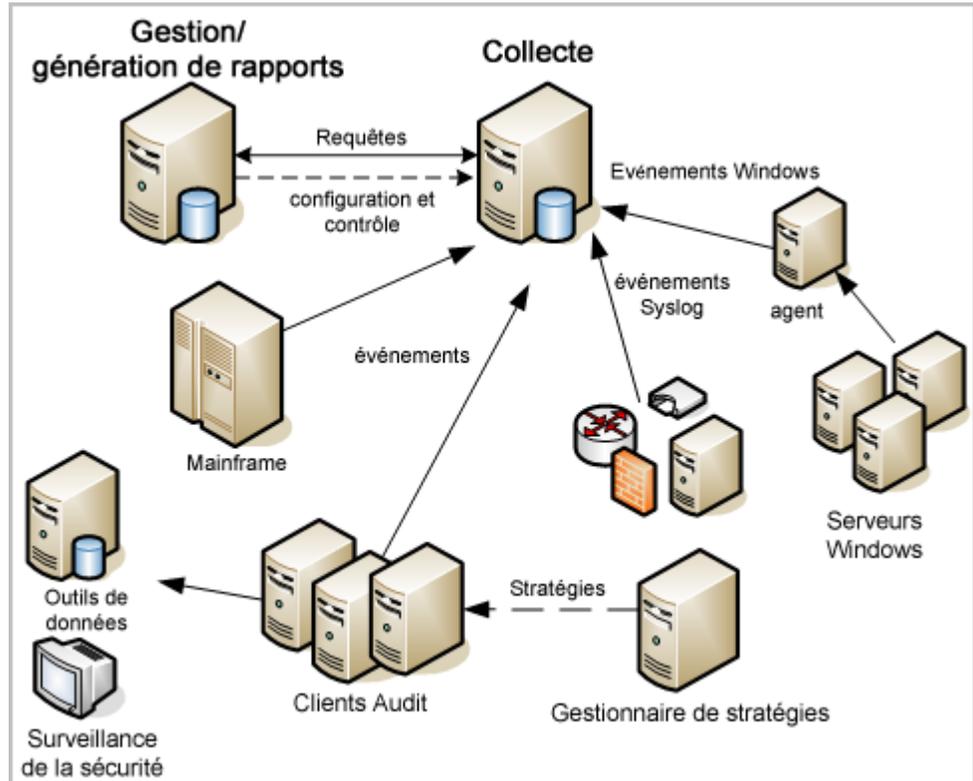
Les agents utilisent des connecteurs (non illustrés) pour collecter les événements. Un seul agent peut gérer plusieurs connecteurs pour collecter simultanément de nombreux types d'événements différents. Cela signifie qu'un seul agent, déployé sur une source individuelle d'événement, peut collecter différents types d'informations. Le serveur CA Enterprise Log Manager dispose également d'écouteurs, qui permettent de collecter les événements provenant d'autres applications CA grâce à des iRecorder et SAPI Recorders sur votre réseau CA Audit.

Vous pouvez fédérer les serveurs CA Enterprise Log Manager pour échelonner votre solution et partager les données de rapports, sans qu'elles soient transportées hors limites. Vous disposez ainsi d'une vue réseau de la conformité, tout en respectant toujours les réglementations concernant la conservation des emplacements physiques des données.

Les mises à jour d'abonnement pour les requêtes et rapports prédéfinis signifient que vous n'avez plus besoin de conserver manuellement les requêtes et les rapports. Les assistants fournis vous permettent de créer vos propres intégrations personnalisées pour les unités et applications tierces qui ne sont pas encore prises en charge.

Architecture intégrée

Le diagramme qui suit illustre un réseau CA Audit classique avec l'ajout de CA Enterprise Log Manager pour bénéficier de ses capacités de gestion de volumes élevés d'événements et de génération de rapports basée sur la conformité.



CA Enterprise Log Manager utilise un Explorateur d'agent intégré, un magasin de journaux d'événements intégré et une seule interface utilisateur pour centraliser et simplifier la collecte de journaux. La technologie d'agent CA Enterprise Log Manager, associée à la grammaire commune aux événements, permet un débit d'événements plus rapide vers le stockage, tout en gérant un plus grand nombre de sources d'événement. Un seul agent peut gérer plusieurs connecteurs reliés aux sources d'événement, ce qui simplifie les tâches de gestion de l'agent et permet de bénéficier des intégrations prédéfinies pour les sources courantes ou communes de journaux d'événements.

Dans cette implémentation, le serveur de collecte CA Enterprise Log Manager reçoit directement les événements Syslog, iTechnology et SAPI Recorder. Le serveur de collecte reçoit des événements provenant de sources d'événement Windows par le biais d'un agent CA Enterprise Log Manager distinct pour Windows. Plusieurs agents peuvent être déployés sur votre réseau et chacun d'entre eux peut collecter de nombreux types différents de données d'événement via leurs connecteurs. Cela permet de réduire le trafic d'événements vers la base de données SEOSDATA et de profiter des requêtes et rapports disponibles dans CA Enterprise Log Manager. Une simple modification de la règle de stratégie permet aux clients CA Audit d'envoyer les événements collectés au serveur d'outils de données et au serveur CA Enterprise Log Manager.

Outre un débit plus élevé, CA Enterprise Log Manager propose des requêtes et rapports prêts à l'emploi, qui vous permettent de prouver votre conformité à l'égard de nombreuses normes, telles que PCI (DSS) et SOX. En associant les requêtes et rapports prédéfinis à votre implémentation CA Audit et CA Security Command Center existante, vous pouvez tirer profit des investissements dans vos solutions personnalisées tout en bénéficiant des rapports et du débit plus élevé de CA Enterprise Log Manager.

Configuration d'adaptateurs CA

Les adaptateurs CA constituent un groupe d'écouteurs recevant des événements de composants hérités comme les clients CA Audit, les iRecorders et les SAPI recorders, ainsi que de sources d'événement qui transmettent les événements de manière native par le biais d'iTechnology.

Paramétrez les options de configuration des adaptateurs CA avant de modifier les configurations des stratégies CA Audit ou des iRecorders. Vous vous assurez ainsi du bon fonctionnement des processus d'écouteurs avant l'arrivée des événements et évitez les données d'événement ayant un mappage incorrect.

Si vous envoyez des événements à CA Audit via iRecorder ou si vous utilisez un client CA Audit avec iRecorder, vous utilisez des adaptateurs SAPI CA Enterprise Log Manager pour recevoir les événements. Pour envoyer des événements à CA Enterprise Log Manager, vous modifiez une stratégie CA Audit existante pour les événements CA Access Control. Vous pouvez ajouter une action Collecteur ou Acheminement à une règle existante.

- Si vous créez une action Collecteur pour une règle d'une stratégie CA Audit existante, configurez l'adaptateur CA du collecteur SAPI pour recevoir les événements.
- Si vous créez une action Acheminement pour une règle d'une stratégie CA Audit existante, configurez l'adaptateur CA du routeur SAPI pour recevoir les événements.

Pour obtenir les instructions de reconfiguration pour l'envoi direct d'événements à CA Enterprise Log Manager, consultez la documentation des sources SAPI.

Si vous envisagez d'installer un iRecorder autonome ou d'utiliser un iRecorder existant, configurez le module d'extension d'événements iTech pour recevoir les événements. Vous pouvez par exemple utiliser cette approche si CA Audit n'est pas installé, mais que vous souhaitez vous servir d'un iRecorder CA pour collecter les événements provenant d'une source d'événement prise en charge. Ce processus inclut les étapes ci-dessous.

- Configuration du module d'extension d'événements iTechnology
- Configuration du produit iRecorder ou iTechnology pour envoyer les événements directement au serveur CA Enterprise Log Manager

A propos du routeur et du collecteur SAPI

Les services SAPI sont généralement utilisés pour recevoir des événements provenant de clients CA Audit et produits intégrés. CA Enterprise Log Manager utilise deux instances d'un service d'écouteur SAPI, l'une installée en tant que collecteur SAPI, l'autre en tant que routeur SAPI.

Les modules SAPI utilisent le démon iGateway pour les commandes et les contrôles. Les modules agissent comme un routeur SAPI et un collecteur SAPI ; ils utilisent des ports statiques ou dynamiques par le biais du mappeur de ports.

Utilisez le collecteur SAPI lors de l'envoi d'événements provenant de clients CA Audit, de telle sorte que vous puissiez utiliser la prise en charge intégrée du basculement dans l'action du collecteur d'Audit.

Utilisez le routeur SAPI lors de l'envoi d'événements provenant de clients CA Audit à l'aide de l'action de routage ou lors de l'envoi d'événements provenant de SAPI Recorders ou d'intégrations qui prennent en charge l'envoi d'événements directement à un client CA Audit. Dans ce cas, vous pouvez configurer l'expéditeur distant comme si le serveur CA Enterprise Log Manager était le client CA Audit.

L'écouteur SAPI ouvre son propre port et écoute passivement les nouveaux événements qui lui sont envoyés. Chaque instance du module SAPI dispose de sa propre configuration, qui spécifie les éléments ci-dessous.

- Port sur lequel écouter
- Fichiers de mappage de données à charger
- Bibliothèques de chiffrement à utiliser

Après réception de l'événement, le module le soumet à la bibliothèque de mappage, puis CA Enterprise Log Manager l'insère dans la base de données.

Important : La bibliothèque de mappage de données peut contenir un ou plusieurs fichiers de mappage portant le même nom, mais des numéros de version différents. Les différents fichiers prennent en charge différents niveaux de version de la même source d'événement, comme un système d'exploitation, une base de données, etc. Vous devez sélectionner un seul fichier de mappage correspondant à la version lorsque vous configurez le collecteur ou le routeur SAPI.

Si deux fichiers portant le même nom sont présents dans la liste des fichiers de mappage sélectionnés, le moteur de mappage utilise uniquement le premier fichier de la liste. Si ce n'est pas le fichier adapté au flux d'événements entrants, le moteur de mappage ne peut pas mapper correctement les événements. De ce fait, les requêtes et rapports risquent d'afficher des informations n'incluant pas les événements mal mappés ou même dépourvus d'événements.

Configuration du service de collecteur SAPI

Utilisez la procédure suivante pour configurer le service de collecteur SAPI.

Vous pouvez modifier les stratégies CA Audit utilisant des actions du collecteur pour envoyer des événements à un serveur CA Enterprise Log Manager en plus ou à la place de l'envoi d'événements à la base de données du collecteur CA Audit. Configurez ce service avant de modifier les stratégies d'audit, pour vous assurer de ne perdre aucun événement.

Pour configurer le service de collecteur SAPI

1. Connectez-vous au serveur CA Enterprise Log Manager et sélectionnez l'onglet Administration.
Le sous-onglet Collecte de journaux s'affiche par défaut.
2. Développez l'entrée Adaptateurs CA.
3. Sélectionnez le service Collecteur SAPI.
4. Pour obtenir des descriptions de chaque champ, reportez-vous à l'aide en ligne.
5. Cliquez sur Enregistrer lorsque vous avez terminé.

Configuration du service de routeur SAPI

Utilisez la procédure suivante pour configurer un service de routeur SAPI.

Vous pouvez modifier les stratégies CA Audit utilisant des actions du routeur pour envoyer des événements à un serveur CA Enterprise Log Manager en plus ou à la place de l'acheminement d'événements vers d'autres destinations. Vous pouvez également rediriger les événements SAPI Recorder pour les transmettre directement à l'écouteur du routeur SAPI en modifiant leurs fichiers de configuration. Configurez ce service avant de modifier les stratégies d'audit ou les configurations SAPI Recorder, pour vous assurer de ne perdre aucun événement.

Pour configurer le service de routeur SAPI

1. Connectez-vous au serveur CA Enterprise Log Manager et sélectionnez l'onglet Administration.
Le sous-onglet Collecte de journaux s'affiche par défaut.
2. Développez l'entrée Adaptateurs CA.

3. Sélectionnez le service Routeur SAPI.
4. Pour obtenir des descriptions de chaque champ, reportez-vous à l'aide en ligne.
5. Cliquez sur Enregistrer lorsque vous avez terminé.

A propos du module d'extension d'événements iTechnology

Le module d'extension d'événements iTechnology reçoit les événements envoyés par le mécanisme de gestion des événements iGateway. Configurez le module d'extension d'événements iTechnology si l'une des conditions ci-dessous se vérifie dans votre environnement.

- Vous disposez d'iRecorders existants sur votre réseau et dépourvus de client CA Audit sur le même système.
- Vous avez d'autres produits, comme CA EEM, qui peuvent transférer des événements via iTechnology.

Après réception d'un événement, ce service le soumet à la bibliothèque de mappage grâce à laquelle CA Enterprise Log Manager insère l'événement mappé dans le magasin de journaux d'événements.

Configuration du module d'extension d'événements iTechnology

Utilisez la procédure suivante pour configurer le module d'extension d'événements iTechnology pour qu'il puisse recevoir des informations provenant d'iRecorders et d'autres sources d'événement iTechnology.

Utilisez le module d'extension iTechnology lorsque vous configurez un iRecorder autonome pour qu'il envoie ses événements à un serveur CA Enterprise Log Manager. Configurez ce service *avant* de configurer ou d'installer un iRecorder, pour vous assurer de ne perdre aucun événement.

Remarque : Si vous voulez envoyer des événements à partir d'un client externe vers l'écouteur du module d'extension d'événements iTechnology, envoyez ces événements uniquement au serveur CA Enterprise Log Manager secondaire.

Pour configurer le module d'extension d'événements iTechnology :

1. Connectez-vous au serveur CA Enterprise Log Manager et sélectionnez l'onglet Administration.
Le sous-onglet Collecte de journaux s'affiche par défaut.
2. Développez l'entrée Adaptateurs CA.

3. Sélectionnez le service Module d'extension d'événements iTechnology.
4. Sélectionnez un ou plusieurs fichiers de mappage de données dans la liste Fichiers de mappage de données disponibles, puis utilisez les flèches pour les déplacer vers la liste Sélectionner les fichiers de mappage de données.

Le service du module d'extension d'événements est préconfiguré pour inclure la plupart des principaux fichiers de mappage de données.

5. Cliquez sur Enregistrer pour stocker les modifications apportées aux fichiers de configuration du serveur de gestion.

Envoi d'événements CA Audit à CA Enterprise Log Manager

Vous pouvez intégrer CA Enterprise Log Manager dans votre implémentation CA Audit de l'une des manières ci-dessous.

- Reconfigurez un iRecorder ne se trouvant pas sur le même hôte qu'un client CA Audit pour envoyer les événements à CA Enterprise Log Manager.
- Modifiez une stratégie CA Audit existante pour envoyer des événements à CA Audit et à CA Enterprise Log Manager.

Configuration d'iRecorder pour envoyer des événements à CA Enterprise Log Manager

CA Enterprise Log Manager reçoit des événements provenant d'iRecorders par le biais de l'écouteur du module d'extension d'événements iTech. Vous devez configurer l'écouteur avant de modifier la configuration d'iRecorder. Sans quoi, vous risquez de perdre des données d'événement. Après avoir configuré l'écouteur, utilisez cette procédure pour configurer l'iRecorder afin qu'il envoie les événements au serveur CA Enterprise Log Manager.

Les iRecorders installés sur le même ordinateur qu'un client CA Audit envoient des événements directement au client. Pour ces ordinateurs, vous devez utiliser des adaptateurs de collecteur ou de routeur SAPI.

Important : Un iRecorder autonome peut envoyer ses événements à une seule destination. Si vous reconfigurez un iRecorder à l'aide de la procédure qui suit, les événements sont stockés *uniquement* dans le magasin de journaux d'événements CA Enterprise Log Manager. Si vous devez conserver des événements dans le magasin de journaux d'événements et dans la base de données du collecteur CA Audit, modifiez une action de règle dans une stratégie existante ou créez une nouvelle stratégie pour un client CA Audit client.

Pour configurer iRecorder pour envoyer des événements à CA Enterprise Log Manager

1. Connectez-vous au serveur hébergeant iRecorder en tant qu'utilisateur doté des droits d'administrateur.
2. Accédez au dossier de votre système d'exploitation.
 - UNIX ou Linux : /opt/CA/SharedComponents/iTechnology
 - Windows : \Program Files\CA\SharedComponents\iTechnology
3. Arrêtez le démon ou le service iGateway avec la commande ci-après.
 - UNIX ou Linux : ./S99gateway stop
 - Windows : net stop igateway
4. Modifiez le fichier iControl.conf.
5. Spécifiez la valeur RouteEvent ci-dessous.

```
<RouteEvent>>true</RouteEvent>
```

Cette entrée indique à iGateway d'envoyer ses événements, notamment tous les événements iRecorder, à l'hôte nommé dans la paire de balises RouteHost.

6. Spécifiez la valeur RouteHost ci-dessous.

```
<RouteHost>nom_hôte_CA_ELM</RouteHost>
```

Cette entrée indique à iGateway d'envoyer ses événements au serveur CA Enterprise Log Manager en utilisant son nom DNS.

7. Redémarrez le démon ou le service iGateway avec la commande ci-après.
 - UNIX ou Linux : ./S99gateway start
 - Windows : net start igateway

Cette action oblige iRecorder à utiliser les nouveaux paramètres et lance le flux d'événements depuis iRecorder vers le serveur CA Enterprise Log Manager.

Informations complémentaires :

[A propos du routeur et du collecteur SAPI](#) (page 252)

[Configuration du service de collecteur SAPI](#) (page 254)

[Configuration du service de routeur SAPI](#) (page 254)

Modification d'une stratégie CA Audit existante pour envoyer des événements à CA Enterprise Log Manager

Utilisez la procédure suivante pour permettre à un client CA Audit d'envoyer des événements *à la fois* à CA Enterprise Log Manager et à la base de données du collecteur CA Audit. En ajoutant une nouvelle cible aux actions Collecteur ou Acheminement d'une règle existante, vous pouvez envoyer les événements collectés aux deux systèmes. Vous pouvez également modifier des stratégies ou règles spécifiques pour envoyer des événements *uniquement* au serveur CA Enterprise Log Manager.

CA Enterprise Log Manager collecte les événements provenant de clients CA Audit à l'aide des écouteurs du routeur SAPI CA Audit et du collecteur SAPI CA Audit. Les événements collectés sont conservés dans le magasin de journaux d'événements CA Enterprise Log Manager uniquement *après* l'envoi de la stratégie aux clients et son activation.

Important : Vous devez configurer les écouteurs CA Enterprise Log Manager pour recevoir des événements avant de modifier et d'activer la stratégie. Si vous n'effectuez pas cette configuration en premier, vous constaterez peut-être des événements mal mappés, s'ils se produisent entre le moment où la stratégie devient active et celui où les écouteurs peuvent mapper correctement les événements.

Pour modifier une action d'une règle de stratégie afin d'envoyer des événements à CA Enterprise Log Manager

1. Connectez-vous au serveur gestionnaire de stratégies et accédez à l'onglet Mes stratégies, dans le volet gauche.
2. Développez le dossier de la stratégie jusqu'à visualiser la stratégie souhaitée.
3. Cliquez sur la stratégie pour afficher ses informations de base dans le volet Détails, sur la droite.
4. Dans le volet Détails, cliquez sur Modifier pour faire un ajout aux règles de la stratégie. L'assistant de règles démarre.

5. Cliquez sur Modifier les actions, en regard de la flèche correspondant à l'étape 3 de l'assistant. La page des actions de règles de l'assistant s'affiche.
6. Cliquez sur l'action Collecteur dans le volet Parcourir les actions, sur la gauche. La liste des actions s'affiche sur la droite.

Vous pouvez également utiliser l'action Acheminement pour créer une règle permettant d'envoyer des événements à un serveur CA Enterprise Log Manager.

7. Cliquez sur Nouveau pour ajouter une nouvelle règle.
8. Entrez l'adresse IP ou le nom d'hôte du serveur CA Enterprise Log Manager de collecte.

Pour les implémentations CA Enterprise Log Manager comptant plusieurs serveurs, vous pouvez entrer un autre nom d'hôte ou adresse IP CA Enterprise Log Manager dans le champ Autre nom d'hôte pour bénéficier de la fonction de basculement automatique de <Aus>. Si le premier serveur CA Enterprise Log Manager n'est pas disponible, CA Audit envoie automatiquement les événements au serveur nommé dans le champ Autre nom d'hôte.

9. Entrez le nom du serveur CA Enterprise Log Manager de gestion dans le champ Autre nom d'hôte, puis créez une description pour cette nouvelle action de règle.
10. Si la case à cocher Effectuer cette action sur un serveur distant est sélectionnée, désélectionnez-la.
11. Cliquez sur Ajouter pour enregistrer la nouvelle action de règle, puis sur Terminer dans la fenêtre de l'assistant.
12. Sélectionnez l'onglet Règles dans le volet inférieur droit, puis sélectionnez une règle à vérifier.
13. Cliquez sur Vérifier les stratégies pour vérifier la règle modifiée avec les nouvelles actions et vous assurer de sa compilation adéquate.
Apportez les modifications nécessaires à la règle et assurez-vous de sa compilation adéquate avant de l'activer.
14. Cliquez sur Activer pour distribuer la stratégie vérifiée, qui contient les nouvelles actions de règle ajoutées.
15. Répétez cette procédure pour chaque règle et stratégie portant sur les événements collectés à envoyer à CA Enterprise Log Manager.

Informations complémentaires :

[A propos du routeur et du collecteur SAPI](#) (page 252)

[Configuration du service de collecteur SAPI](#) (page 254)

[Configuration du service de routeur SAPI](#) (page 254)

Modification d'une stratégie r8 SP2 pour envoyer des événements à CA Enterprise Log Manager

Utilisez la procédure suivante pour permettre à un client CA Audit r8 SP2 d'envoyer des événements à CA Enterprise Log Manager et à la base de données du collecteur CA Audit. En ajoutant une nouvelle cible aux actions Collecteur ou Acheminement d'une règle existante, vous pouvez envoyer les événements collectés aux deux systèmes. Vous pouvez également modifier des stratégies ou règles spécifiques pour envoyer des événements *uniquement* au serveur CA Enterprise Log Manager.

Vous trouverez plus d'informations sur l'utilisation des stratégies dans le *Manuel d'implémentation CA Audit r8 SP2*. Reportez-vous à cette ressource pour plus de détails sur la réalisation des étapes de la procédure qui suit.

CA Enterprise Log Manager collecte les événements provenant de clients CA Audit à l'aide des écouteurs du routeur SAPI CA Audit et du collecteur SAPI CA Audit. Les événements collectés sont conservés dans le magasin de journaux d'événements CA Enterprise Log Manager *uniquement après* l'envoi de la stratégie aux clients et son activation.

Important : Vous devez configurer les écouteurs CA Enterprise Log Manager pour recevoir des événements avant de modifier et d'activer la stratégie. Si vous n'effectuez pas cette configuration en premier, vous constaterez peut-être des événements mal mappés entre le moment où la stratégie devient active et celui où les écouteurs peuvent mapper correctement les événements.

Pour modifier une action d'une règle de stratégie r8 SP2 afin d'envoyer des événements à CA Enterprise Log Manager

1. Connectez-vous au serveur gestionnaire de stratégies en tant qu'utilisateur doté du rôle Maker.
2. Accédez à la règle que vous souhaitez modifier en développant son dossier dans le volet Stratégies et en choisissant la stratégie souhaitée.
La stratégie s'affiche, accompagnée de ses règles, dans le volet Détails.
3. Cliquez sur la règle que vous souhaitez modifier.
La règle s'affiche, accompagnée de ses actions, dans le volet Détails.
4. Cliquez sur Modifier.
L'assistant de modification de règle s'affiche.
5. Utilisez l'assistant de modification de règle pour modifier la règle afin qu'elle envoie les événements au serveur CA Enterprise Log Manager en plus des destinations actuelles ou à la place de celles-ci, puis cliquez sur Terminer une fois la modification terminée.
6. Vérifiez et validez la stratégie en tant qu'utilisateur Maker, pour qu'elle puisse être approuvée par un utilisateur doté d'un rôle Checker.
7. Déconnectez-vous, puis reconnectez-vous au serveur gestionnaire de stratégies en tant qu'utilisateur doté du rôle Checker, si votre entreprise pratique la séparation des fonctions.
8. Examinez et approuvez le dossier contenant la stratégie et la règle modifiées.
Une fois la stratégie approuvée, les paramètres du serveur de distribution du gestionnaire de stratégies déterminent à quel moment la nouvelle stratégie est distribuée aux noeuds d'audit. Vous pouvez examiner le journal d'activation pour vérifier l'état d'activation d'une stratégie.
9. Répétez cette procédure pour chaque règle et stratégie portant sur les événements collectés à envoyer à CA Enterprise Log Manager.

Quand importer des événements

Si vous disposez d'un serveur d'outils de données CA Audit avec une base de données de collecteur, vous disposez d'une table SEOSDATA contenant des données d'événement. Pour exécuter vos systèmes CA Audit et CA Enterprise Log Manager en parallèle et afficher des rapports sur les données déjà collectées, vous souhaitez peut-être importer des données provenant de votre table SEOSDATA.

Vous pouvez exécuter l'utilitaire d'importation SEOSDATA pour effectuer une importation des données d'événement de votre base de données de collecteur vers un magasin de journaux d'événements CA Enterprise Log Manager. En général, vous importez des données d'événement immédiatement après avoir déployé un serveur CA Enterprise Log Manager. Si vous intégrez les deux systèmes, vous pouvez décider d'effectuer l'importation des données à plusieurs reprises, en fonction de votre utilisation et de la configuration du réseau.

Remarque : L'importation de données provenant de la table SEOSDATA ne supprime *pas* ou ne modifie pas les données stockées dans la table. La procédure d'importation copie les données, les analyse et les mappe vers le magasin de journaux d'événements CA Enterprise Log Manager.

A propos de l'utilitaire d'importation SEOSDATA

L'utilitaire d'importation LMSeosImport utilise une interface de ligne de commande et prend en charge les systèmes d'exploitation Windows et Solaris. L'utilitaire effectue les actions ci-dessous.

- Il se connecte à la table SEOSDATA pour extraire les événements de la manière spécifiée.
- Il analyse les événements SEOSDATA sélectionnés par paires nom-valeur.
- Il envoie les événements aux CA Enterprise Log Manager par le biais du sponsor d'événements SAPI ou iTech, pour les insérer dans le magasin de journaux d'événements.

Les événements sont mappés vers la grammaire commune aux événements (CEG), qui constitue la base des tables de base de données du magasin de journaux d'événements. Vous pouvez ensuite utiliser les requêtes et rapports prédéfinis pour collecter des informations sur vos événements stockés.

Importation à partir d'une table SEOSDATA en temps réel

L'exécution de l'utilitaire LMSeosImport sur une table SEOSDATA en temps réel n'est pas recommandée, mais elle peut parfois être inévitable. Si vous devez exécuter l'utilitaire sur une table en temps réel, celui-ci importe uniquement une certaine section de données. En effet, les événements ajoutés à la base de données *après* le lancement de l'utilitaire LMSeosImport ne sont pas importés au cours de cette session d'importation.

Par exemple, si vous ne spécifiez pas les paramètres `-minid` et `-maxid` dans la ligne de commande, lorsque l'utilitaire démarre, il envoie une requête à la base de données pour trouver les ID d'entrée minimal et maximal existants. Par la suite, l'utilitaire se sert de ses requêtes et importe les activités en fonction de ces valeurs. Les événements insérés dans la base de données après le démarrage de l'utilitaire sont dotés d'ID d'entrée en dehors de cette plage et ne sont donc pas importés.

Une fois la session d'importation terminée, l'utilitaire affiche le dernier ID d'entrée traité. Vous devrez peut-être exécuter plusieurs sessions d'importation pour obtenir tous vos événements. Vous pouvez également choisir d'attendre une période de moindre activité des événements et du réseau pour exécuter l'utilitaire d'importation. Vous pouvez exécuter d'autres sessions d'importation, si nécessaire, à l'aide de l'ID d'entrée de fin de la dernière session comme valeur `-minid` de la nouvelle session.

Importation des données d'une table SEOSDATA

Utilisez ce processus pour importer des données provenant d'une base de données de collecteur (table SEOSDATA), afin de garantir les meilleurs résultats possibles.

1. Copiez l'utilitaire `LMSeosImport` dans le dossier `iTechnology` d'un serveur d'outils de données CA Audit.

Remarque : L'utilitaire `LMSeosImport` implique les bibliothèques de prise en charge `etsapi` et `etbase`, fournies avec le client CA Audit.

2. Découvrez les options et la ligne de commande `LMSeosImport`.
3. Créez un rapport d'événements pour afficher les types d'événements, leur nombre et les plages d'ID d'entrée.
4. Prévisualisez les résultats d'importation grâce aux paramètres que vous envisagez d'utiliser.

Vous pouvez décider d'exécuter une nouvelle fois l'importation prévisualisée pour ajuster les options de la ligne de commande, le cas échéant.

5. Importez des événements d'une base de données de collecteur à l'aide des options ajustées de la ligne de commande.

Copie de l'utilitaire d'importation d'événements sur un serveur d'outils de données Solaris

Avant de pouvoir importer des données à partir de votre table SEOSDATA, vous devez copier l'utilitaire LMSeosImport depuis le DVD-ROM d'installation de l'application CA Enterprise Log Manager vers votre serveur d'outils de données Solaris.

Remarque : L'utilitaire LMSeosImport nécessite la présence des bibliothèques *etsapi* et *etbase*. Ces fichiers font partie de l'installation de base du serveur d'outils de données. Avant d'essayer d'utiliser l'utilitaire LMSeosImport, assurez-vous que le répertoire d'installation d'CA Audit est inclus dans votre instruction PATH système. Le répertoire par défaut est `opt/CA/eTrustAudit/bin`.

Avant d'exécuter l'utilitaire, définissez les variables d'environnement ci-après avec la commande *env*.

- ODBC_HOME=<répertoire d'installation des outils de données CA Audit>/odbc
- ODBCINI=<répertoire d'installation des outils de données CA Audit>/odbc/odbc.ini

Pour copier l'utilitaire

1. Ouvrez une invite de commande sur le serveur d'outils de données Solaris.
2. Insérez le DVD-ROM d'installation de l'application CA Enterprise Log Manager.
3. Accédez au répertoire `/CA/ELM/Solaris_sparc`.
4. Copiez l'utilitaire LMSeosImport dans le répertoire iTechnology du serveur d'outils de données CA Audit : `/opt/CA/SharedComponents/iTechnology`.

L'utilitaire est prêt à être utilisé après avoir été copié dans le répertoire désigné et une fois les variables d'environnement requises définies. Il n'existe aucune installation distincte à exécuter.

Copie de l'utilitaire d'importation sur un serveur d'outils de données Windows

Avant de pouvoir importer des données à partir de votre table SEOSDATA, vous devez copier l'utilitaire LMSeosImport depuis le DVD-ROM d'installation de l'application CA Enterprise Log Manager vers votre serveur d'outils de données Windows.

Remarque : L'utilitaire LMSeosImport nécessite la présence des bibliothèques de liens dynamiques *etsapi* et *etbase*. Ces fichiers font partie de l'installation de base du serveur d'outils de données. Avant d'essayer d'utiliser l'utilitaire LMSeosImport, assurez-vous que le répertoire Program Files\CA\Trust Audit\bin est inclus dans votre instruction PATH système.

Pour copier l'utilitaire

1. Ouvrez une invite de commande sur le serveur d'outils de données Windows.
2. Insérez le DVD-ROM d'installation de l'application CA Enterprise Log Manager.
3. Accédez au répertoire \CA\ELM\Windows.
4. Copiez l'utilitaire LMSeosImport.exe dans le répertoire iTechnology du serveur d'outils de données CA Audit : <lecteur>:\Program Files\CA\SharedComponents\iTechnology.

L'utilitaire est prêt à être utilisé après avoir été copié dans le répertoire désigné. Il n'existe aucune installation distincte à exécuter.

Présentation de la ligne de commande LMSeosImport

L'utilitaire LMSeosImport propose de nombreux arguments de ligne de commande qui vous permettent de contrôler les événements migrés. Chaque événement de la table SEOSDATA compose une ligne et dispose d'un *ID d'entrée* unique pour l'identifier. Vous pouvez utiliser l'utilitaire d'importation pour récupérer un rapport répertoriant plusieurs types différents d'informations utiles. Le rapport répertorie le nombre d'événements dans la table SEOSDATA (nombre d'ID d'entrée), les nombres d'événements par type de journal et les plages de dates des événements. L'utilitaire propose une option de reprise en cas d'erreur au cours de l'importation d'un événement.

Vous pouvez également exécuter un job d'aperçu pour connaître les résultats de l'importation avec une structure de commande spécifique. Les jobs d'aperçu n'importent pas réellement les données. Cela vous permet d'ajuster vos options de ligne de commande avant la migration réelle.

Vous pouvez exécuter plusieurs fois l'utilitaire de migration, en utilisant différents paramètres pour importer différents types de données. Par exemple, vous pouvez choisir de migrer vos données en plusieurs sessions adaptées, en fonction d'une plage d'ID d'entrée, du type de journal ou de plages de dates précises.

Remarque : L'utilitaire ne propose *pas* le suivi d'importation des sessions antérieures. Il est possible de dupliquer les données dans votre base de données CA Enterprise Log Manager si vous exécutez la commande plusieurs fois avec les mêmes paramètres.

Pour obtenir les meilleurs résultats, restreignez votre importation au type de journal (à l'aide de l'option `-log`) ou à l'ID d'entrée (à l'aide des options `-minid` et `-maxid`) pour améliorer les performances de l'importation. Utilisez l'option `-retry` pour permettre la récupération après n'importe quelle erreur pouvant survenir au cours de l'importation d'événements. L'utilitaire utilise la valeur `-retry` par défaut de 300 secondes, afin d'optimiser la réussite de l'importation.

Commande et options de l'utilitaire d'importation

L'utilitaire `LMSeosImport` prend en charge la syntaxe et les options de la ligne de commande répertoriées ci-dessous.

```
LMSeosImport -dsn nom_dsn -user nom_utilisateur -password mot_de_passe -target  
nom_cible {-sid nnn -eid nnnn -stm aaaa-mm-jj -etm aaaa-mm-jj -log nom_journal -  
transport (sapi|itech) -chunk nnnn -pretend -verbose -delay -report -retry}
```

-dsn

Spécifie le nom du serveur hôte sur lequel se trouve la table SEOSDATA. Ce paramètre est obligatoire.

-user

Spécifie un ID d'utilisateur valide bénéficiant au minimum d'un accès en lecture à la table SEOSDATA. Ce paramètre est obligatoire.

-password

Spécifie le mot de passe du compte d'utilisateur précisé par le paramètre `-user`. Ce paramètre est obligatoire.

-target

Spécifie le nom d'hôte ou l'adresse IP du serveur CA Enterprise Log Manager pour recevoir les événements migrés depuis la table SEOSDATA. Ce paramètre est obligatoire.

-minid nnnn

Indique l'ENTRYID de début utilisé lors de la sélection d'événements dans la table SEOSDATA. Ce paramètre est facultatif.

-maxid nnnn

Indique l'ENTRYID de fin utilisé lors de la sélection d'événements dans la table SEOSDATA. Ce paramètre est facultatif.

-mintm AAAA-MM-JJ

Indique l'heure de début (au format AAAA-MM-JJ) utilisée lors de la sélection d'événements dans la table SEOSDATA. Ce paramètre est facultatif.

-maxtm AAAA-MM-JJ

Indique l'heure de fin (au format AAAA-MM-JJ) utilisée lors de la sélection d'événements dans la table SEOSDATA. Ce paramètre est facultatif.

-log nom_journal

Spécifie que l'utilitaire doit sélectionner uniquement les enregistrements d'événements avec le nom de journal spécifié. Ce paramètre est facultatif. Si le nom du journal contient des espaces, il doit être placé entre guillemets doubles.

-transport <sapi | itech >

Spécifie la méthode de transport qui doit être utilisée entre l'utilitaire d'importation et CA Enterprise Log Manager. La méthode de transport par défaut est sapi.

-chunk nnnn

Spécifie le nombre d'enregistrements d'événements à sélectionner dans la table SEOSDATA à chaque passage. La valeur par défaut est 5 000 événements (lignes). Ce paramètre est facultatif.

-preview

Sort les résultats des sélections d'enregistrements d'événements vers STDOUT, mais n'importe pas réellement les données. Ce paramètre est facultatif.

-port

Spécifie le numéro de port à utiliser si vous définissez l'option de transport sur SAPI et que vous avez configuré le routeur SAPI CA Enterprise Log Manager pour utiliser une valeur de port fixe (sans utiliser le mappeur de ports).

-verbose

Spécifie que l'utilitaire envoie des messages de traitement détaillés à STDOUT. Ce paramètre est facultatif.

-delay

Spécifie le nombre de secondes de pause entre le traitement de deux événements. Ce paramètre est facultatif.

-report

Affiche un rapport sur la période, la plage ENTRYID et le nombre de journaux dans la table SEOSDATA. Ce paramètre est facultatif.

-retry

Spécifie le nombre total de secondes au cours desquelles des tentatives de reprise sont effectuées à chaque fois qu'une erreur se produit au cours de l'importation d'un événement. Le traitement continue lorsque l'envoi de cet événement est à nouveau réussi. L'utilitaire utilise automatiquement une valeur par défaut de 300 secondes. Vous n'avez pas à entrer le paramètre, sauf si vous souhaitez spécifier une valeur différente. Les messages liés à l'état de la reprise sont envoyés à STDOUT.

Exemples de la ligne de commande LMSeosImport

Vous pouvez utiliser les exemples suivants de ligne de commande pour créer votre commande personnalisée lors de l'utilisation de l'utilitaire d'importation SEOSDATA.

Pour exécuter l'importation d'enregistrements entre les ENTRYID 1 000 et 4 000

Entrez la ligne de commande ci-dessous.

```
LMSeosImport -dsn eAudit_DSN -user sa -password sa -target 130.200.137.192 -minid 1000 -maxid 4000
```

Pour exécuter l'importation d'enregistrements pour des événements d'applications Windows NT uniquement

Entrez la ligne de commande ci-dessous.

```
LMSeosImport -dsn eAudit_DSN -user sa -password sa -target 130.200.137.192 -log NT-Application
```

Création d'un rapport d'événements

L'exécution d'un rapport d'événements SEOSDATA avant l'importation réelle des données vous fournit les informations nécessaires concernant les événements de la table. Le rapport indique la période de l'événement, le nombre d'événements par type de journal et la plage d'ID d'entrée. Vous pouvez utiliser les valeurs affichées dans le rapport pour affiner vos options de ligne de commande concernant une commande antérieure ou la commande d'importation réelle.

Pour afficher un rapport des informations d'événements SEOSDATA actuels sous Windows

1. Ouvrez une invite de commande sur le serveur d'outils de données CA Audit.
2. Accédez au répertoire \Program Files\CA\SharedComponents\iTechnology.
3. Entrez la ligne de commande ci-dessous.

```
LMSeosImport -dsn eAudit_DSN -user sa -password sa -target <nom_hôte_Log_Manager> -report
```

L'affichage du rapport généré est similaire à l'exemple qui suit.

```
SEOSProcessor::InitOdbc: liaison réussie à la source [eAudit_DSN]
```

```
----- Période d'événement SEOSDATA -----
```

```
DUREE minimale = 2007-08-27
```

```
DUREE maximale = 2007-10-06
```

```
----- Nombre d'événements par journal -----
```

```
com.ca.iTechnology.iSponsor : 3 052
```

```
EiamSdk : 1 013
```

```
NT-Application : 776
```

```
NT-System : 900
```

```
----- Plage EntryID SEOSDATA -----
```

```
ENTRYID minimal : 1
```

```
ENTRYID maximal : 5 741
```

```
Rapport terminé.
```

Prévisualisation des résultats de l'importation

Vous pouvez exécuter une importation test avec une sortie vers STDOUT pour prévisualiser les résultats d'importation sans réellement importer ou migrer les données. Il s'agit là d'un test efficace des paramètres de la ligne de commande, entrés pour une migration unique ou pour un job régulier d'importation en lot planifiée.

Pour exécuter une importation test afin de prévisualiser les résultats de l'importation

1. Ouvrez une invite de commande sur le serveur d'outils de données CA Audit.
2. Accédez au répertoire adéquat.

```
Solaris : /opt/CA/SharedComponents/iTechnology
```

```
Windows : \Program Files\CA\SharedComponents\iTechnology
```

3. Entrez la ligne de commande ci-dessous.

Pour Solaris

```
./LMSeosImport.sh -dsn eAudit_DSN -user sa -password sa -target
<nom_hôte_ou_IP_Log_Manager> -minid 1000 -maxid 4000 -preview
```

Pour Windows

```
LMSeosImport.exe -dsn eAudit_DSN -user sa -password sa -target
<nom_hôte_ou_IP_Log_Manager> -minid 1000 -maxid 4000 -preview
```

Importation d'événements provenant d'une base de données de collecteur Windows

Vous pouvez utiliser cette procédure pour importer des données d'événement provenant d'une base de données du collecteur qui se trouve sur un serveur d'outils de données Windows.

Pour importer des événements provenant d'une table SEOSDATA sur un serveur Windows

1. Localisez le nom du serveur sur lequel se trouve la table SEOSDATA.
2. Assurez-vous de disposer des informations d'identification d'accès utilisateur pour ce serveur, avec au minimum un accès en lecture à la table SEOSDATA.
3. Ouvrez une invite de commande sur le serveur d'outils de données CA Audit.
4. Accédez au répertoire \Program Files\CA\Shared Components\iTechnology.
5. Lancez l'utilitaire d'importation à l'aide de la syntaxe de commande ci-après.

```
LMSeosImport.exe -dsn <nom_dsn> -user <UID> -password <mot_de_passe> -target
<nom_hôte_cible> <indicateurs facultatifs>
```

Importation d'événements provenant d'une base de données de collecteur Solaris

Vous pouvez utiliser cette procédure pour importer des données d'événement provenant d'une base de données du collecteur qui se trouve sur un serveur d'outils de données Solaris.

Pour importer des événements provenant d'une table SEOSDATA sur un serveur Solaris

1. Localisez le nom du serveur sur lequel se trouve la table SEOSDATA.
2. Assurez-vous de disposer des informations d'identification d'accès utilisateur pour ce serveur, avec au minimum un accès en lecture à la table SEOSDATA.
3. Ouvrez une invite de commande sur le serveur d'outils de données CA Audit.
4. Accédez au répertoire /opt/CA/SharedComponents/iTechnology.
5. Lancez l'utilitaire d'importation à l'aide de la syntaxe de commande ci-après.

```
./LMSeosImport -dsn <nom_dsn> -user <UID> -password <mot_de_passe> -target  
<nom_hôte_cible> <indicateurs facultatifs>
```

Annexe B : Remarques pour les utilisateurs de CA Access Control

Ce chapitre traite des sujets suivants :

[Intégration avec CA Access Control](#) (page 273)

[Modification des stratégies CA Audit pour envoyer des événements à CA Enterprise Log Manager](#) (page 275)

[Configuration d'un iRecorder CA Access Control pour envoyer des événements à CA Enterprise Log Manager](#) (page 283)

[Importation d'événements CA Access Control provenant d'une base de données de collecteur CA Audit](#) (page 287)

Intégration avec CA Access Control

Vous pouvez intégrer CA Enterprise Log Manager avec CA Access Control en utilisant l'un des différents niveaux de version. L'approche générale est indiquée ci-dessous.

Pour les versions de CA Access Control qui utilisent un serveur de messages TIBCO pour le routage des événements, suivez la procédure ci-dessous.

- Installez un agent CA Enterprise Log Manager.
- Configurez un connecteur utilisant le connecteur `AccessControl_R12SP1_TIBCO_Connector`.

Pour CA Access Control r12.5, reportez-vous au *Manuel d'implémentation CA Access Control r12.5* et au *Manuel du connecteur CA Enterprise Log Manager CA Access Control*.

Pour CA Access Control r12 SP1, reportez-vous au *Manuel d'implémentation CA Access Control r12 SP1, 3e édition* et au *Manuel du connecteur CA Enterprise Log Manager pour CA Access Control*.

Remarque : Ces implémentations utilisent les composants inclus dans CA Access Control Premium Edition.

Pour les versions de CA Access Control qui utilisent selogrd pour le routage des événements, suivez la procédure ci-dessous.

- Installez un agent CA Enterprise Log Manager.
- Configurez un connecteur utilisant l'intégration ACSelogrd.

Vous trouverez plus d'informations sur la configuration d'un connecteur pour collecter les événements CA Access Control dans le *Manuel du connecteur CA Access Control r8 SP1*.

Si vous envoyez actuellement les événements CA Access Control à CA Audit, appliquez l'une des méthodes suivantes pour transmettre les événements à CA Enterprise Log Manager.

- Modifiez une stratégie CA Audit existante pour envoyer les événements à CA Audit et à CA Enterprise Log Manager, si vous utilisez un iRecorder CA Audit pour collecter des événements. Si vous le souhaitez, vous pouvez modifier la stratégie pour que les événements soient envoyés uniquement au serveur CA Enterprise Log Manager.
- Configurez le fichier control.conf afin qu'un iRecorder envoie les événements directement à CA Enterprise Log Manager.

Remarque : Si vous disposez d'une version d'eTrust Access Control qui ne prend pas en charge les iRecorders, vous pouvez envoyer les événements directement au routeur CA Audit. Pour plus d'informations, reportez-vous aux informations d'intégration de CA Audit contenues dans le *Manuel d'administration d'eTrust Access Control r5.3*.

Dans les instructions qui suivent, la série r8 SP2 est utilisée pour l'interface utilisateur du gestionnaire de stratégies. Les procédures générales sont les mêmes si vous utilisez une versions précédente de CA Audit, bien que l'interface utilisateur soit différente.

Modification des stratégies CA Audit pour envoyer des événements à CA Enterprise Log Manager

Le processus de modification d'une stratégie CA Audit existante pour envoyer des événements à CA Enterprise Log Manager implique les étapes ci-dessous.

- Collectez les informations nécessaires.
 - Assurez-vous de disposer des informations d'identification d'utilisateur du gestionnaire de stratégies CA Audit avec l'autorisation de créer, vérifier et activer des stratégies.
 - Obtenez l'adresse IP ou le nom d'hôte nécessaire pour accéder à l'interface utilisateur Administrator d'Audit. L'URL pour accéder à l'application Web du serveur du gestionnaire de stratégies de la série r8 SP2 est de la forme suivante.

```
https://<adresse_IP_gestionnaire_strategies_CA  
Audit>:5250/spin/auditadmin
```

- Configurez le service du collecteur SAPI ou du routeur SAPI CA Enterprise Log Manager en fonction de la méthode de création d'action de règle que vous voulez appliquer.

Si vous envisagez de créer une action Collecteur, configurez le collecteur SAPI. Si vous envisagez de configurer une action Acheminement, configurez le routeur SAPI.

Remarque : L'exemple de cette section utilise l'action Collecteur.

- Repérez et modifiez une stratégie CA Access Control existante pour envoyer des événements à CA Enterprise Log Manager.
- Vérifiez et activez la stratégie modifiée pour la distribuer aux noeuds d'audit.

Répétez ce processus pour ajouter de nouvelles actions de règle à d'autres règles de stratégies, le cas échéant.

Informations complémentaires :

[A propos du routeur et du collecteur SAPI](#) (page 252)

Configuration de l'adaptateur du collecteur SAPI pour recevoir des événements CA Access Control

Utilisez la procédure suivante pour configurer l'adaptateur du collecteur SAPI pour recevoir des événements CA Access Control provenant d'une implémentation CA Audit.

Vous pouvez modifier les stratégies CA Audit utilisant des actions du collecteur pour envoyer des événements à un serveur CA Enterprise Log Manager en plus ou à la place de l'envoi d'événements à la base de données du collecteur CA Audit. Configurez ce service *avant* de modifier les stratégies CA Audit pour vous assurer de ne perdre aucun événement.

Vous pouvez configurer un serveur de routeur SAPI de manière similaire. Si vous utilisez à la fois les services de routeur et de collecteur, assurez-vous que les ports répertoriés sont différents ou qu'ils sont contrôlés par le service du mappeur de ports.

Pour configurer le service de collecteur SAPI

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur Administrator et sélectionnez l'onglet Administration.

Le sous-onglet Collecte de journaux s'affiche par défaut.

2. Développez l'entrée Adaptateurs CA.



3. Sélectionnez le service Collecteur SAPI.

Configuration globale du service: CA Audit SAPI Collector

Administration **Evénements d'autosurveillance**

Enregistrer **Réinitialiser** **Utiliser les valeurs par défaut**

Configuration globale du service: CA Audit SAPI Collector

Affichez ou modifiez les détails de cette configuration.

= Requis

Activer l'écouteur **Port SAPI:**

Register **Clé de chiffrement:**

Classement des événements **Régulation des événements:**

Nombre de threads par file d'attente:

Chiffres

Disponible(s)	Sélectionné(e)(s)
	<input type="button" value="→"/> Aes256
	<input type="button" value="→"/> Aes128
	<input type="button" value="→"/> 3Des
	<input type="button" value="→"/> Des
	<input type="button" value="↑"/>
	<input type="button" value="↓"/>

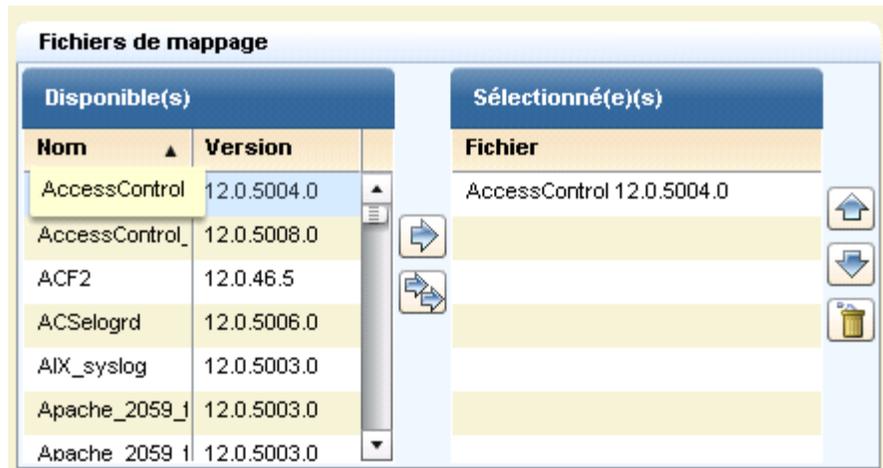
4. Cochez la case Activer l'écouteur et entrez dans le champ Port SAPI le même numéro de port que celui utilisé par CA Audit.

La valeur CA Enterprise Log Manager par défaut, 0, correspond à l'utilisation du service du mappeur de ports pour mapper les ports. Si un port est défini dans CA Audit, utilisez son numéro ici.

5. Acceptez les valeurs par défaut des autres champs et faites défiler l'affichage jusqu'à la liste des Fichiers de mappage.

Si vous cochez la case Enregistrer, vous devez spécifier un numéro de port SAPI.

6. Ajoutez l'entrée du fichier de mappage pour Access Control si elle est absente, puis supprimez les autres sélections de fichiers de mappage de la liste des fichiers de mappage Sélectionné(s).



7. Cliquez sur Enregistrer.

Modification d'une stratégie CA Audit existante pour envoyer des événements à CA Enterprise Log Manager

Utilisez la procédure suivante pour permettre à un client CA Audit d'envoyer des événements *à la fois* à CA Enterprise Log Manager et à la base de données du collecteur CA Audit. En ajoutant une nouvelle cible aux actions Collecteur ou Acheminement d'une règle existante, vous pouvez envoyer les événements collectés aux deux systèmes. Vous pouvez également modifier des stratégies ou règles spécifiques pour envoyer des événements *uniquement* au serveur CA Enterprise Log Manager.

CA Enterprise Log Manager collecte les événements provenant de clients CA Audit à l'aide des écouteurs du routeur SAPI CA Audit et du collecteur SAPI CA Audit. CA Enterprise Log Manager peut également collecter directement les événements en utilisant le module d'extension iTech si vous avez configuré des iRecorders afin qu'ils envoient directement les événements au serveur CA Enterprise Log Manager. Les événements collectés sont conservés dans le magasin de journaux d'événements CA Enterprise Log Manager uniquement *après* l'envoi de la stratégie aux clients et son activation.

Important : Configurez les écouteurs CA Enterprise Log Manager pour recevoir des événements avant de modifier et d'activer la stratégie. Si vous n'effectuez pas cette configuration en premier, des erreurs de mappage d'événements risquent de se produire entre le moment où la stratégie devient active et celui où les écouteurs peuvent mapper correctement les événements.

Pour modifier une action d'une règle de stratégie afin d'envoyer des événements à CA Enterprise Log Manager

1. Connectez-vous au serveur gestionnaire de stratégies et accédez à l'onglet Mes stratégies, dans le volet gauche.
2. Développez le dossier de la stratégie jusqu'à visualiser la stratégie souhaitée.



3. Cliquez sur la stratégie pour afficher ses informations de base dans le volet Détails, sur la droite.

The screenshot shows a window titled 'Détails' with a yellow background. At the top right, there are buttons: 'Nouvelle règle', 'Modifier', 'Supprimer', and 'Aide'. The main content area displays the following information:
Nom : Suspicious Events
Type : Rule
Description : Suspicious Events

4. Dans le volet Détails, cliquez sur Modifier pour faire un ajout aux règles de la stratégie.

L'assistant de règles démarre.

The screenshot shows the 'Modifier une règle : Information' wizard. At the top right, there are buttons: 'Précédent', 'Suivant', 'Terminer', 'Annuler', and 'Aide'. Below the title bar, there is a progress bar with three steps: '1 Modifier les informations' (highlighted with a yellow diamond), '2 Modifier le script', and '3 Modifier les actions'. The main area is divided into two panes:
Informations relatives à la règle (left):
Modifier le nom et la description de la règle.
Nom de règle: Suspicious Events
Description de règle: Suspicious Events
Aide rapide (right):
• Modifier le nom et la description de la règle.

5. Cliquez sur Modifier les actions en regard de la flèche correspondant à l'étape 3.

La page des actions de règles s'affiche.

The screenshot shows the 'Modifier une règle : Actions' wizard. At the top right, there are buttons: 'Précédent', 'Suivant', 'Terminer', 'Annuler', and 'Aide'. Below the title bar, there is a progress bar with three steps: '1 Modifier les informations', '2 Modifier le script', and '3 Modifier les actions' (highlighted with a yellow diamond). The main area is titled 'Parcourir les actions' and includes an 'Aide' button. Below the title, it says: 'Parcourez la liste des actions et créez-en de nouvelles à ajouter à la règle.' A list of actions is displayed, each with a small icon and a text label:

- Collector
- E-Mail
- eSCC Status Monitor
- External Program
- File
- Route
- Screen
- Security Monitor
- Snmp
- Unicenter

6. Cliquez sur l'action Collecteur dans le volet Parcourir les actions pour afficher la liste des actions à droite.

Modifier une règle : Actions Précédent Suivant Terminer Annuler Aide

1 Modifier les informations 2 Modifier le script 3 Modifier les actions

Parcourir les actions Aide
Parcourez la liste des actions et créez-en de nouvelles à ajouter à la règle.

- Collector
- E-Mail
- eSCC Status Monitor
- External Program
- File

Liste des actions Nouveau Modifier Supprimer

Nom d'hôte ou adresse IP	Utiliser le serveur distant	Paramètres optionnels	Description

Vous pouvez également utiliser l'action Routage, mais l'action Collecteur offre l'avantage de proposer un autre nom d'hôte pour le traitement de base du basculement.

7. Cliquez sur Nouveau pour ajouter une nouvelle règle.
8. Entrez l'adresse IP ou le nom d'hôte du serveur CA Enterprise Log Manager de collecte.

Modifier une règle : Actions Précédent Suivant Terminer Annuler Aide

1 Modifier les informations 2 Modifier le script 3 Modifier les actions

Parcourir les actions Aide
Parcourez la liste des actions et créez-en de nouvelles à ajouter à la règle.

- Collector
- E-Mail
- eSCC Status Monitor
- External Program
- File
- Route
- Screen
- Security Monitor
- Snmp
- Unicenter

Collector Ajouter Annuler

Nom d'hôte ou adresse IP: CA-ELM-Collector
 Nom de l'hôte secondaire: CA-ELM-Management
 Description: CA Enterprise Log Manager action

Effectuer cette action sur un serveur distant
 Le serveur est défini par le groupe de NA
 Le serveur est:

Dans le cas d'une implémentation CA Enterprise Log Manager comptant plusieurs serveurs, vous pouvez entrer un nom d'hôte ou une adresse IP CA Enterprise Log Manager différente dans le champ Autre nom d'hôte. Cela permet de bénéficier de la fonction de basculement automatique de CA Audit. Si le premier serveur CA Enterprise Log Manager n'est pas disponible, CA Audit envoie automatiquement les événements au serveur nommé dans le champ Autre nom d'hôte.

- Entrez le nom du serveur CA Enterprise Log Manager de gestion dans le champ Autre nom d'hôte, puis créez une description pour cette nouvelle action de règle.
- Si la case à cocher Effectuer cette action sur un serveur distant est sélectionnée, désélectionnez-la.
- Cliquez sur Ajouter pour enregistrer la nouvelle action de règle, puis sur Terminer dans la fenêtre de l'assistant.

Remarque : Vous devez ensuite vérifier et activer la stratégie ; ne vous déconnectez donc *pas* du gestionnaire de stratégies CA Audit.

Informations complémentaires :

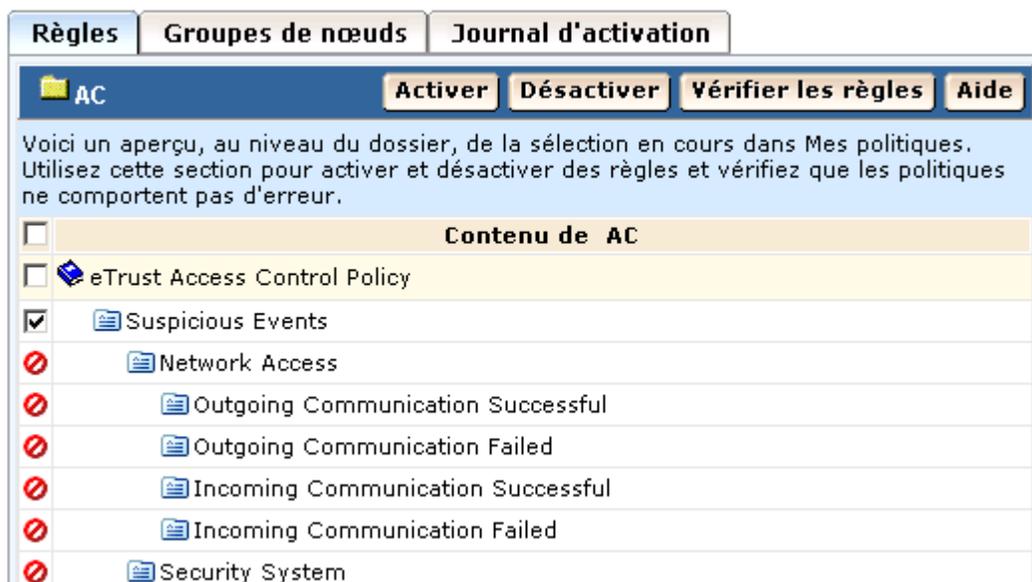
[Modification d'une stratégie r8 SP2 pour envoyer des événements à CA Enterprise Log Manager](#) (page 260)

Vérification et activation de la stratégie modifiée

Après avoir modifié une stratégie existante pour ajouter une action de règle, vérifiez-la (compilez-la), puis activez-la.

Pour vérifier et activer une stratégie CA Access Control

- Sélectionnez l'onglet Règles dans le volet inférieur droit, puis sélectionnez une règle à vérifier.



2. Cliquez sur Vérifier les stratégies pour vérifier la règle modifiée avec les nouvelles actions et vous assurer de sa compilation adéquate.
Apportez les modifications nécessaires à la règle et assurez-vous de sa compilation adéquate avant de l'activer.
3. Cliquez sur Activer pour distribuer la stratégie vérifiée, qui contient les nouvelles actions de règle ajoutées.
4. Répétez cette procédure pour chaque règle et stratégie portant sur les événements collectés à envoyer à CA Enterprise Log Manager.

Configuration d'un iRecorder CA Access Control pour envoyer des événements à CA Enterprise Log Manager

Vous pouvez configurer un iRecorder CA Access Control autonome pour qu'il envoie directement les événements qu'il collecte au serveur CA Enterprise Log Manager à des fins de stockage et de génération de rapport. Ce processus inclut les étapes ci-dessous.

1. Configurez l'écouteur du module d'extension d'événements iTech pour recevoir les informations d'un iRecorder CA Access Control.
2. Téléchargez et installez un iRecorder CA Access Control.
3. Configurez l'iRecorder afin qu'il envoie directement les événements qu'il a collectés à CA Enterprise Log Manager.
4. Vérifiez que CALM reçoit bien les événements.

Remarque : Les iRecorders peuvent envoyer leurs événements à une seule destination. Si vous avez suivi cette procédure pour la configuration, la seule destination est le serveur CA Enterprise Log Manager nommé.

Configuration du module d'extension d'événements iTech pour des événements CA Access Control

Avant de reconfigurer un iRecorder pour envoyer les événements directement à CA Enterprise Log Manager, vous devez configurer un écouteur pour recevoir ces événements.

Pour configurer l'écouteur

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur doté du rôle Administrator.
2. Accédez à l'onglet Administration, puis développez le noeud Adaptateurs CA.



3. Développez le noeud du module d'extension d'événements iTechnology.
4. Sélectionnez le serveur CA Enterprise Log Manager actuel pour afficher les paramètres locaux.
5. Veillez à ce que le fichier de mappage AccessControl soit le premier de la liste des fichiers de mappage Sélectionné(s), afin de garantir des opérations très efficaces.
6. Vérifiez que la valeur Niveau de journal est paramétrée sur NOTSET pour collecter tous les niveaux d'événements.
7. Cliquez sur Enregistrer.

Téléchargement et installation d'un iRecorder CA Access Control

Vous pouvez collecter les événements CA Access Control à envoyer à un serveur CA Enterprise Log Manager même si vous n'avez pas installé CA Audit. Lorsque vous collectez des événements de cette manière, vous utilisez un iRecorder en mode autonome. Vous pouvez obtenir un iRecorder sur le site Web du support CA.

Remarque : Les iRecorders sont pris en charge uniquement par CA Access Control r8 et version ultérieure.

Pour télécharger et installer un iRecorder

1. Accédez au site Web CA ci-dessous.

<https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/154/cacirecr8-certmatrix.html#caacirec> (en anglais)

2. Sélectionnez l'iRecorder adapté à votre version de CA Access Control.
3. Affichez et suivez les instructions d'installation disponibles grâce au lien Manuel d'intégration dans la matrice.

Configuration d'un iRecorder CA Access Control autonome

Utilisez la procédure suivante pour configurer votre iRecorder pour qu'il envoie des événements CA Access Control à CA Enterprise Log Manager.

Important : Un iRecorder autonome peut envoyer ses événements à une seule destination. Si vous configurez un iRecorder à l'aide de la procédure qui suit, tous les iRecorders installés sur ce système envoient leurs événements *uniquement* au magasin de journaux d'événements CA Enterprise Log Manager nommés.

Les iRecorders installés sur le même ordinateur qu'un client CA Audit envoient des événements directement au client. Pour ces serveurs, vous devez modifier une stratégie CA Audit existante pour ajouter des actions de règle, puis configurer les adaptateurs de collecteur ou de routeur SAPI CA Enterprise Log Manager.

Pour configurer iRecorder pour envoyer des événements à CA Enterprise Log Manager

1. Connectez-vous au serveur hébergeant iRecorder en tant qu'utilisateur doté des droits Administrator ou root.
2. Accédez au dossier de votre système d'exploitation.
 - UNIX ou Linux : /opt/CA/SharedComponents/iTechnology
 - Windows : \Program Files\CA\SharedComponents\iTechnology
3. Arrêtez le démon ou le service iGateway avec la commande ci-après.
 - UNIX ou Linux : ./S99gateway stop
 - Windows : net stop igateway
4. Modifiez le fichier iControl.conf.

Vous trouverez ci-dessous un exemple de fichier iControl, dans lequel les sections que vous devez modifier apparaissent en gras.

```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<iSponsor>
  <Name>iControl</Name>
  <ImageName>iControl</ImageName>
  <Version>4.5.0.2</Version>
  <DispatchEP>iDispatch</DispatchEP>
  <ISType>DSP</ISType>
  <Gated>>false</Gated>
  <PreLoad>>true</PreLoad>
  <RouteEvent>false</RouteEvent>
  <RouteEventHost>localhost</RouteEventHost>
  <EventsToCache>100</EventsToCache>
  <EventUseHttps>>true</EventUseHttps>
  <EventUsePersistentConnections>>true</EventUsePersistentConnections>
  <EventUsePipeline>>false</EventUsePipeline>
  <StoreEventHost max="10000">localhost</StoreEventHost>
  <RetrieveEventHost interval="60">localhost</RetrieveEventHost>
  <UID>ef1f44ef-r8sp1cr3596a1052-abcd28-2</UID>
  <PublicKey>Valeur_clé_publicue</PublicKey>
  <PrivateKey>Valeur_clé_privée</PrivateKey>
  <EventsToQueue>10</EventsToQueue>
</iSponsor>
```

5. Spécifiez la valeur RouteEvent ci-dessous.

```
<RouteEvent>true</RouteEvent>
```

Cette entrée indique à iGateway d'envoyer ses événements, notamment tous les événements iRecorder, à l'hôte nommé dans la paire de balises RouteEventHost.

6. Spécifiez la valeur RouteEventHost ci-dessous.

```
<RouteEventHost>Votre_nom_hôte_CA_Enterprise_Log_Manager</RouteEventHost>
```

Cette entrée indique à iGateway d'envoyer ses événements au serveur CA Enterprise Log Manager en utilisant son nom DNS.

7. Enregistrez et fermez le fichier.
8. Redémarrez le démon ou le service iGateway avec la commande ci-après.

- UNIX ou Linux : `./S99gateway start`
- Windows : `net start gateway`

Cette action oblige iRecorder à utiliser les nouveaux paramètres et lance le flux d'événements depuis iRecorder vers le serveur CA Enterprise Log Manager.

Importation d'événements CA Access Control provenant d'une base de données de collecteur CA Audit

Le processus d'importation d'événements CA Access Control à partir d'une table SEOSDATA existante inclut les étapes ci-après.

1. Copiez l'utilitaire LMSeosImport sur le serveur d'outils de données CA Audit.
2. Créez un rapport d'événements pour déterminer si les événements CA Access Control sont présents dans la base de données.
3. Exécutez un aperçu de l'importation avec les paramètres spécifiques à CA Access Control.
4. Importez les événements CA Access Control.
5. Exécutez les requêtes et rapports CA Enterprise Log Manager sur les événements importés.

Tâches requises avant l'importation d'événements CA Access Control

Avant d'utiliser l'utilitaire LMSeosImport, suivez les étapes ci-dessous.

- Obtenez un compte d'utilisateur de bases de données doté au minimum de l'accès en lecture à la table SEOSDATA de CA Audit.
- Copiez l'utilitaire LMSeosImport sur le serveur d'outils de données CA Audit.
- Accédez à une invite de commande sur le serveur d'outils de données et recherchez le répertoire adéquat.

Solaris : /opt/CA/SharedComponents/iTechnology

Windows : \Program Files\CA\SharedComponents\iTechnology

Copie de l'utilitaire d'importation sur un serveur d'outils de données Windows

Avant de pouvoir importer des données à partir de votre table SEOSDATA, vous devez copier l'utilitaire LMSeosImport depuis le DVD-ROM d'installation de l'application CA Enterprise Log Manager vers votre serveur d'outils de données Windows.

Remarque : L'utilitaire LMSeosImport nécessite la présence des bibliothèques de liens dynamiques *etsapi* et *etbase*. Ces fichiers font partie de l'installation de base du serveur d'outils de données. Avant d'essayer d'utiliser l'utilitaire LMSeosImport, assurez-vous que le répertoire Program Files\CA\eTrust Audit\bin est inclus dans votre instruction PATH système.

Pour copier l'utilitaire

1. Ouvrez une invite de commande sur le serveur d'outils de données Windows.
2. Insérez le DVD-ROM d'installation de l'application CA Enterprise Log Manager.
3. Accédez au répertoire \CA\ELM\Windows.
4. Copiez l'utilitaire LMSeosImport.exe dans le répertoire iTechnology du serveur d'outils de données CA Audit : <lecteur>:\Program Files\CA\SharedComponents\iTechnology.

L'utilitaire est prêt à être utilisé après avoir été copié dans le répertoire désigné. Il n'existe aucune installation distincte à exécuter.

Copie de l'utilitaire d'importation d'événements sur un serveur d'outils de données Solaris

Avant de pouvoir importer des données à partir de votre table SEOSDATA, vous devez copier l'utilitaire LMSeosImport depuis le DVD-ROM d'installation de l'application CA Enterprise Log Manager vers votre serveur d'outils de données Solaris.

Remarque : L'utilitaire LMSeosImport nécessite la présence des bibliothèques *etsapi* et *etbase*. Ces fichiers font partie de l'installation de base du serveur d'outils de données. Avant d'essayer d'utiliser l'utilitaire LMSeosImport, assurez-vous que le répertoire d'installation d'CA Audit est inclus dans votre instruction PATH système. Le répertoire par défaut est `opt/CA/eTrustAudit/bin`.

Avant d'exécuter l'utilitaire, définissez les variables d'environnement ci-après avec la commande *env*.

- ODBC_HOME=<répertoire d'installation des outils de données CA Audit>/odbc
- ODBCINI=<répertoire d'installation des outils de données CA Audit>/odbc/odbc.ini

Pour copier l'utilitaire

1. Ouvrez une invite de commande sur le serveur d'outils de données Solaris.
2. Insérez le DVD-ROM d'installation de l'application CA Enterprise Log Manager.
3. Accédez au répertoire `/CA/ELM/Solaris_sparc`.
4. Copiez l'utilitaire LMSeosImport dans le répertoire iTechnology du serveur d'outils de données CA Audit : `/opt/CA/SharedComponents/iTechnology`.

L'utilitaire est prêt à être utilisé après avoir été copié dans le répertoire désigné et une fois les variables d'environnement requises définies. Il n'existe aucune installation distincte à exécuter.

Création d'un rapport d'événements SEOSDATA sur des événements CA Access Control

Pour déterminer si une table SEOSDATA contient des événements CA Access Control et décider de la méthode d'importation, vous devez exécuter un rapport d'événements. Le nom de journal pour les événements CA Access Control est *eTrust Access Control*. Le rapport répertorie tous les événements contenus dans la base de données, séparés par leurs noms de journaux. La méthode la plus simple pour importer des événements CA Access Control consiste à les importer en fonction de leur nom de journal.

Pour créer un rapport d'événements

1. Créez un rapport d'événements pour pouvoir visualiser les événements CA Access Control présents dans la table SEOSDATA.

```
LMSeosImport -dsn Mon_DSN_Audit -user sa -password sa -report
```

Après traitement, l'utilitaire affiche un rapport qui ressemble à ce qui suit.

```
Importation débutée Le Ven Jan  2 15:20:30 2009
```

```
Aucun transport spécifié, SAPI par défaut...
```

```
Préparation des connexions ODBC...
```

```
Liaison réussie à la source [Mon_DSN_Audit]
```

```
----- Période d'événement SEOSDATA -----
```

```
DUREE minimale = 2008-05-27
```

```
DUREE maximale = 2009-01-02
```

```
----- Nombre d'événements par journal -----
```

```
Unix : 12 804
```

```
ACF2 : 1 483
```

```
eTrust AC : 143 762
```

```
com.ca.iTechnology.iSponsor : 66 456
```

```
NT-Application : 5 270
```

```
CISCO PIX Firewall : 5 329
```

```
MS IIS : 6 765
```

```
Netscape : 530
```

```
RACF : 14
```

```
Apache : 401
```

```
S/O : 28 222
```

```
SNMP-recorder : 456
```

```
Check Point FW-1 : 1 057
```

```
EiamSdk : 2 790
```

```
MS ISA : 609
```

```
ORACLE : 2 742
```

```
eTrust PCM : 247
```

```
NT-System : 680
```

```
eTrust Audit : 513
```

```
NT-Security : 14 714
```

```
Unité CISCO : 41 436
```

```
SNORT : 1 089
```

```
----- Plage EntryID SEOSDATA -----
```

```
ENTRYID minimal : 1  
ENTRYID maximal : 10 000 010 243
```

Rapport terminé.

Déconnexion réussie de la source [Mon_DSN_Audit]

Sortie de l'importation...

2. Examinez le rapport pour vérifier la présence des événements provenant de CA Access Control.

La ligne en gras dans cet extrait du rapport indique que la table SEOSDATA contient des événements CA Access Control.

----- Nombre d'événements par journal -----

```
Unix : 12 804  
ACF2 : 1 483  
eTrust AC : 143 762  
com.ca.iTechnology.iSponsor : 66 456  
NT-Application : 5 270  
...
```

Prévisualisation de l'importation d'événements CA Access Control

Vous pouvez utiliser la prévisualisation de l'importation pour affiner le réglage de vos paramètres d'importation. Cet exemple illustre deux passages de prévisualisation, basés sur la nécessité d'importer des événements à partir d'une période spécifique. L'exemple suppose les éléments ci-dessous.

- Le serveur d'outils de données CA Audit se trouve sur un ordinateur Windows.
- Le nom de base de données de la table SEOSDATA est Mon_DSN_Audit.
- Le nom d'utilisateur de la base de données est sa et le mot de passe est également sa.
- La prévisualisation de l'importation utilise uniquement le nom de journal comme critère de recherche et d'importation.

Le résultat de la commande avec l'option `-preview` envoie un échantillon de résultats d'importation à STDOUT (cet exemple utilise la valeur `Mon_serveur_CA-ELM` pour représenter un nom de serveur CA Enterprise Log Manager).

Pour prévisualiser l'importation

1. Prévisualisez votre importation d'événements CA Access Control avec la commande ci-après.

```
LMSeosImport.exe -dsn Mon_DSN_Audit -user sa -password sa -target  
Mon_serveur_CA-ELM -log "eTrust Access Control" -preview
```

La commande -preview affiche les informations ci-dessous.

```
Importation débuté le Ven Jan  2 15:35:37 2009
```

```
Aucun transport spécifié, SAPI par défaut...
```

```
Préparation des connexions ODBC...
```

```
Liaison réussie à la source [Mon_DSN_Audit]
```

```
Aucun ENTRYID de début spécifié, utilisation de l'ENTRYID minimal de 1...
```

```
Importation (prévisualisation) en cours, veuillez patienter...
```

```
.....
```

```
Importation (prévisualisation) terminée (143 762 enregistrements en 4 minutes  
12 secondes).
```

```
----- Événements importés (prévisualisation) par journal -----
```

```
eTrust AC :      143 762
```

```
Dernier EntryId traité : 101 234 500
```

```
Déconnexion réussie de la source [Mon_DSN_Audit]
```

```
Sortie de l'importation...
```

Les résultats de la prévisualisation indiquent un nombre assez important d'événements CA Access Control à importer. Supposons pour cet exemple que vous deviez importer uniquement les événements qui se sont produits au cours d'une période de deux mois. Vous pouvez adapter la commande de prévisualisation pour importer un groupe moins important d'événements en fonction de la date.

2. Modifiez les paramètres d'importation pour inclure une plage de dates, puis exécutez à nouveau la prévisualisation avec la commande ci-dessous.

```
LMSeosImport.exe -dsn Mon_DSN_Audit -user sa -password sa -target  
Mon_serveur_CA-ELM -log "eTrust Access Control" -mintm 2008-11-01 -maxtm  
2009-12-31 -preview
```

La commande modifiée affiche les informations ci-dessous.

```
Importation débuté le Ven Jan  2 15:41:23 2009
```

```
Aucun transport spécifié, SAPI par défaut...
```

```
Préparation des connexions ODBC...
```

```
Liaison réussie à la source [Mon_DSN_Audit]
```

```
Aucun ENTRYID de début spécifié, utilisation de l'ENTRYID minimal de 1...
```

```
Importation (prévisualisation) en cours, veuillez patienter...
```

```
.....
```

```
Importation (prévisualisation) terminée (143 762 enregistrements en 4 minutes  
37 secondes).
```

```
----- Evénements importés (prévisualisation) par journal -----
```

```
eTrust AC :      2 349
```

```
Dernier EntryId traité : 5 167 810 102
```

```
Déconnexion réussie de la source [Mon_DSN_Audit]
```

```
Sortie de l'importation...
```

Cette prévisualisation d'importation indique que la plage de dates crée un sous-ensemble moins important d'événements à importer. Vous pouvez dès lors exécuter la véritable importation.

Informations complémentaires :

[Présentation de la ligne de commande LMSeosImport](#) (page 265)

[Prévisualisation des résultats de l'importation](#) (page 270)

Importation d'événements CA Access Control

Après avoir exécuté le rapport d'événements et une prévisualisation de l'importation, vous êtes prêt à importer les événements CA Access Control à partir de la table SEOSDATA.

Pour importer des événements CA Access Control

Utilisez la commande de la prévisualisation sans l'option -preview pour récupérer les événements CA Access Control de la plage de dates nommée.

```
LMSeosImport.exe -dsn [Mon_DSN_Audit] -user sa -password sa -target [Mon-serveur-CA-ELM] -log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31
```

L'utilitaire affiche les résultats ci-après.

```
Importation débuté le Ven Jan  2 15:41:23 2009
```

```
Aucun transport spécifié, SAPI par défaut...
```

```
Préparation des connexions ODBC...
```

```
Liaison réussie à la source [Mon_DSN_Audit]
```

```
Aucun ENTRYID de début spécifié, utilisation de l'ENTRYID minimal de 1...
```

```
Importation en cours, veuillez patienter...
```

```
.....
```

```
Importation terminée (143 762 enregistrements en 5 minutes 18 secondes).
```

```
----- Evénements importés (prévisualisation) par journal -----
```

```
eTrust AC :      2 241
```

```
Dernier EntryId traité : 5 167 810 102
```

```
Déconnexion réussie de la source [Mon_DSN_Audit]
```

```
Sortie de l'importation...
```

Informations complémentaires :

[Présentation de la ligne de commande LMSeosImport](#) (page 265)

[Importation d'événements provenant d'une base de données de collecteur Windows](#) (page 271)

[Importation d'événements provenant d'une base de données de collecteur Solaris](#) (page 271)

Affichage de requêtes et de rapports sur des événements CA Access Control

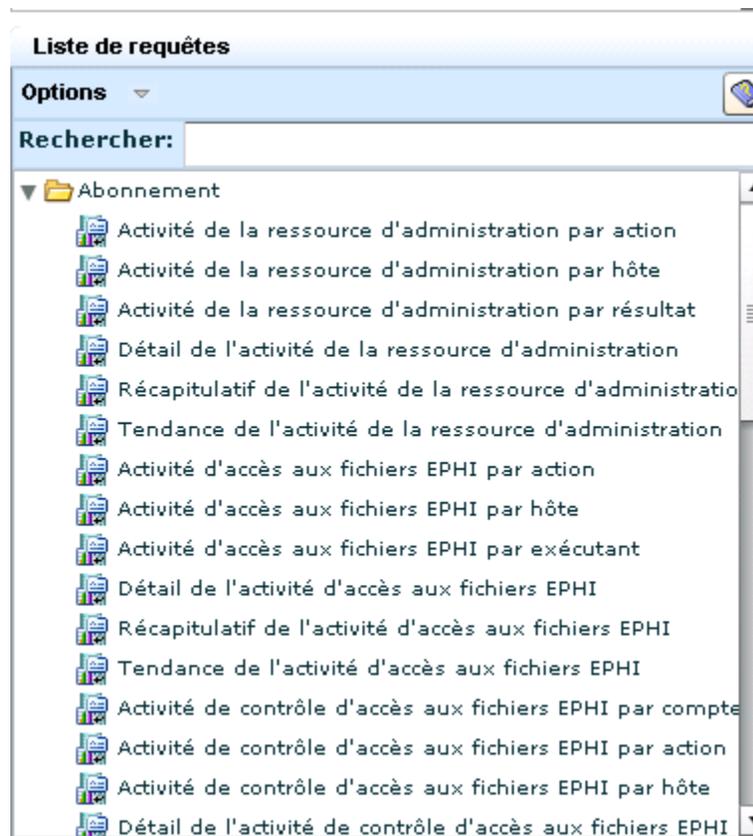
CA Enterprise Log Manager propose un certain nombre de requêtes et de rapports pour examiner les événements collectés à partir de CA Access Control. Suivez la procédure ci-dessous pour accéder aux requêtes et aux rapports CA Access Control.

Pour accéder aux requêtes CA Access Control

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur autorisé à afficher les requêtes et rapports.
2. Dans l'onglet Requêtes et rapports, accédez au sous-onglet Requêtes s'il n'est pas déjà affiché.



3. Cliquez sur la balise de requête CA Access Control pour afficher à gauche la liste des requêtes disponibles.



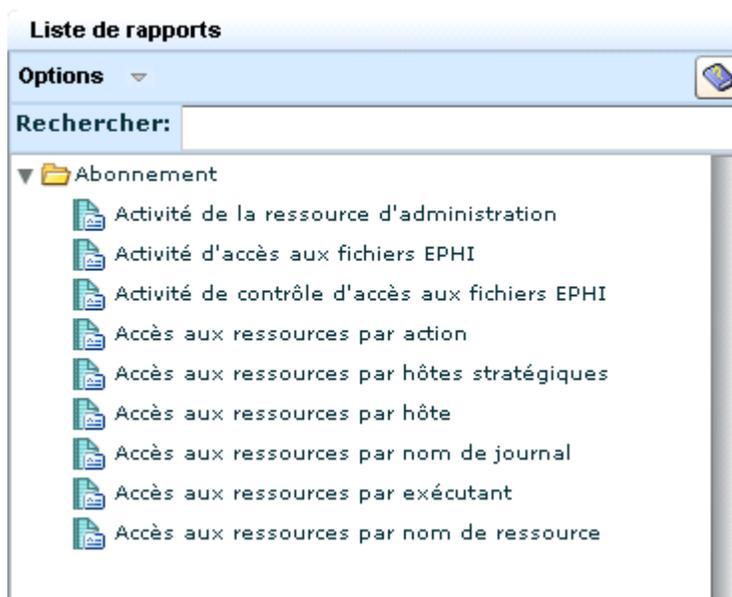
4. Sélectionnez une requête pour afficher les données d'événement.

Pour accéder aux rapports CA Access Control

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur autorisé à afficher les requêtes et rapports.
2. Dans l'onglet Requetes et rapports, accédez au sous-onglet Rapports s'il n'est pas déjà affiché.



3. Cliquez sur la balise de rapport CA Access Control pour afficher à gauche la liste des rapports disponibles.



4. Sélectionnez un rapport pour afficher les données d'événement.

Annexe C : Remarques sur CA IT PAM

Ce chapitre traite des sujets suivants :

[Scénario : Utilisation de CA EEM sur CA Enterprise Log Manager pour l'authentification CA IT PAM](#) (page 300)

[Processus d'implémentation de l'authentification CA IT PAM](#) (page 300)

[Préparation de l'implémentation de l'authentification CA IT sur un CA EEM partagé](#) (page 302)

[Copiez un fichier XML dans le serveur de gestion CA Enterprise Log Manager](#) (page 303)

[Enregistrez CA IT PAM avec un CA EEM partagé](#) (page 303)

[Copie du certificat dans le serveur CA IT PAM](#) (page 305)

[Définition des mots de passe pour les comptes d'utilisateur CA IT PAM prédéfinis](#) (page 305)

[Installation de composants tiers requis par CA IT PAM](#) (page 307)

[Installation du domaine CA IT PAM](#) (page 308)

[Démarrez le service du serveur CA ITPAM.](#) (page 309)

[Lancez la console du serveur CA IT PAM et connectez-vous.](#) (page 310)

Scénario : Utilisation de CA EEM sur CA Enterprise Log Manager pour l'authentification CA IT PAM

Cette annexe présente le scénario d'installation de CA IT PAM sur un serveur Windows et le partage de CA EEM sur le serveur CA Enterprise Log Manager pour l'authentification. Ces procédures complètent celles documentées dans le *Manuel d'installation de CA IT Process Automation*.

Important : Le partage de CA EEM *n'est pas pris en charge en mode FIPS*, car CA IT PAM *n'est pas compatible avec la norme FIPS*. Si vous mettez à niveau votre serveur CA Enterprise Log Manager vers le mode FIPS, l'intégration avec CA IT PAM échouera.

Remarque : Si vous comptez installer CA IT PAM sur un serveur UNIX ou utiliser LDAP ou un CA EEM local pour l'authentification, la documentation de cette annexe ne vous concerne pas. Dans ces instances, vous ne partagez pas le même serveur CA EEM. CA Enterprise Log Manager r12.1 SP1 peut être exécuté en mode FIPS et communiquer avec CA IT PAM, mais ces communications ne sont pas compatibles avec la norme FIPS.

Pour tous les scénarios d'installation, téléchargez le *manuel d'installation* pour CA IT Process Automation Manager r2.1 SP03 à partir du [support en ligne](#). Téléchargez également Adobe Acrobat Reader pour pouvoir ouvrir le fichier pdf.

Le processus qui vous permet d'utiliser CA EEM sur CA Enterprise Log Manager pour l'authentification CA IT PAM implique deux étapes manuelles. Vous copiez un fichier à partir du serveur Windows vers le dispositif et un autre fichier à partir du dispositif vers le serveur Windows. Cette annexe aborde ces étapes. La documentation de CA IT PAM n'aborde pas ces étapes.

Processus d'implémentation de l'authentification CA IT PAM

Le processus d'implémentation de l'authentification CA IT PAM utilisant CA EEM sur le serveur de gestion CA Enterprise Log Manager est le suivant :

1. Préparez l'implémentation de l'authentification CA IT PAM.
 - a. Chargez le module d'installation CA IT PAM sur le serveur Windows dans lequel vous comptez installer CA IT PAM.
 - b. Modifiez le mot de passe par défaut du certificat itpamcert.p12 (facultatif).
2. Copiez le fichier ITPAM_eem.xml à partir de l'hôte où vous comptez installer CA IT PAM vers le dispositif CA Enterprise Log Manager qui inclut CA EEM.

3. Enregistrez ITPAM comme instance d'application sur le même CA EEM qui utilise CA Enterprise Log Manager. L'exécution de la commande safex génère le certificat itpamcert.p12 et l'instance d'application ITPAM avec deux comptes d'utilisateur, itpamadmin et itpamuser.

Remarque : Pour obtenir de l'aide sur l'utilisation de la commande safex, saisissez ./safex.

4. Copiez le fichier itpamcert.p12 à partir du dispositif CA Enterprise Log Manager vers l'hôte Windows sur lequel vous comptez installer le domaine CA IT PAM.
5. Naviguez jusqu'à l'application ITPAM et réinitialisez les mots de passe des comptes itpamadmin et itpamuser.
6. Connectez-vous au serveur Windows et installez les composants tiers en utilisant les procédures décrites dans le *Manuel d'installation de CA IT Process Automation Manager*.
7. Installez le domaine CA IT PAM à l'aide des instructions fournies dans cette annexe et des instructions d'installation de CA IT PAM.
8. Redémarrez le service du serveur CA ITPAM.
9. Lancez la console CA IT PAM et connectez-vous.

Préparation de l'implémentation de l'authentification CA IT sur un CA EEM partagé

Une fois votre package d'installation chargé sur le serveur Windows où vous comptez installer le domaine CA IT PAM, vous pouvez définir un mot de passe pour le certificat itpamcert.cer.

Pour préparer l'implémentation de l'authentification de CA IT PAM sur le serveur de gestion CA Enterprise Log Manager :

1. Décompressez l'image iso CA IT PAM dans l'hôte Windows Server 2003 où vous comptez installer CA IT PAM.

Remarque : L'image .iso de CA IT PAM est disponible sur le CD 2 de la source d'installation de CA IT PAM.

2. Modifiez le mot de passe par défaut du certificat IT PAM (facultatif).
 - a. Accédez au dossier <install path>\eem.
 - b. Ouvrez le fichier ITPAM_eem.xml.
 - c. Remplacez "itpamcertpass" dans la ligne suivante :

```
<Register certfile="itpamcert.p12" password="itpamcertpass"/>
```
 - d. Enregistrez le fichier.

Copiez un fichier XML dans le serveur de gestion CA Enterprise Log Manager

La commande safex génère des objets de sécurité CA IT PAM à partir du fichier ITPAM_eem.xml. Vous devez copier ce fichier dans le dispositif CA Enterprise Log Manager où il sera accessible lors du traitement safex.

Pour copier le fichier ITPAM_eem.xml sur le dispositif CA Enterprise Log Manager :

Copiez le fichier ITPAM_eem.xml situé sur le disque d'installation de CA IT PAM dans le dispositif CA Enterprise Log Manager qui inclut CA EEM. Si vous avez extrait le fichier .iso dans le serveur Windows, utilisez Winscp pour copier ITPAM_eem.xml dans le répertoire /tmp du dispositif.

- Fichier source sur le disque d'installation de CA IT PAM :
ITPAM_eem.xml
- Chemin de destination sur le serveur de gestion CA Enterprise Log Manager :
/opt/CA/SharedComponents/iTechnology

Enregistrez CA IT PAM avec un CA EEM partagé

Vous pouvez enregistrer CA IT PAM avec le CA EEM intégré au serveur de gestion CA Enterprise Log Manager. L'enregistrement auprès d'un CA EEM ajoute des objets de sécurité CA IT PAM.

Les objets de sécurité CA IT PAM ajoutés à CA EEM lors de l'enregistrement sont les suivants :

- L'instance d'application, ITPAM.
- Les stratégies liées à l'accès CA IT PAM
- Les groupes et utilisateurs, notamment les comptes prédéfinis ITPAMAdmins, ITPAMUsers, itpamadmin et itpamuser
- Le certificat, itpamcert.p12

Vous pouvez créer les objets CA IT PAM sur le serveur de gestion CA Enterprise Log Manager. Avant de commencer, obtenez le mot de passe caelmadmin, si vous ne le connaissez pas.

Pour enregistrer CA IT PAM avec CA EEM sur le serveur de gestion CA Enterprise Log Manager :

1. Connectez-vous au dispositif CA Enterprise Log Manager au moyen de ssh en tant qu'utilisateur caelmadmin.

2. Basculez sur le compte d'utilisateur root.

```
su -
```

3. Modifiez les répertoires par le chemin cible et dressez la liste du contenu.

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

4. Vérifiez que les fichiers suivants sont répertoriés :

- ITPAM_eem.xml
- Safex

5. Exécutez la commande ci-dessous.

```
./safex -h <ELM_nomhôte> -u EiamAdmin -p <motdepasse> -f ITPAM_eem.xml
```

Ce processus crée l'application CA IT PAM dans le serveur de gestion CA Enterprise Log Manager, ajoute les utilisateurs par défaut et génère le certificat nécessaire pendant l'installation d'IT PAM. Le certificat est généré avec le mot de passe que vous avez spécifié dans le fichier ITPAM_eem.xml ou s'il n'est pas modifié.

Remarque : Pour obtenir de l'aide sur l'utilisation de la commande safex, saisissez ./safex.

6. Dressez la liste du contenu des répertoires et vérifiez que le certificat itpamcert.cer est présent.

7. Supprimez le fichier XML de configuration CA IT PAM. Cela est conseillé pour des raisons de sécurité.

```
rm ITPAM_eem.xml
```

Copie du certificat dans le serveur CA IT PAM

Quand vous avez exécuté la commande safex dans CA Enterprise Log Manager pour enregistrer CA IT PAM avec son CA EEM, ce processus a généré le certificat itpamcert.p12. Vous devez copier ce certificat sur le serveur Windows où vous comptez installer le domaine CA IT PAM. Lors de l'installation du domaine CA IT PAM, accédez à ce fichier de certificat.

Pour copier le certificat à partir du dispositif CA Enterprise Log Manager vers le serveur Windows cible :

Copiez le fichier itpamcert.p12 à partir du dispositif CA Enterprise Log Manager qui inclut CA EEM vers l'hôte où vous comptez installer CA IT PAM.

- Fichier source sur le serveur de gestion CA Enterprise Log Manager :

`/opt/CA/SharedComponents/iTechnology/itpamcert.log`

- Chemin d'accès de la destination sur le serveur >Windows cible :

`<chemin_installation>`

Remarque : Vous pouvez copier ce fichier dans l'emplacement de votre choix. Vous sélectionnez ce fichier dans son emplacement lors de l'installation du domaine CA IT PAM.

Définition des mots de passe pour les comptes d'utilisateur CA IT PAM prédéfinis

L'exécution de la commande safex crée les éléments suivants :

- Des groupes de sécurité IT PAM :
 - ITPAMAdmins
 - ITPAMUsers
- Utilisateurs IT PAM
 - itpamadmin avec un mot de passe par défaut
 - itpamuser avec un mot de passe par défaut

Vous devez réinitialiser le mot de passe pour les deux utilisateurs IT PAM prédéfinis.

Pour réinitialiser les mots de passe des comptes itpamadmin et itpamuser dans l'application IT PAM sur CA EEM :

1. Accédez à l'URL du serveur sur lequel le CA EEM utilisé par CA Enterprise Log Manager est installé, par exemple, le serveur de gestion de CA Enterprise Log Manager :

`https://<serveur_gestion_ELM_management>5250/spin/eiam`

L'écran d'accès CA EEM s'affiche. La liste déroulante de l'application inclut <Global>, CAELM et ITPAM.
2. Connectez-vous à l'application IT PAM.
 - a. Sélectionnez ITPAM comme application.
 - b. Saisissez EiamAdmin comme nom d'utilisateur.
 - c. Saisissez le mot de passe du compte d'utilisateur EiamAdmin.
 - d. Cliquez sur Connexion.
3. Cliquez sur l'onglet Gérer identités.
4. Dans la boîte de dialogue Rechercher des utilisateurs, saisissez itpam pour la Valeur et cliquez sur OK.

Les utilisateurs suivants apparaissent dans la liste
 - itpamadmin
 - itpamuser
5. Réinitialisez le mot de passe du compte itpamadmin :
 - a. Sélectionnez itpamadmin dans la liste et accédez à Authentification dans le panneau de droite.
 - b. Sélectionnez Réinitialiser le mot de passe.
 - c. Saisissez le mot de passe de ce compte dans les champs Nouveau mot de passe et Confirmer le mot de passe.
 - d. Cliquez sur Enregistrer.

6. Réinitialisez le mot de passe du compte itpamuser :
 - a. Sélectionnez itpamuser dans la liste et accédez à Authentification dans le panneau de droite.
 - b. Sélectionnez Réinitialiser le mot de passe.
 - c. Saisissez le mot de passe de ce compte dans les champs Nouveau mot de passe et Confirmer le mot de passe.
 - d. Cliquez sur Enregistrer.
7. Cliquez sur Déconnexion.

Installation de composants tiers requis par CA IT PAM

JDK 1.6 ou une version ultérieure doit être installée sur votre système avant d'installer les composants tiers. Exécutez `Third_Party_Installer_windows.exe` sur le serveur Windows où vous comptez installer CA IT PAM. Consultez le *manuel d'installation de CA IT Process Automation Manager* pour de plus amples détails.

Installation du domaine CA IT PAM

L'exécution de l'assistant CA IT PAM avec les spécifications décrites ici relie le certificat de sorte que CA IT PAM et CA EEM soient sécurisés sur le serveur de gestion CA Enterprise Log Manager.

Conservez à votre disposition les informations ci-dessous.

- Le mot de passe du fichier du certificat EEM, itpamcert.p12. Il se peut que vous ayez modifié la valeur par défaut dans le fichier ITPAM_eem.xml pendant l'étape, Préparation de l'implémentation de l'authentification CA IT PAM sur un CA EEM partagé.
- Le nom d'hôte du serveur de gestion CA Enterprise Log Manager. Il s'agit du serveur auquel vous vous êtes connecté pour l'étape, Enregistrement de CA IT PAM avec un CA EEM partagé.
- Le mot de passe itpamadmin défini pendant l'étape Définition des mots de passe pour les comptes d'utilisateurs CA IT PAM prédéfinis.
- Le mot de passe du certificat utilisé pour contrôler l'accès aux clés utilisées pour chiffrer les mots de passe. Il s'agit d'un nouveau paramètre qui n'existait pas auparavant.

Pour obtenir des instructions sur l'installation du domaine CA IT PAM, voir le *manuel d'installation de CA IT Process Automation Manager* qui est fourni avec le logiciel. Utilisez la procédure suivante pour obtenir des instructions sur la configuration des paramètres de sécurité EEM.

Pour installer le domaine CA IT PAM :

1. Si l'assistant d'installation IT PAM n'est pas lancé suite à l'installation de composants tiers, lancez CA_ITPAM_Domain_windows.exe.
2. Suivez les instructions fournies dans votre documentation CA IT PAM, jusqu'à ce que vous sélectionniez le type de serveur de sécurité.
3. Quand la boîte de dialogue Select Security Server Type (Sélection du type de serveur de sécurité) s'affiche, sélectionnez EEM comme serveur de sécurité et cliquez sur Suivant.

La page Paramètres de sécurité EEM s'affiche.

4. Complétez les paramètres de sécurité EEM comme suit :
 - a. Saisissez le nom d'hôte du serveur de gestion CA Enterprise Log Manager dans le champ du serveur EEM.
 - b. Saisissez ITPAM dans le champ de l'application EEM.
 - c. Cliquez sur Parcourir et accédez au dossier contenant le fichier itpamcert.p12.
 - d. Sélectionnez le fichier itpamcert.p12.
 - e. Renseignez le champ du mot de passe du certificat EEM de l'une des façons suivantes :
 - Saisissez le mot de passe que vous avez remplacé dans le fichier ITPAM_eem.xml lors de l'étape de préparation.
 - Saisissez itpamcertpass, le mot de passe par défaut.
5. Cliquez sur Test EEM Settings (Tester les paramètres EEM).

Le message suivant s'affiche : "Performing a test...may take a few minutes" (Test en cours... Cela peut prendre quelques minutes).
6. Cliquez sur OK.

La boîte de dialogue Verify EEM settings (Vérifier les paramètres EEM) s'affiche :
7. Saisissez itpamadmin comme nom d'utilisateur. Saisissez le mot de passe que vous avez défini pour le compte d'utilisateur itpamadmin, puis cliquez sur OK.
8. Cliquez sur Suivant. Suivez les instructions IT PAM fournies pour compléter le reste de l'assistant.

Démarrez le service du serveur CA ITPAM.

Démarrez le service du serveur CA ITPAM de sorte que vous-même et d'autres utilisateurs puissiez lancer le serveur CA IT PAM.

Pour démarrer le service du serveur CA ITPAM :

1. Connectez-vous au serveur Windows où le domaine CA IT PAM est installé.
2. Dans le menu Démarrer, sélectionnez Programmes, Domaine ITPAM, Démarrer le service du serveur.

Remarque : Si cette option de menu ne s'affiche pas, sélectionnez Outils d'administration, Services de composants. Cliquez sur Services, Serveur CA IT PAM, puis sur Démarrer le service.

Lancez la console du serveur CA IT PAM et connectez-vous.

Vous pouvez lancer le serveur CA IT PAM à partir d'un navigateur sur n'importe quel système où l'API Java JRE 1.6 ou JDK 1.6 est installée et intégrée.

Pour lancer la console de gestion CA IT PAM :

1. Saisissez l'URL suivante dans la barre d'adresse d'un navigateur :
`http://<nomhôte_serveur_itpam>:8080/itpam/`
L'écran de connexion de l'application CA IT Process Automation Manager s'affiche.
2. Saisissez `itpamadmin` dans le champ Connexion de l'utilisateur.
3. Saisissez le mot de passe attribué à ce compte dans le champ Mot de passe.
4. Cliquez sur Connexion.

Le serveur CA EEM sur le dispositif CA Enterprise Log Manager authentifie vos informations de connexion et ouvre CA IT Process Automation Manager.

Pour plus de détails sur l'intégration et l'utilisation de CA IT PAM avec CA Enterprise Log Manager, voir la section "Utilisation des processus de l'événement/de sortie CA IT PAM" du chapitre Alertes d'action dans le *manuel d'administration CA Enterprise Log Manager*.

Annexe D : Récupération après sinistre

Ce chapitre traite des sujets suivants :

[Planification de la récupération après sinistre](#) (page 311)

[A propos de la sauvegarde du serveur CA EEM](#) (page 312)

[Sauvegarde d'une instance d'application CA EEM](#) (page 313)

[Restauration d'un serveur CA EEM pour l'utiliser avec CA Enterprise Log Manager](#) (page 314)

[Sauvegarde d'un serveur CA Enterprise Log Manager](#) (page 315)

[Restauration d'un serveur CA Enterprise Log Manager à partir des fichiers de sauvegarde](#) (page 315)

[Restauration d'un serveur CA Enterprise Log Manager suite à une mise à jour d'abonnement](#) (page 317)

[Remplacement d'un serveur CA Enterprise Log Manager](#) (page 317)

Planification de la récupération après sinistre

La planification de la récupération après sinistre fait partie intégrante de tout bon plan d'administration réseau. La planification de la récupération après sinistre CA Enterprise Log Manager est relativement simple et directe. La réussite de la récupération après sinistre pour CA Enterprise Log Manager repose sur la conservation de sauvegardes régulières.

Vous devez effectuer les sauvegardes des informations ci-dessous.

- Instance d'application CA Enterprise Log Manager sur le serveur de gestion
- Dossier `/opt/CA/LogManager/data` sur chaque serveur CA Enterprise Log Manager
- Fichiers de certificat dans le dossier `/opt/CA/SharedComponents/iTechnology` sur chaque serveur CA Enterprise Log Manager

Si votre implémentation repose sur la conservation de niveaux élevés de débit, vous pouvez choisir de disposer d'un serveur de réserve, doté des mêmes caractéristiques matérielles que celui sur lequel vous installez vos autres serveurs CA Enterprise Log Manager. Si un serveur CA Enterprise Log Manager est désactivé, vous pouvez installer un autre serveur en utilisant exactement le même nom. Lorsque le nouveau serveur démarre, il reçoit les fichiers de configuration nécessaires de la part du serveur de gestion. Si ce niveau de performances n'est pas critique pour votre implémentation, vous pouvez installer un serveur CA Enterprise Log Manager sur n'importe quel serveur vide, capable d'héberger le système d'exploitation de base et répondant aux exigences minimales de mémoire et de disque dur.

Vous trouverez plus d'informations sur les exigences matérielles et logicielles dans les *Notes de parution CA Enterprise Log Manager*.

Le serveur CA EEM interne, installé sur le serveur de gestion, dispose également de ses processus de configuration du basculement pour assurer la continuité du fonctionnement, processus évoqués en détail dans le *Manuel de mise en oeuvre de CA EEM*.

A propos de la sauvegarde du serveur CA EEM

La configuration de chaque serveur, agent et connecteur CA Enterprise Log Manager, tout comme celle des requêtes, rapports, alertes, etc., est conservée séparément dans le référentiel CA EEM du serveur CA Enterprise Log Manager de gestion. Pour effectuer une récupération correcte du serveur, il est essentiel de conserver des sauvegardes régulières des informations stockées dans l'instance d'application CA Enterprise Log Manager.

Une *instance d'application* est un espace commun dans le référentiel CA EEM, où sont stockées les informations ci-après.

- Utilisateurs, groupes et stratégies d'accès
- Agent, intégration, écouteur, connecteur et configurations enregistrées
- Requêtes, rapports et règles de suppression et de récapitulation personnalisés
- Relations de fédération
- Informations de gestion du code binaire
- Clés de chiffrement

Vous pouvez effectuer la procédure de sauvegarde de CA EEM depuis l'interface du navigateur Web CA EEM. En général, tous les serveurs CA Enterprise Log Manager d'une entreprise utilisent la même instance d'application. La valeur de l'instance d'application CA Enterprise Log Manager par défaut est CAELM. Vous pouvez installer des serveurs CA Enterprise Log Manager avec différentes instances d'application, mais vous pouvez uniquement fédérer les serveurs partageant la même instance d'application. Les serveurs configurés pour utiliser le même serveur CA EEM avec différentes instances d'application partagent uniquement le magasin d'utilisateurs, les stratégies de mots de passe et les groupes globaux.

Le *Manuel de mise en oeuvre de CA EEM* contient plus d'informations sur les opérations de sauvegarde et de restauration.

Sauvegarde d'une instance d'application CA EEM

Vous pouvez effectuer une sauvegarde d'une instance d'application CA Enterprise Log Manager depuis le serveur CA EEM interne, sur le serveur de gestion.

Pour sauvegarder une instance d'application

1. Accédez au serveur CA EEM à l'aide de l'URL ci-dessous.
`https://<nom_serveur>:5250/spin/eiam`
2. Dans la page de connexion, développez la liste Application et sélectionnez le nom de l'instance d'application utilisé lors de l'installation de vos serveurs CA Enterprise Log Manager.

Le nom d'instance d'application par défaut pour CA Enterprise Log Manager est CAELM.
3. Connectez-vous en tant qu'utilisateur EiamAdmin ou en tant qu'utilisateur doté du rôle Administrator de CA EEM.
4. Accédez à l'onglet Configuration et sélectionnez le sous-onglet Serveur EEM.
5. Sélectionnez l'élément Exporter l'application dans le volet de navigation, sur la gauche.
6. Sélectionnez toutes les options, à l'exception de la case à cocher Remplacer la taille maximale de la recherche.

Remarque : Si vous utilisez un répertoire externe, ne sélectionnez pas les options Utilisateurs Globaux, Groupes globaux et Dossiers globaux.

7. Cliquez sur Exporter pour créer un fichier d'exportation XML pour l'instance d'application.

La boîte de dialogue Téléchargement de fichier affiche le nom du fichier, `<Nom_Instance_App>.xml.gz` (par exemple, `CAELM.xml.gz`), et un bouton Enregistrer.

8. Cliquez sur Enregistrer et sélectionnez votre emplacement de sauvegarde sur un serveur distant mappé. Vous pouvez également enregistrer le fichier en local, puis le copier ou le déplacer vers votre emplacement de sauvegarde sur un autre serveur.

Restauration d'un serveur CA EEM pour l'utiliser avec CA Enterprise Log Manager

Vous pouvez restaurer une instance d'application CA Enterprise Log Manager vers un serveur de gestion. La restauration de la fonctionnalité CA EEM du serveur de gestion implique l'exécution de l'utilitaire `safex`, qui importe l'instance d'application sauvegardée.

Pour restaurer la fonctionnalité CA EEM du serveur de gestion à partir d'une sauvegarde

1. Installez le dispositif logiciel CA Enterprise Log Manager sur un nouveau serveur matériel.
2. Accédez à une invite de commande et recherchez le répertoire `/opt/CA/LogManager/EEM`.
3. Copiez le fichier de sauvegarde `<Nom_Instance_App>.xml.gz` provenant de votre serveur de sauvegarde externe vers ce répertoire.
4. Exécutez la commande ci-dessous pour récupérer le fichier d'exportation XML.

```
gunzip <Nom_Instance_App>.xml.gz
```

5. Exécutez la commande ci-dessous pour restaurer le fichier d'exportation sur le nouveau serveur de gestion.

```
./safex -h nom_hôte_serveur_eem -u EiamAdmin -p mot_passe -f  
Nom_Instance_App.xml
```

Si le mode d'exécution choisi est FIPS, assurez-vous d'inclure l'option `-fips`.

6. Accédez au répertoire `/opt/CA/ELMAgent/bin`.
7. Remplacez le fichier par défaut `AgentCert.cer` par le fichier sauvegardé, `CAELM_AgentCert.cer`, pour garantir le bon démarrage de l'agent.

Sauvegarde d'un serveur CA Enterprise Log Manager

Vous pouvez sauvegarder l'ensemble d'un serveur CA Enterprise Log Manager à partir du dossier `/opt/CA/LogManager/data`. Ce dossier de données est un lien symbolique vers le dossier de données du répertoire racine (`/data`).

Pour sauvegarder un serveur CA Enterprise Log Manager

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur `caelmadmin`.
2. Accédez au compte `root` à l'aide de l'utilitaire `su`.
3. Accédez au répertoire `/opt/CA/LogManager`.
4. Exécutez la commande TAR ci-dessous pour créer une copie de sauvegarde des fichiers du serveur CA Enterprise Log Manager.

```
tar -hcvf backupData.tgz /data
```

Cette commande crée le fichier de sortie compressé `backupData.tgz` à l'aide des fichiers du répertoire `/data`.

5. Accédez au répertoire `/opt/CA/SharedComponents/iTechnology`.
6. Exécutez la commande TAR ci-dessous pour créer une copie de sauvegarde des certificats numériques (tous les fichiers ayant une extension `.cer`).

```
tar -zcvf backupCerts.tgz *.cer
```

Cette commande crée le fichier de sortie compressé `backupCerts.tgz`.

```
tar -hcvf backupCerts.tgz /data
```

Restauration d'un serveur CA Enterprise Log Manager à partir des fichiers de sauvegarde

Vous pouvez restaurer un serveur CA Enterprise Log Manager à partir des fichiers de sauvegarde après avoir installé le dispositif logiciel CA Enterprise Log Manager sur le nouveau serveur.

Pour restaurer un serveur CA Enterprise Log Manager à partir des sauvegardes

1. Arrêtez le processus `iGateway` sur le nouveau serveur.

Pour ce faire, accédez au dossier `/opt/CA/SharedComponents/iTechnology` et exécutez la commande ci-dessous.

```
./S99gateway stop
```

2. Copiez les fichiers backupData.tgz et backupCerts.tgz files dans le répertoire /opt/CA/LogManager sur le nouveau serveur.
3. Développez le contenu du fichier backupData.tgz à l'aide de la commande ci-dessous.

```
tar -xzvf backupData.tgz
```

Cette commande remplace le contenu du dossier de données par le contenu du fichier de sauvegarde.

4. Accédez au répertoire /opt/CA/SharedComponents/iTechnology.
5. Développez le contenu du fichier backupCerts.tgz file à l'aide de la commande ci-dessous.

```
tar -xzvf backupCerts.tgz
```

Cette commande remplace les fichiers de certificats (.p12) du dossier actuel par les fichiers de certificats du fichier de sauvegarde.

6. Démarrez le processus iGateway.

Pour ce faire, exécutez la commande ci-dessous.

```
./S99gateway start
```

Restauration d'un serveur CA Enterprise Log Manager suite à une mise à jour d'abonnement

Vous pouvez restaurer un serveur CA Enterprise Log Manager après l'échec d'une mise à jour d'abonnement ou dans le cas d'une mise à jour non nécessaire pour quelque raison que ce soit. Lors de chaque téléchargement d'abonnement, des fichiers de sauvegarde sont créés avec la date de la sauvegarde. Cette procédure permet de restaurer uniquement le serveur de gestionnaire de journaux même, mais pas les autres composants, comme EEM.

Pour restaurer un serveur suite à une mise à jour d'abonnement :

1. Arrêtez le processus iGateway sur le nouveau serveur.

Pour ce faire, accédez au dossier `/opt/CA/SharedComponents/iTechnology` et exécutez la commande ci-dessous.

```
./S99igateway stop
```

2. Accédez au répertoire `/opt/CA/SharedComponents/iTechnology`.
3. Entrez la commande suivante :

```
sh ./restore.sh <backupdate> <backupversion>
```

Exemple :

```
sh ./restore.sh 22-Sep-2010 12.0.45.10
```

4. Accédez au répertoire `/opt/CA/SharedComponents/iTechnology`.
5. Démarrez le processus iGateway.

Pour ce faire, exécutez la commande ci-dessous.

```
./S99igateway start
```

Remplacement d'un serveur CA Enterprise Log Manager

Utilisez la procédure suivante pour remplacer un serveur CA Enterprise Log Manager de collecte après un sinistre ou une panne de grande ampleur. Cette procédure permet la récupération après un sinistre en créant un nouveau serveur CA Enterprise Log Manager pour reprendre la collecte d'événements à la place du serveur en échec.

Remarque : Cette procédure ne récupère pas les données d'événement qui se trouvent dans le magasin de journaux d'événements du serveur en échec. Utilisez les techniques classiques de récupération des données pour récupérer les données d'événement dans le magasin de journaux d'événements du serveur défaillant.

Pour effectuer une récupération à partir d'un serveur CA Enterprise Log Manager désactivé

1. Installez le dispositif logiciel CA Enterprise Log Manager sur un autre serveur, en utilisant le nom d'hôte affecté au serveur défaillant.

Lorsque l'installation demande le nom de l'instance d'application CA EEM, assurez-vous d'utiliser la même instance d'application que celle utilisée par l'ancien serveur. Cet enregistrement réussi permet au serveur CA EEM de synchroniser la configuration.

2. Démarrez le nouveau serveur CA Enterprise Log Manager et connectez-vous en tant qu'utilisateur d'administration par défaut, EiamAdmin.

Lorsque le nouveau serveur CA Enterprise Log Manager démarre, il se connecte automatiquement au serveur CA EEM, qui télécharge ensuite les fichiers de configuration. Après avoir reçu les fichiers de configuration, le nouveau serveur CA Enterprise Log Manager reprend la collecte de journaux.

Annexe E : CA Enterprise Log Manager et virtualisation

Ce chapitre traite des sujets suivants :

[Hypothèses de déploiement](#) (page 319)

[Création de serveurs CA Enterprise Log Manager à l'aide d'ordinateurs virtuels](#) (page 320)

[Création de serveurs CA Enterprise Log Manager à l'aide d'ordinateurs virtuels](#) (page 336)

Hypothèses de déploiement

L'utilisation de CA Enterprise Log Manager dans un environnement virtuel, ou dans un environnement mixte incluant des serveurs virtuels et de dispositifs, suppose les éléments ci-après.

- Dans un environnement totalement virtuel, installez au moins un serveur CA Enterprise Log Manager en tant que serveur de gestion. Celui-ci a pour rôle de gérer les configurations, les contenus des abonnements et les contenus définis par l'utilisateur, et de communiquer avec les agents. Ce serveur ne reçoit pas les journaux d'événements et ne gère pas les requêtes et les rapports.
- Dans un environnement mixte, installez le serveur CA Enterprise Log Manager de gestion sur un matériel certifié.
- Chaque hôte d'ordinateur virtuel compte quatre processeurs dédiés, nombre maximal autorisé par VMware ESX Server 3.5.

Remarques

Un serveur CA Enterprise Log Manager dédié affiche des performances optimales avec huit processeurs au minimum. VMware ESX Server autorise quatre processeurs au maximum pour un seul ordinateur virtuel. Pour obtenir des performances similaires à un serveur dédié affichant huit processeurs, installez CA Enterprise Log Manager sur plusieurs ordinateurs virtuels, puis fédérez-les pour générer des rapports consolidés.

Deux serveurs CA Enterprise Log Manager fonctionnant comme des invités sous VMware ESX Server v3.5 se rapprochent de la capacité d'un seul serveur CA Enterprise Log Manager dédié. Utilisez le tableau suivant pour planifier votre réseau virtuel.

Rôle du serveur CA Enterprise Log Manager	Nombre de processeurs (minimum)	Vitesse de l'UC en GHz (par UC)	Mémoire totale en Go (Configuration minimale requise)
Gestion	8	3	8
Génération de rapport	8	3	8
Collecte	4	3	8

Remarque : Le nombre maximum d'événements par seconde est de 1 K dans une configuration de déploiement moyenne et de 5 K dans une configuration de déploiement importante.

Création de serveurs CA Enterprise Log Manager à l'aide d'ordinateurs virtuels

Vous pouvez créer des serveurs CA Enterprise Log Manager virtuels pour votre environnement de collecte de journaux d'événements à l'aide des scénarios ci-dessous.

- Ajout de serveurs virtuels à un environnement CA Enterprise Log Manager existant : création d'un environnement mixte
- Création d'un environnement virtuel de collecte de journaux
- Clonage et déploiement de serveurs CA Enterprise Log Manager virtuels pour une évolutivité rapide de l'environnement
- Création de serveurs CA Enterprise Log Manager à l'aide d'ordinateurs virtuels

Informations complémentaires :

[Ajout de serveurs virtuels à votre environnement](#) (page 341)

[Création d'un environnement complètement virtuel](#) (page 365)

[Déploiement rapide de serveurs virtuels](#) (page 391)

Ajout de serveurs virtuels à votre environnement

Si vous disposez déjà d'une implémentation CA Enterprise Log Manager, vous pouvez ajouter des serveurs de collecte CA Enterprise Log Manager virtuels pour gérer un volume d'événements accru sur votre réseau. Ce scénario suppose que vous avez déjà installé un serveur de gestion CA Enterprise Log Manager et un ou plusieurs serveurs CA Enterprise Log Manager pour la collecte et la génération de rapports.

Remarque : Pour obtenir les meilleures performances possibles, installez CA Enterprise Log Manager sur des serveurs virtuels pour gérer uniquement les tâches de collecte et de génération de rapports.

Le processus d'ajout de serveurs de collecte virtuels à votre environnement inclut les procédures ci-dessous.

1. Créez un nouvel ordinateur virtuel.
2. Ajoutez des lecteurs de disques virtuels.
3. Installez CA Enterprise Log Manager sur l'ordinateur virtuel.
4. Configurez le serveur CA Enterprise Log Manager en vous référant à la section traitant de l'installation.

Après avoir installé le serveur de collecte virtuel, vous pouvez l'ajouter à votre fédération pour effectuer des requêtes et des rapports.

Création d'un nouvel ordinateur virtuel

Utilisez la procédure suivante pour créer un nouvel ordinateur à l'aide du client VMware Infrastructure. Utilisez quatre processeurs pour chaque serveur CA Enterprise Log Manager virtuel afin d'obtenir des performances acceptables.

Pour créer un nouvel ordinateur virtuel

1. Accédez au client VMware Infrastructure.
2. Cliquez avec le bouton droit sur l'hôte ESX dans le volet gauche, puis sélectionnez **Nouvel ordinateur virtuel** pour appeler l'assistant de création d'un ordinateur virtuel. Cette action affiche une boîte de dialogue de type de configuration.
3. Sélectionnez la configuration **Personnalisée** et cliquez sur **Suivant**. Une boîte de dialogue de nom et d'emplacement s'affiche.

4. Entrez un nom pour le serveur CA Enterprise Log Manager à installer sur cet ordinateur virtuel et cliquez sur Suivant.
5. Spécifiez les paramètres de stockage pour votre ordinateur virtuel, puis cliquez sur Suivant.

Vérifiez que vos paramètres de stockage sont suffisamment importants pour votre serveur CA Enterprise Log Manager. Nous recommandons un espace minimal de 500 Go.

Remarque : La configuration de lecteurs de disques virtuels supplémentaires pour stocker les journaux d'événements collectés fait l'objet d'une autre procédure.

6. Sélectionnez Red Hat Enterprise Linux 5 (32 bits) comme Système d'exploitation invité et cliquez sur Suivant.
7. Sélectionnez 4 comme nombre de processeurs virtuels dans la liste déroulante Nombre de processeurs virtuels.

Votre serveur hôte physique doit être capable de consacrer quatre UC physiques *exclusivement* à cette instance CA Enterprise Log Manager. Cliquez sur Suivant.
8. Configurez la taille de la mémoire de l'ordinateur virtuel et cliquez sur Suivant. La taille *minimale* acceptable de la mémoire pour CA Enterprise Log Manager est 8 Go ou 8 192 Mo.
9. Configurez votre contrôleur d'interface réseau (NIC). CA Enterprise Log Manager nécessite au moins une connexion réseau. Sélectionnez NIC x dans la liste de NIC disponibles et paramétrez la valeur Adaptateur sur Flexible.

Remarque : Vous n'avez pas besoin de configurer un NIC séparé pour chaque serveur CA Enterprise Log Manager hébergé sur ce serveur physique. Toutefois, vous devez allouer et affecter une adresse IP statique à chaque serveur.

10. Sélectionnez l'option Connecter au démarrage et cliquez sur Suivant. La boîte de dialogue Types d'adaptateurs E/S s'affiche.
11. Select LSI Logic pour l'adaptateur E/S, puis cliquez sur Suivant. La boîte de dialogue Sélectionner un disque s'affiche.
12. Sélectionnez l'option Créer un nouveau disque virtuel, puis cliquez sur Suivant. La boîte de dialogue concernant la capacité et l'emplacement du disque s'affiche.

13. Précisez la capacité et l'emplacement de votre disque, puis cliquez sur Suivant. Une boîte de dialogue d'options avancées s'affiche.

Vous pouvez stocker ce disque avec votre ordinateur virtuel ou spécifier un autre emplacement. Nous recommandons un espace minimal de 500 Go.

14. Acceptez les valeurs par défaut des options avancées et cliquez sur Suivant.
15. Confirmez vos paramètres et cliquez sur Terminer pour créer le nouvel ordinateur virtuel.

Ajout de lecteurs de disques virtuels

Utilisez la procédure suivante afin d'ajouter des lecteurs de disques virtuels pour le stockage de journaux d'événements. Utilisez les mêmes paramètres, sans tenir compte du rôle joué par un serveur CA Enterprise Log Manager spécifique sur votre réseau.

Pour modifier les paramètres

1. Cliquez avec le bouton droit sur votre ordinateur virtuel dans le client VMware Infrastructure et sélectionnez Modifier les paramètres.
La boîte de dialogue Propriétés de l'ordinateur virtuel s'affiche.
2. Mettez en surbrillance les propriétés du lecteur de CD/DVD 1.
3. Cliquez sur le bouton d'option Unité hôte et sélectionnez votre lecteur de DVD-ROM dans la liste déroulante.
4. Sélectionnez l'option Etat de l'unité, Connecter au démarrage.
5. Cliquez sur Ajouter pour lancer l'assistant d'ajout de matériel et ajouter un deuxième disque dur.
6. Mettez le disque dur en surbrillance dans la liste des unités et cliquez sur Suivant. La boîte de dialogue Sélectionner un disque s'affiche.
7. Sélectionnez l'option Créer un nouveau disque virtuel et cliquez sur Suivant.

8. Spécifiez la taille de votre nouveau disque et sélectionnez l'option Spécifier un magasin de données pour paramétrer son emplacement.

CA Enterprise Log Manager détecte ce lecteur supplémentaire au cours de l'installation et l'affecte au magasin de données. Nous vous recommandons d'optimiser l'espace de stockage que vous pouvez mettre à disposition de CA Enterprise Log Manager.

Remarque : Le paramètre de taille de bloc par défaut du serveur VMware ESX Server est 1 Mo, ce qui limite à 256 Go l'espace disque maximal que vous pouvez créer. Si vous avez besoin d'espace supplémentaire, jusqu'à 512 Go, augmentez le paramètre de taille de bloc à 2 Mo grâce à la commande ci-dessous.

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

Redémarrez l'instance ESX Server pour que les changements entrent en vigueur. Pour plus d'informations sur cette commande et sur d'autres commandes, consultez la documentation VMware ESX Server.

Cliquez sur Suivant pour afficher la boîte de dialogue Spécifier les options avancées.

9. Acceptez les valeurs par défaut des options avancées et cliquez sur Suivant. La boîte de dialogue Prêt à terminer s'affiche.
10. Cliquez sur Terminer pour stocker vos modifications sur cet ordinateur virtuel. Cette action vous renvoie à la boîte de dialogue du client VMware Infrastructure.

Installation de CA Enterprise Log Manager sur l'ordinateur virtuel

Utilisez la procédure suivante pour installer CA Enterprise Log Manager sur un ordinateur virtuel précédemment créé.

Vous pouvez configurer un serveur CA Enterprise Log Manager virtuel ou dédié après l'installation pour qu'il affiche l'un des nombreux rôles fonctionnels, tels que la gestion, la collecte ou la génération de rapports. Si vous installez un serveur de gestion CA Enterprise Log Manager, ne l'utilisez pas pour recevoir des journaux d'événements ou pour exécuter des requêtes et des rapports. Installez des serveurs CA Enterprise Log Manager virtuels distincts pour faire office de serveurs de rapports et de collecte, afin d'obtenir les meilleures performances possibles.

Examinez les instructions d'installation normale avant d'installer CA Enterprise Log Manager dans un environnement virtuel. La feuille de calcul d'installation vous permet de collecter les informations nécessaires.

Pour installer CA Enterprise Log Manager sur un ordinateur virtuel

1. Chargez votre disque d'installation du SE CA Enterprise Log Manager dans le lecteur physique de DVD-ROM ou recherchez le répertoire dans lequel vous avez copié l'image de l'installation.
2. Mettez votre ordinateur virtuel en surbrillance dans la liste d'inventaire des ordinateurs virtuels, cliquez dessus avec le bouton droit et sélectionnez Démarrage.
3. Poursuivez l'installation normale de CA Enterprise Log Manager.
4. Configurez le serveur CA Enterprise Log Manager installé pour le rôle fonctionnel souhaité, en utilisant les informations de la section traitant de l'installation d'un serveur CA Enterprise Log Manager.

Informations complémentaires :

[Installation de CA Enterprise Log Manager](#) (page 83)

Création d'un environnement complètement virtuel

Si vous n'avez pas encore implémenté un environnement CA Enterprise Log Manager, vous pouvez créer un environnement entièrement virtuel de collecte de journaux. Ce scénario suppose de disposer d'un nombre suffisant de serveurs physiques disponibles, tous dotés d'un groupe de quatre processeurs au minimum, pour installer chacun des serveurs CA Enterprise Log Manager souhaités.

Installez un serveur CA Enterprise Log Manager comme serveur de gestion. Lors de la configuration, n'envoyez pas les journaux d'événements à ce serveur et ne l'utilisez pas pour générer des rapports. En configurant ainsi votre environnement, vous conservez le débit de collecte des journaux d'événements requis par la production d'une entreprise.

En général, vous installez deux serveurs CA Enterprise Log Manager dotés de quatre processeurs en lieu et place de chacun des serveurs de dispositifs normalement installés en cas d'utilisation de matériel certifié (les serveurs de dispositifs comptent huit processeurs au minimum).

Le processus que vous suivez pour créer un environnement virtuel comprend les procédures ci-après.

1. Créez un nouvel ordinateur virtuel pour chaque serveur CA Enterprise Log Manager que vous envisagez d'installer.
2. Ajoutez des lecteurs de disques virtuels.
3. Sur l'un des hôtes d'ordinateurs virtuels, installez un serveur CA Enterprise Log Manager virtuel pour les fonctions de gestion.
4. Installez plusieurs serveurs CA Enterprise Log Manager pour la collecte et la génération de rapports.
5. Configurez les serveurs CA Enterprise Log Manager conformément à la section traitant de l'installation d'un serveur CA Enterprise Log Manager.

Création d'un nouvel ordinateur virtuel

Utilisez la procédure suivante pour créer un nouvel ordinateur à l'aide du client VMware Infrastructure. Utilisez quatre processeurs pour chaque serveur CA Enterprise Log Manager virtuel afin d'obtenir des performances acceptables.

Pour créer un nouvel ordinateur virtuel

1. Accédez au client VMware Infrastructure.
2. Cliquez avec le bouton droit sur l'hôte ESX dans le volet gauche, puis sélectionnez Nouvel ordinateur virtuel pour appeler l'assistant de création d'un ordinateur virtuel. Cette action affiche une boîte de dialogue de type de configuration.
3. Sélectionnez la configuration Personnalisée et cliquez sur Suivant. Une boîte de dialogue de nom et d'emplacement s'affiche.
4. Entrez un nom pour le serveur CA Enterprise Log Manager à installer sur cet ordinateur virtuel et cliquez sur Suivant.
5. Spécifiez les paramètres de stockage pour votre ordinateur virtuel, puis cliquez sur Suivant.

Vérifiez que vos paramètres de stockage sont suffisamment importants pour votre serveur CA Enterprise Log Manager. Nous recommandons un espace minimal de 500 Go.

Remarque : La configuration de lecteurs de disques virtuels supplémentaires pour stocker les journaux d'événements collectés fait l'objet d'une autre procédure.

6. Sélectionnez Red Hat Enterprise Linux 5 (32 bits) comme Système d'exploitation invité et cliquez sur Suivant.

7. Sélectionnez 4 comme nombre de processeurs virtuels dans la liste déroulante Nombre de processeurs virtuels.

Votre serveur hôte physique doit être capable de consacrer quatre UC physiques *exclusivement* à cette instance CA Enterprise Log Manager. Cliquez sur Suivant.
8. Configurez la taille de la mémoire de l'ordinateur virtuel et cliquez sur Suivant. La taille *minimale* acceptable de la mémoire pour CA Enterprise Log Manager est 8 Go ou 8 192 Mo.
9. Configurez votre contrôleur d'interface réseau (NIC). CA Enterprise Log Manager nécessite au moins une connexion réseau. Sélectionnez NIC x dans la liste de NIC disponibles et paramétrez la valeur Adaptateur sur Flexible.

Remarque : Vous n'avez pas besoin de configurer un NIC séparé pour chaque serveur CA Enterprise Log Manager hébergé sur ce serveur physique. Toutefois, vous devez allouer et affecter une adresse IP statique à chaque serveur.
10. Sélectionnez l'option Connecter au démarrage et cliquez sur Suivant. La boîte de dialogue Types d'adaptateurs E/S s'affiche.
11. Select LSI Logic pour l'adaptateur E/S, puis cliquez sur Suivant. La boîte de dialogue Sélectionner un disque s'affiche.
12. Sélectionnez l'option Créer un nouveau disque virtuel, puis cliquez sur Suivant. La boîte de dialogue concernant la capacité et l'emplacement du disque s'affiche.
13. Précisez la capacité et l'emplacement de votre disque, puis cliquez sur Suivant. Une boîte de dialogue d'options avancées s'affiche.

Vous pouvez stocker ce disque avec votre ordinateur virtuel ou spécifier un autre emplacement. Nous recommandons un espace minimal de 500 Go.
14. Acceptez les valeurs par défaut des options avancées et cliquez sur Suivant.
15. Confirmez vos paramètres et cliquez sur Terminer pour créer le nouvel ordinateur virtuel.

Ajout de lecteurs de disques virtuels

Utilisez la procédure suivante afin d'ajouter des lecteurs de disques virtuels pour le stockage de journaux d'événements. Utilisez les mêmes paramètres, sans tenir compte du rôle joué par un serveur CA Enterprise Log Manager spécifique sur votre réseau.

Pour modifier les paramètres

1. Cliquez avec le bouton droit sur votre ordinateur virtuel dans le client VMware Infrastructure et sélectionnez Modifier les paramètres.
La boîte de dialogue Propriétés de l'ordinateur virtuel s'affiche.
2. Mettez en surbrillance les propriétés du lecteur de CD/DVD 1.
3. Cliquez sur le bouton d'option Unité hôte et sélectionnez votre lecteur de DVD-ROM dans la liste déroulante.
4. Sélectionnez l'option Etat de l'unité, Connecter au démarrage.
5. Cliquez sur Ajouter pour lancer l'assistant d'ajout de matériel et ajouter un deuxième disque dur.
6. Mettez le disque dur en surbrillance dans la liste des unités et cliquez sur Suivant. La boîte de dialogue Sélectionner un disque s'affiche.
7. Sélectionnez l'option Créer un nouveau disque virtuel et cliquez sur Suivant.
8. Spécifiez la taille de votre nouveau disque et sélectionnez l'option Spécifier un magasin de données pour paramétrer son emplacement.

CA Enterprise Log Manager détecte ce lecteur supplémentaire au cours de l'installation et l'affecte au magasin de données. Nous vous recommandons d'optimiser l'espace de stockage que vous pouvez mettre à disposition de CA Enterprise Log Manager.

Remarque : Le paramètre de taille de bloc par défaut du serveur VMware ESX Server est 1 Mo, ce qui limite à 256 Go l'espace disque maximal que vous pouvez créer. Si vous avez besoin d'espace supplémentaire, jusqu'à 512 Go, augmentez le paramètre de taille de bloc à 2 Mo grâce à la commande ci-dessous.

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

Redémarrez l'instance ESX Server pour que les changements entrent en vigueur. Pour plus d'informations sur cette commande et sur d'autres commandes, consultez la documentation VMware ESX Server.

Cliquez sur Suivant pour afficher la boîte de dialogue Spécifier les options avancées.

9. Acceptez les valeurs par défaut des options avancées et cliquez sur Suivant. La boîte de dialogue Prêt à terminer s'affiche.
10. Cliquez sur Terminer pour stocker vos modifications sur cet ordinateur virtuel. Cette action vous renvoie à la boîte de dialogue du client VMware Infrastructure.

Installation de CA Enterprise Log Manager sur l'ordinateur virtuel

Utilisez la procédure suivante pour installer CA Enterprise Log Manager sur un ordinateur virtuel précédemment créé.

Vous pouvez configurer un serveur CA Enterprise Log Manager virtuel ou dédié après l'installation pour qu'il affiche l'un des nombreux rôles fonctionnels, tels que la gestion, la collecte ou la génération de rapports. Si vous installez un serveur de gestion CA Enterprise Log Manager, ne l'utilisez pas pour recevoir des journaux d'événements ou pour exécuter des requêtes et des rapports. Installez des serveurs CA Enterprise Log Manager virtuels distincts pour faire office de serveurs de rapports et de collecte, afin d'obtenir les meilleures performances possibles.

Examinez les instructions d'installation normale avant d'installer CA Enterprise Log Manager dans un environnement virtuel. La feuille de calcul d'installation vous permet de collecter les informations nécessaires.

Pour installer CA Enterprise Log Manager sur un ordinateur virtuel

1. Chargez votre disque d'installation du SE CA Enterprise Log Manager dans le lecteur physique de DVD-ROM ou recherchez le répertoire dans lequel vous avez copié l'image de l'installation.
2. Mettez votre ordinateur virtuel en surbrillance dans la liste d'inventaire des ordinateurs virtuels, cliquez dessus avec le bouton droit et sélectionnez Démarrage.
3. Poursuivez l'installation normale de CA Enterprise Log Manager.
4. Configurez le serveur CA Enterprise Log Manager installé pour le rôle fonctionnel souhaité, en utilisant les informations de la section traitant de l'installation d'un serveur CA Enterprise Log Manager.

Informations complémentaires :

[Installation de CA Enterprise Log Manager](#) (page 83)

Déploiement rapide de serveurs CA Enterprise Log Manager virtuels

Vous pouvez cloner un serveur CA Enterprise Log Manager virtuel pour créer une image déployable qui vous permettra de faire évoluer rapidement votre environnement de collecte de journaux.

Remarque : Pour des performances optimales, il est recommandé d'installer CA Enterprise Log Manager sur des serveurs virtuels pour gérer uniquement des tâches de collecte. Ne clonez pas un ordinateur virtuel qui contient un serveur de gestion CA Enterprise Log Manager.

Avant d'effectuer cette opération, assurez-vous de disposer d'un environnement adéquat ou installez un serveur CA Enterprise Log Manager pour exécuter les fonctions de gestion sur un serveur dédié ou virtuel. Vous devez également disposer de la version appropriée du logiciel VMware pour prendre en charge la fonction de clonage.

La procédure de création et de clonage d'un serveur CA Enterprise Log Manager virtuel à des fins de collecte comporte les étapes ci-après.

1. Créez un nouvel ordinateur virtuel.
2. Ajoutez des lecteurs de disques virtuels.
3. Installez un serveur CA Enterprise Log Manager sur l'ordinateur virtuel.
4. Clonez l'ordinateur virtuel contenant le nouveau serveur CA Enterprise Log Manager en suivant les instructions du fournisseur.

Remarque : Vous devez créer une image clone complète. N'utilisez pas de clones liés avec CA Enterprise Log Manager.

5. Importez l'ordinateur virtuel cloné sur un serveur physique cible.
6. Mettez à jour l'ordinateur virtuel cloné avant de le connecter au réseau.
7. Configurez le serveur CA Enterprise Log Manager conformément à la procédure décrite dans le *Manuel d'implémentation*.

Création d'un nouvel ordinateur virtuel

Utilisez la procédure suivante pour créer un nouvel ordinateur à l'aide du client VMware Infrastructure. Utilisez quatre processeurs pour chaque serveur CA Enterprise Log Manager virtuel afin d'obtenir des performances acceptables.

Pour créer un nouvel ordinateur virtuel

1. Accédez au client VMware Infrastructure.
2. Cliquez avec le bouton droit sur l'hôte ESX dans le volet gauche, puis sélectionnez Nouvel ordinateur virtuel pour appeler l'assistant de création d'un ordinateur virtuel. Cette action affiche une boîte de dialogue de type de configuration.
3. Sélectionnez la configuration Personnalisée et cliquez sur Suivant. Une boîte de dialogue de nom et d'emplacement s'affiche.

4. Entrez un nom pour le serveur CA Enterprise Log Manager à installer sur cet ordinateur virtuel et cliquez sur Suivant.
5. Spécifiez les paramètres de stockage pour votre ordinateur virtuel, puis cliquez sur Suivant.

Vérifiez que vos paramètres de stockage sont suffisamment importants pour votre serveur CA Enterprise Log Manager. Nous recommandons un espace minimal de 500 Go.

Remarque : La configuration de lecteurs de disques virtuels supplémentaires pour stocker les journaux d'événements collectés fait l'objet d'une autre procédure.

6. Sélectionnez Red Hat Enterprise Linux 5 (32 bits) comme Système d'exploitation invité et cliquez sur Suivant.
7. Sélectionnez 4 comme nombre de processeurs virtuels dans la liste déroulante Nombre de processeurs virtuels.

Votre serveur hôte physique doit être capable de consacrer quatre UC physiques *exclusivement* à cette instance CA Enterprise Log Manager. Cliquez sur Suivant.
8. Configurez la taille de la mémoire de l'ordinateur virtuel et cliquez sur Suivant. La taille *minimale* acceptable de la mémoire pour CA Enterprise Log Manager est 8 Go ou 8 192 Mo.
9. Configurez votre contrôleur d'interface réseau (NIC). CA Enterprise Log Manager nécessite au moins une connexion réseau. Sélectionnez NIC x dans la liste de NIC disponibles et paramétrez la valeur Adaptateur sur Flexible.

Remarque : Vous n'avez pas besoin de configurer un NIC séparé pour chaque serveur CA Enterprise Log Manager hébergé sur ce serveur physique. Toutefois, vous devez allouer et affecter une adresse IP statique à chaque serveur.

10. Sélectionnez l'option Connecter au démarrage et cliquez sur Suivant. La boîte de dialogue Types d'adaptateurs E/S s'affiche.
11. Select LSI Logic pour l'adaptateur E/S, puis cliquez sur Suivant. La boîte de dialogue Sélectionner un disque s'affiche.
12. Sélectionnez l'option Créer un nouveau disque virtuel, puis cliquez sur Suivant. La boîte de dialogue concernant la capacité et l'emplacement du disque s'affiche.

13. Précisez la capacité et l'emplacement de votre disque, puis cliquez sur Suivant. Une boîte de dialogue d'options avancées s'affiche.

Vous pouvez stocker ce disque avec votre ordinateur virtuel ou spécifier un autre emplacement. Nous recommandons un espace minimal de 500 Go.

14. Acceptez les valeurs par défaut des options avancées et cliquez sur Suivant.

15. Confirmez vos paramètres et cliquez sur Terminer pour créer le nouvel ordinateur virtuel.

Ajout de lecteurs de disques virtuels

Utilisez la procédure suivante afin d'ajouter des lecteurs de disques virtuels pour le stockage de journaux d'événements. Utilisez les mêmes paramètres, sans tenir compte du rôle joué par un serveur CA Enterprise Log Manager spécifique sur votre réseau.

Pour modifier les paramètres

1. Cliquez avec le bouton droit sur votre ordinateur virtuel dans le client VMware Infrastructure et sélectionnez Modifier les paramètres.

La boîte de dialogue Propriétés de l'ordinateur virtuel s'affiche.

2. Mettez en surbrillance les propriétés du lecteur de CD/DVD 1.

3. Cliquez sur le bouton d'option Unité hôte et sélectionnez votre lecteur de DVD-ROM dans la liste déroulante.

4. Sélectionnez l'option Etat de l'unité, Connecter au démarrage.

5. Cliquez sur Ajouter pour lancer l'assistant d'ajout de matériel et ajouter un deuxième disque dur.

6. Mettez le disque dur en surbrillance dans la liste des unités et cliquez sur Suivant. La boîte de dialogue Sélectionner un disque s'affiche.

7. Sélectionnez l'option Créer un nouveau disque virtuel et cliquez sur Suivant.

8. Spécifiez la taille de votre nouveau disque et sélectionnez l'option Spécifier un magasin de données pour paramétrer son emplacement.

CA Enterprise Log Manager détecte ce lecteur supplémentaire au cours de l'installation et l'affecte au magasin de données. Nous vous recommandons d'optimiser l'espace de stockage que vous pouvez mettre à disposition de CA Enterprise Log Manager.

Remarque : Le paramètre de taille de bloc par défaut du serveur VMware ESX Server est 1 Mo, ce qui limite à 256 Go l'espace disque maximal que vous pouvez créer. Si vous avez besoin d'espace supplémentaire, jusqu'à 512 Go, augmentez le paramètre de taille de bloc à 2 Mo grâce à la commande ci-dessous.

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

Redémarrez l'instance ESX Server pour que les changements entrent en vigueur. Pour plus d'informations sur cette commande et sur d'autres commandes, consultez la documentation VMware ESX Server.

Cliquez sur Suivant pour afficher la boîte de dialogue Spécifier les options avancées.

9. Acceptez les valeurs par défaut des options avancées et cliquez sur Suivant. La boîte de dialogue Prêt à terminer s'affiche.
10. Cliquez sur Terminer pour stocker vos modifications sur cet ordinateur virtuel. Cette action vous renvoie à la boîte de dialogue du client VMware Infrastructure.

Installation de CA Enterprise Log Manager sur l'ordinateur virtuel

Utilisez la procédure suivante pour installer CA Enterprise Log Manager sur un ordinateur virtuel précédemment créé.

Vous pouvez configurer un serveur CA Enterprise Log Manager virtuel ou dédié après l'installation pour qu'il affiche l'un des nombreux rôles fonctionnels, tels que la gestion, la collecte ou la génération de rapports. Si vous installez un serveur de gestion CA Enterprise Log Manager, ne l'utilisez pas pour recevoir des journaux d'événements ou pour exécuter des requêtes et des rapports. Installez des serveurs CA Enterprise Log Manager virtuels distincts pour faire office de serveurs de rapports et de collecte, afin d'obtenir les meilleures performances possibles.

Examinez les instructions d'installation normale avant d'installer CA Enterprise Log Manager dans un environnement virtuel. La feuille de calcul d'installation vous permet de collecter les informations nécessaires.

Pour installer CA Enterprise Log Manager sur un ordinateur virtuel

1. Chargez votre disque d'installation du SE CA Enterprise Log Manager dans le lecteur physique de DVD-ROM ou recherchez le répertoire dans lequel vous avez copié l'image de l'installation.
2. Mettez votre ordinateur virtuel en surbrillance dans la liste d'inventaire des ordinateurs virtuels, cliquez dessus avec le bouton droit et sélectionnez Démarrage.
3. Poursuivez l'installation normale de CA Enterprise Log Manager.
4. Configurez le serveur CA Enterprise Log Manager installé pour le rôle fonctionnel souhaité, en utilisant les informations de la section traitant de l'installation d'un serveur CA Enterprise Log Manager.

Informations complémentaires :

[Installation de CA Enterprise Log Manager](#) (page 83)

Clonage d'un serveur CA Enterprise Log Manager virtuel

Cette procédure vous permet de cloner un serveur CA Enterprise Log Manager virtuel. Elle suppose que vous avez déjà créé un nouvel ordinateur virtuel, que vous y avez déjà ajouté des lecteurs de disque et que vous avez installé CA Enterprise Log Manager.

Pour cloner un serveur virtuel

1. Accédez à VMware VirtualCenter et recherchez l'ordinateur virtuel contenant CA Enterprise Log Manager.
2. Désactivez-le.
3. Sélectionnez Exporter et indiquez l'emplacement d'exportation de l'ordinateur virtuel.

VMware ESX Server offre d'autres méthodes de clonage des ordinateurs virtuels. Pour plus d'informations, reportez-vous à la documentation VMware.

Importation d'un ordinateur virtuel cloné sur un serveur cible

Utilisez la procédure suivante pour importer un ordinateur virtuel cloné sur un autre ordinateur afin de l'activer.

Pour importer un ordinateur virtuel cloné

1. Vérifiez que vous avez accès au serveur hôte cible.
2. Accédez à VMware VirtualCenter à partir du serveur qui héberge VMware ESX.
3. Sélectionnez Importer et recherchez le serveur cible, en répondant aux invitations qui s'affichent.

L'importation déplace l'ordinateur virtuel cloné vers le serveur cible. Pour plus d'informations, consultez la documentation de VMware ESX.

Mise à jour d'un serveur CA Enterprise Log Manager cloné avant le déploiement

Utilisez la procédure suivante pour mettre à jour un serveur CA Enterprise Log Manager virtuel cloné.

Un serveur CA Enterprise Log Manager virtuel cloné conserve le nom d'hôte que vous lui avez attribué au cours de l'installation. Cependant, le nom d'hôte de chaque serveur CA Enterprise Log Manager actif doit être unique au sein de votre implémentation de collecte de journaux. C'est pourquoi, avant d'activer un serveur virtuel cloné, vous devez modifier le nom d'hôte et l'adresse IP du serveur avec le script *Rename_ELM.sh*.

Le script de mise à jour effectue notamment les actions ci-dessous.

- Arrêt et redémarrage automatique de l'agent par défaut
- Arrêt et redémarrage automatique du service iGateway
- Invitation à modifier le nom d'hôte, et les adresses IP et DNS IP
- Mise à jour automatique des fichiers de configuration avec des mots de passe chiffrés pour les différents certificats

Pour mettre à jour un serveur CA Enterprise Log Manager virtuel cloné

1. Connectez-vous au serveur physique cible en tant qu'utilisateur root.
2. Accédez à l'image ISO ou au DVD de l'application, puis au répertoire /CA/Linux_x86.

Vous trouverez également le script dans le système de fichiers d'un serveur CA Enterprise Log Manager installé. Le script se trouve dans le répertoire opt/CA/LogManager.

3. Copiez le script Rename_ELM.sh sur le serveur cible.
4. Modifiez les informations du serveur CA Enterprise Log Manager virtuel à l'aide de la commande ci-dessous.

```
./Rename_ELM.sh
```

5. Répondez aux invites.
6. Démarrez l'ordinateur virtuel qui contient le serveur virtuel mis à jour.

Création de serveurs CA Enterprise Log Manager à l'aide d'ordinateurs virtuels

Vous pouvez déployer CA Enterprise Log Manager en tant que dispositif virtuel au format OVF (Open Virtualization Format). Le provisionnement du dispositif virtuel requiert moins de temps que pour l'installation ou le clonage d'un serveur CA Enterprise Log Manager sur un ordinateur virtuel.

Dispositifs virtuels CA Enterprise Log Manager

Le format OVF est une norme ouverte de packaging et de distribution de dispositifs virtuels. CA Enterprise Log Manager utilise le format de fichier VMDK (Virtual Machine Disk) basé sur la norme OVF. Le package OVF contient les fichiers suivants :

Fichier OVF de descripteur XML

Un fichier OVF de descripteur XML avec extension .ovf. Ce fichier contient les spécifications matérielles virtuelles, les paramètres de configuration de CA Enterprise Log Manager et le contrat de licence.

Fichiers de disques virtuels

Il s'agit des fichiers de disques virtuels VMware vSphere suivants, qui contiennent des fichiers d'image disque utilisés pour le déploiement de l'appareil virtuel :

- CA Enterprise Log Manager 1.vmdk
- CA Enterprise Log Manager 2.vmdk
- CA Enterprise Log Manager 3.vmdk

Fichier Manifest

Il s'agit du fichier CA Enterprise Log Manager.mf, qui contient la signature de tous les fichiers.

Remarque : Nous vous recommandons vivement de ne pas modifier les fichiers de disques virtuels ni le fichier Manifest, car cela pourrait affecter les performances du dispositif virtuel.

Par défaut, le Client VMware vSphere lit les détails importés à l'aide du modèle OVF et effectue le provisionnement du dispositif virtuel.

Fonctionnement du dispositif virtuel

Vous pouvez utiliser un dispositif virtuel pour créer des serveurs CA Enterprise Log Manager virtuels pour votre environnement de collecte de journaux d'événements à l'aide des scénarios ci-dessous.

- Ajout de serveurs virtuels à un environnement CA Enterprise Log Manager existant : création d'un environnement mixte
- Création d'un environnement virtuel de collecte de journaux
- Déploiement de serveurs CA Enterprise Log Manager virtuels pour une évolutivité rapide

Utilisez le client VMware vSphere pour une installation silencieuse ou manuelle du dispositif virtuel. Le fichier OVF de descripteur contient les paramètres de configuration requis par CA Enterprise Log Manager. Entrez une valeur pour chaque paramètre de configuration pendant l'installation.

Feuille de calcul d'installation de dispositifs virtuels

Avant d'installer le dispositif virtuel, collectez les informations indiquées dans le tableau ci-après. Une fois la feuille de calcul renseignée, vous pouvez l'utiliser lors de votre travail, pour répondre aux invites de l'installation. Vous pouvez imprimer et renseigner une feuille de calcul distincte pour chaque serveur CA Enterprise Log Manager que vous envisagez d'installer.

Informations requises	Valeur	Commentaires
Paramètres spécifiques aux hôtes		
Nom d'hôte	<i>Nom d'hôte pour ce serveur CA Enterprise Log Manager</i> Exemple : CA-ELM1	Spécifiez le nom d'hôte de ce serveur en utilisant uniquement les caractères pris en charge par les hôtes. Les normes du secteur recommandent les lettres de A à Z (insensibles à la casse), les chiffres de 0 à 9 et le tiret, avec une lettre en premier caractère et un caractère alphanumérique en dernière position. N'utilisez pas le caractère de soulignement dans un nom d'hôte et ne lui ajoutez pas de nom de domaine. Remarque : Le nom d'hôte ne peut pas dépasser 15 caractères.

Informations requises	Valeur	Commentaires
Mot passe root	<i>nouveau mot de passe root</i>	Créez et confirmez un nouveau mot de passe root pour ce serveur.
Adresse IP	<i>Adresse IPv4 correspondante</i>	Entrez une adresse IP valide pour ce serveur.
Masque de sous-réseau	<i>Adresse IP correspondante</i>	Entrez un masque de sous-réseau valide à utiliser avec ce serveur.
Passerelle par défaut	<i>Adresse IP correspondante</i>	Entrez une passerelle par défaut valide à utiliser avec ce serveur.
Serveurs DNS	<i>Adresses IPv4 correspondantes</i>	Entrez une ou plusieurs adresses IP de serveur DNS à utiliser sur votre réseau. La liste est séparée par des virgules, sans espace entre les entrées. Si vos serveurs DNS utilisent l'adressage IPv6, entrez ces adresses avec ce format.
Nom de domaine	<i>votre nom de domaine</i>	Entrez le nom de domaine complet au sein duquel opère le serveur, par exemple mycompany.com. Remarque : Le nom de domaine doit être enregistré auprès du serveur DNS (Domain Name Server) de votre réseau pour permettre la résolution du nom d'hôte vers l'adresse IP.
EULA	Accepter	Lisez l'ensemble du contrat de licence CA, puis cliquez sur Accepter pour en accepter les conditions.
Fuseau horaire	<i>le fuseau horaire que vous souhaitez</i>	Sélectionnez le fuseau horaire dont dépend ce serveur.
Paramètres spécifiques aux applications		

Informations requises	Valeur	Commentaires
Emplacement du serveur CA EEM	Local pour le premier serveur installé (serveur de gestion) Distant pour chaque serveur supplémentaire	Indiquez si vous prévoyez d'utiliser un serveur CA EEM local ou distant. Pour un serveur CA Enterprise Log Manager de gestion, choisissez l'option locale. L'installation vous invite à créer un mot de passe pour le compte d'utilisateur EiamAdmin par défaut. Pour chaque serveur supplémentaire, choisissez l'option distante. L'installation vous invite à indiquer le nom du serveur de gestion. Que vous choisissiez l'option locale ou distante, vous devez utiliser l'ID et le mot de passe du compte EiamAdmin lors de la première connexion à chaque serveur CA Enterprise Log Manager.
Nom d'hôte ou adresse IP du serveur CA EEM	<i>adresse IP ou nom d'hôte</i>	Entrez cette valeur uniquement si vous sélectionnez l'option de serveur distant. Entrez l'adresse IP ou le nom d'hôte du serveur CA Enterprise Log Manager de gestion installé en premier. Le nom d'hôte doit être enregistré auprès du serveur DNS. Si vous voulez utiliser un serveur CA EEM local, la valeur par défaut n'est Aucun .

Informations requises	Valeur	Commentaires
Mot de passe pour le serveur CA EEM	<i>mot de passe du compte</i> <i>EiamAdmin</i>	<p>Enregistrez le mot de passe du compte d'administrateur par défaut, EiamAdmin.</p> <p>Votre serveur CA Enterprise Log Manager doit disposer de ces informations d'identification de compte pour la connexion initiale.</p> <p>Si vous installez le serveur de gestion, vous créez et confirmez ici un nouveau mot de passe EiamAdmin.</p> <p>Notez ce mot de passe, car vous l'utiliserez à nouveau lors de l'installation d'autres serveurs et agents CA Enterprise Log Manager.</p> <p>Remarque : Le mot de passe entré ici est également le mot de passe initial du compte caelmadmin par défaut, que vous utiliserez pour accéder directement au serveur CA Enterprise Log Manager via ssh.</p> <p>Si vous le souhaitez, vous pouvez créer d'autres comptes d'administrateur pour accéder aux fonctions CA EEM après l'installation.</p>
FIPS	Oui ou Non	Spécifie si le dispositif virtuel doit être exécuté en mode FIPS ou non. Si vous choisissez un serveur CA EEM local, choisissez le mode de votre choix. Si vous choisissez un serveur CA EEM distant, choisissez le mode utilisé par ce serveur.

Ajout de serveurs virtuels à votre environnement

Si vous disposez déjà d'une implémentation CA Enterprise Log Manager, vous pouvez ajouter des serveurs de collecte CA Enterprise Log Manager virtuels pour gérer un volume d'événements accru sur votre réseau. Ce scénario suppose que vous avez déjà installé un serveur de gestion CA Enterprise Log Manager et un ou plusieurs serveurs CA Enterprise Log Manager pour la collecte et la génération de rapports.

Remarque : Pour obtenir les meilleures performances possibles, installez CA Enterprise Log Manager sur des serveurs virtuels pour gérer uniquement les tâches de collecte et de génération de rapports.

Le processus d'ajout de serveurs de collecte virtuels à votre environnement inclut les procédures ci-dessous.

1. Téléchargez le package de dispositif virtuel CA Enterprise Log Manager.
2. Installez un serveur CA Enterprise Log Manager à l'aide du dispositif virtuel.
3. Configurez le serveur CA Enterprise Log Manager en vous référant à la section traitant de l'installation.

Après avoir installé le serveur de collecte virtuel, vous pouvez l'ajouter à votre fédération pour effectuer des requêtes et des rapports.

Important : Si vous voulez effectuer le provisionnement d'un serveur CA Enterprise Log Manager à l'aide du dispositif virtuel, le nom d'instance d'application du serveur CA Enterprise Log Manager principal doit être CAELM.

Téléchargez le package de dispositif virtuel.

L'image de distribution du dispositif virtuel de CA Enterprise Log Manager est disponible à partir du support en ligne du liens de téléchargement. Vous devez télécharger cinq fichiers :

- Le fichier Manifest
- Le fichier .ovf
- Trois fichiers de disque virtuel

Installation manuelle d'un serveur CALM

Lors de l'installation manuelle du dispositif virtuel, effectuez les tâches suivantes :

1. Déployez un modèle OVF.
2. Définissez les paramètres Paravirtualization et Resource.
3. Démarrez le serveur CA Enterprise Log Manager provisionné.

Déploiement d'un modèle OVF

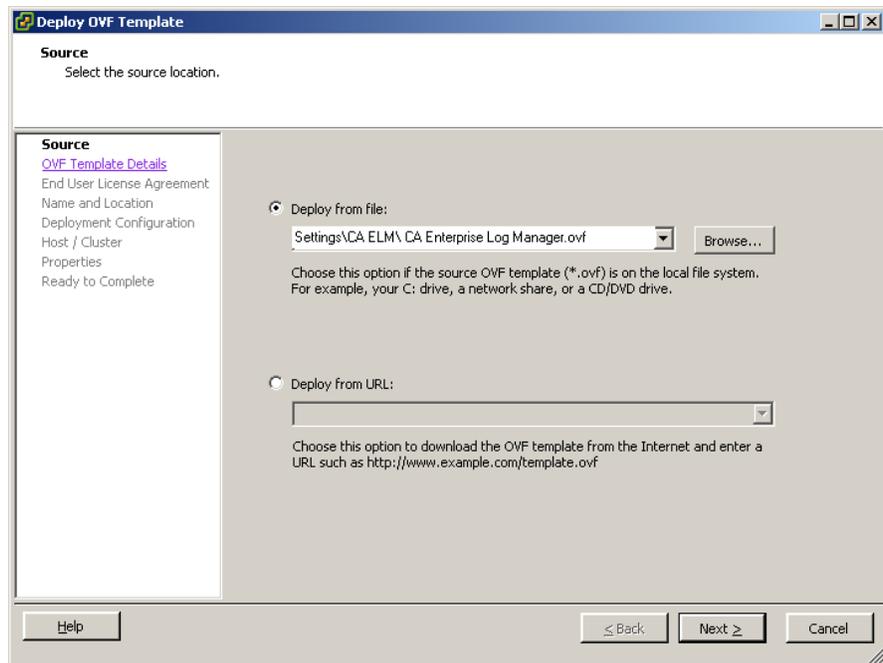
Vous pouvez spécifier les propriétés du dispositif virtuel dans un modèle OVF. VMware utilise ce modèle pour effectuer le provisionnement d'un serveur CA Enterprise Log Manager. Utilisez le Client VMware vSphere pour déployer le modèle OVF.

Remarque : Les captures d'écran qui figurent dans les procédures suivantes contiennent des exemples de données à titre indicatif. Ces captures d'écran concernent le Client VMware vSphere 4.0.0. Nous vous recommandons de spécifier des données propres à votre environnement.

Pour déployer un modèle OVF :

1. Cliquez sur Démarrer, Tous les programmes, Client VMware vSphere sur l'ordinateur où le Client VMware vSphere est installé.
La boîte de dialogue VMware vSphere Client s'ouvre.
2. Dans le champ IP address/Name (Adresse IP/Nom), saisissez l'adresse IP ou le nom d'hôte du serveur VMware vSphere auquel vous souhaitez vous connecter.
3. Entrez les informations d'identification dans les champs User name (nom d'utilisateur) et Password (mot de passe).
4. Cliquez sur Logon (connexion).
La fenêtre de l'application s'ouvre.
5. Sélectionnez l'emplacement où vous voulez effectuer le provisionnement d'un serveur CA Enterprise Log Manager sous un centre de données dans le volet gauche.
6. Cliquez sur File (Fichier), puis sur Deploy OVF Template (Déployer le modèle OVF).
La fenêtre Deploy OVF Template (Déployer le modèle OVF) s'affiche. Par défaut, cette fenêtre affiche la page Source. Saisissez l'emplacement du modèle OVF dans cette page.
Remarque : Les pages affichées dans la fenêtre Deploy OVF Template peuvent varier selon la version de Client VMware vSphere et des paramètres utilisés. Pour plus d'informations sur le déploiement d'un modèle OVF, visitez le site Web www.vmware.com.
7. Sélectionnez l'option Deploy from file (Déployer à partir du fichier) et cliquez sur Parcourir pour sélectionner l'emplacement du modèle OVF.
8. Accédez à l'emplacement du modèle OVF à partir de la boîte de dialogue Open (Ouvrir), sélectionnez le modèle OVF et cliquez sur Open.

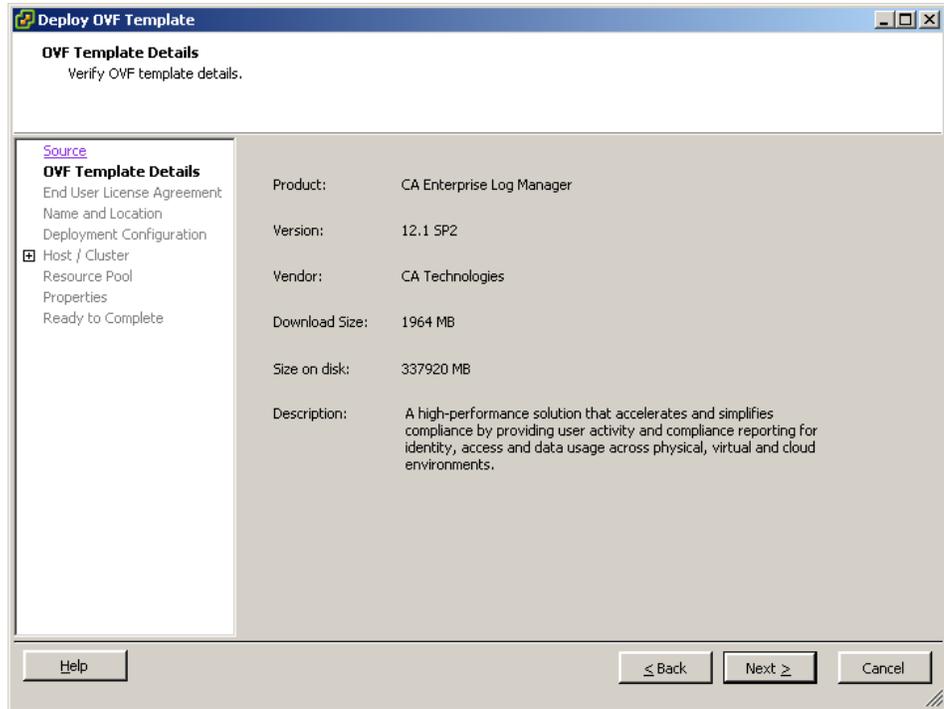
Le chemin d'accès de l'emplacement du modèle OVF s'affiche dans le champ Deploy from file (Déployer à partir du fichier).



9. Cliquez sur Suivant.

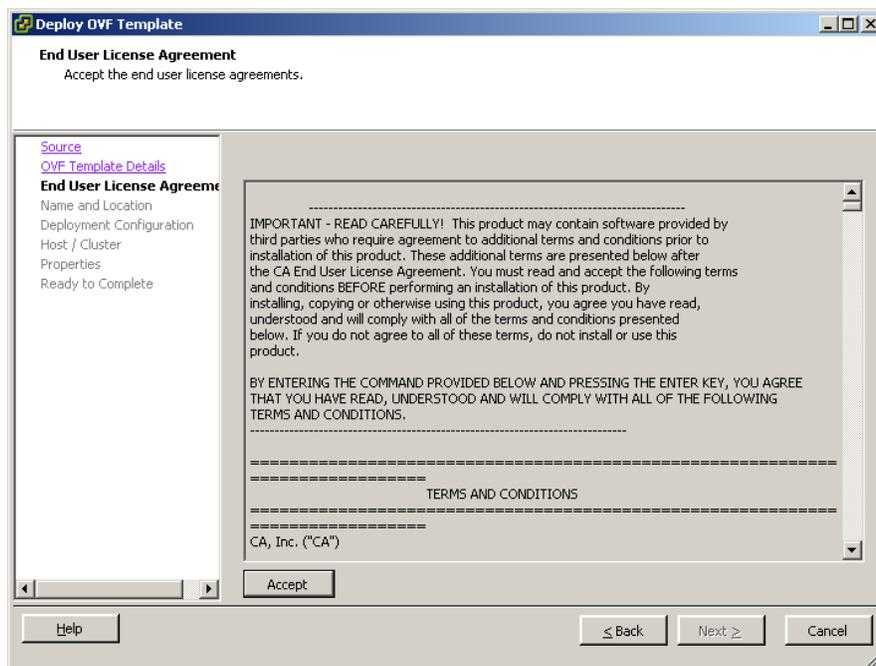
La page OVF Template Details (Informations du modèle OVF) s'ouvre. Cette page contient les informations stockées dans le modèle OVF, tels que la taille de téléchargement, la taille de disque disponible et le nom des fournisseurs.

10. Vérifiez que le serveur VMware dispose de 350 Go minimum d'espace disque, puis cliquez sur Suivant.



La page End User License Agreement (Contrat de licence de l'utilisateur final) s'affiche. Cette page contient le contrat de licence de produits tiers. Vous devez accepter ce contrat de licence pour installer CA Enterprise Log Manager.

11. Lisez le contrat de licence.

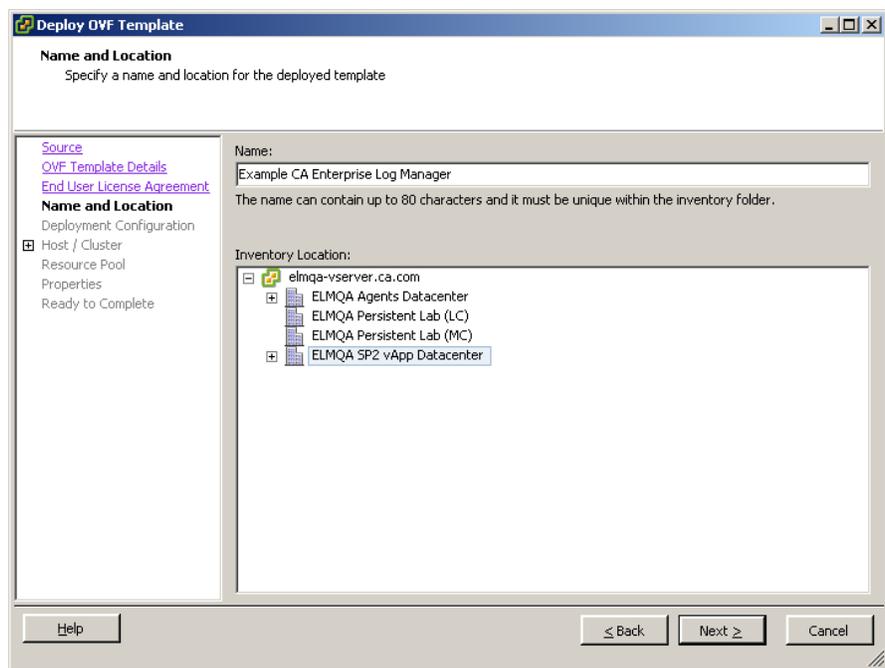


12. Cliquez sur Accept (Accepter), puis sur Suivant.

La page Name and Location (Nom et emplacement) s'ouvre. Elle permet d'ajouter un nom pour identifier le serveur CA Enterprise Log Manager et de spécifier le centre de données où vous voulez effectuer le provisionnement de ce serveur.

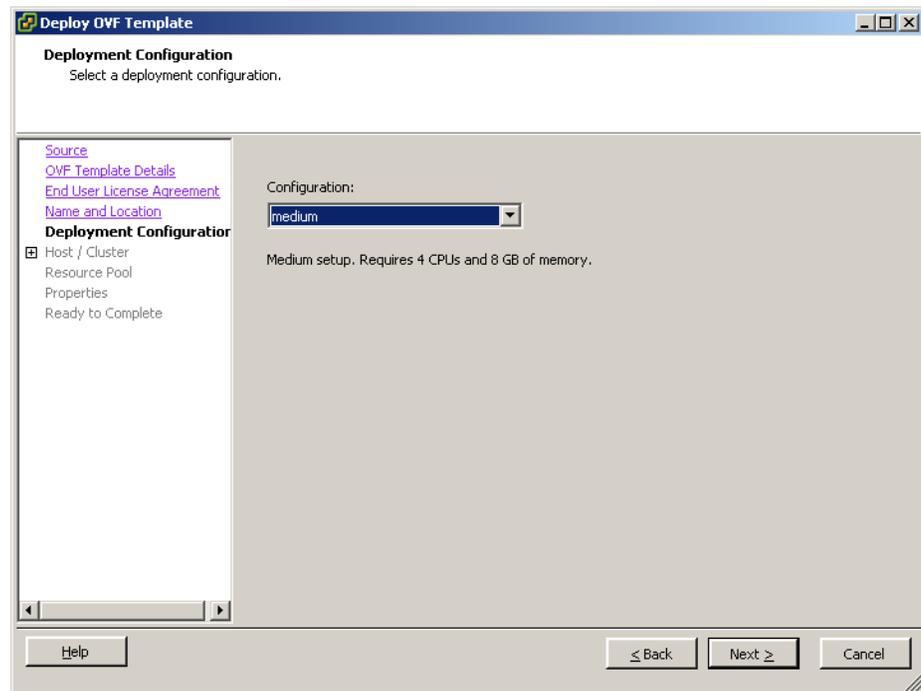
13. Saisissez le nom du serveur CA Enterprise Log Manager dans le champ Nom, sélectionnez le centre de données dans la liste Inventory Location (Emplacement de l'inventaire), puis cliquez sur Suivant.

Remarque : Par défaut, le nom spécifié dans le modèle OVF s'affiche dans le champ Nom.



La page Deployment Configuration (Configuration du déploiement) s'affiche. Elle permet de spécifier le mode de configuration du serveur CA Enterprise Log Manager pour lequel vous voulez effectuer le provisionnement.

14. Dans la liste déroulante Configuration, sélectionnez Moyenne ou Grande, puis cliquez sur Suivant.

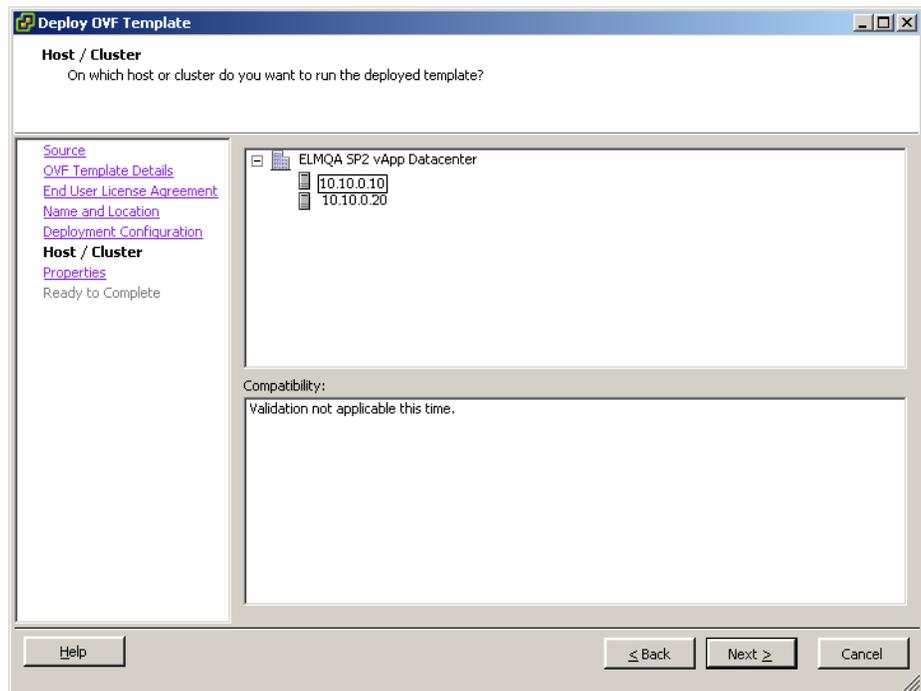


Si vous sélectionnez Moyenne, VMware indique 4 UC de 8 Go de mémoire RAM chacune. Si vous sélectionnez Large, VMware indique huit UC de 8 Go de mémoire RAM chacune.

Remarque : Nous vous recommandons vivement d'utiliser une configuration de déploiement moyenne pour effectuer le provisionnement d'un serveur de collecte, mais une configuration de déploiement importante pour le provisionnement d'un serveur de gestion ou de génération de rapports.

La page Host / Cluster (Hôte / Cluster) s'ouvre. Elle s'affiche uniquement si vous n'avez pas sélectionné le pool de ressources avant l'importation du modèle OVF. Cette page contient le centre de données sélectionné et ses clusters disponibles. Spécifiez l'emplacement des clusters sous le centre de données où vous voulez effectuer le provisionnement du serveur CA Enterprise Log Manager.

15. Sélectionnez un cluster sous le centre de données, puis cliquez sur Suivant.



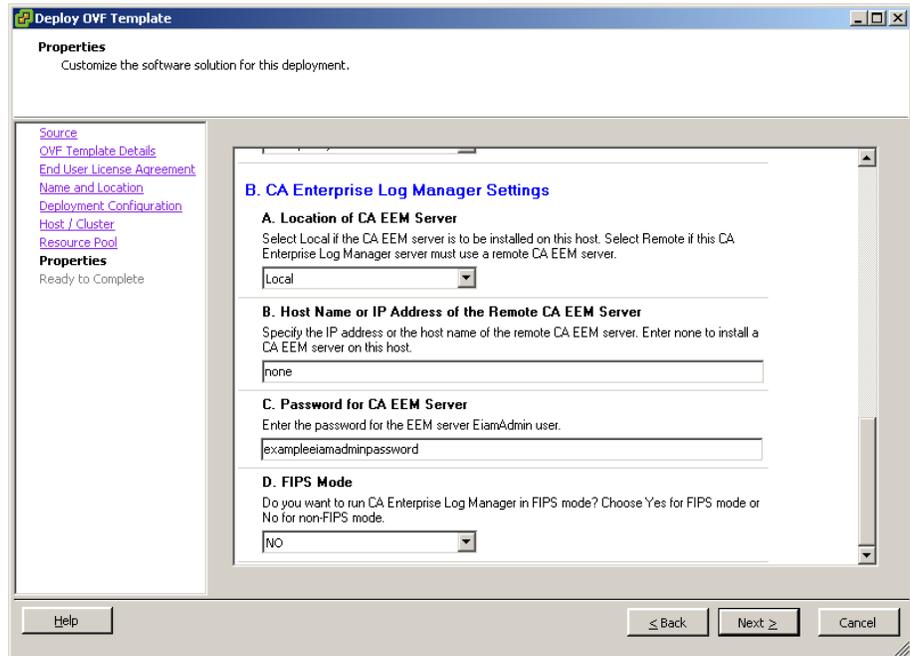
La page Propriétés (Propriétés)s'ouvre. Cette page contient les paramètres de l'hôte et de CA Enterprise Log Manager.

16. Indiquez des valeurs dans chaque champ relatives aux informations collectées dans la feuille de calcul Installation, puis cliquez sur Suivant.

The screenshot shows a window titled "Deploy OVF Template" with a "Properties" tab. The window contains a list of links on the left and a main configuration area on the right. The main area is titled "A. Host Settings" and contains the following fields:

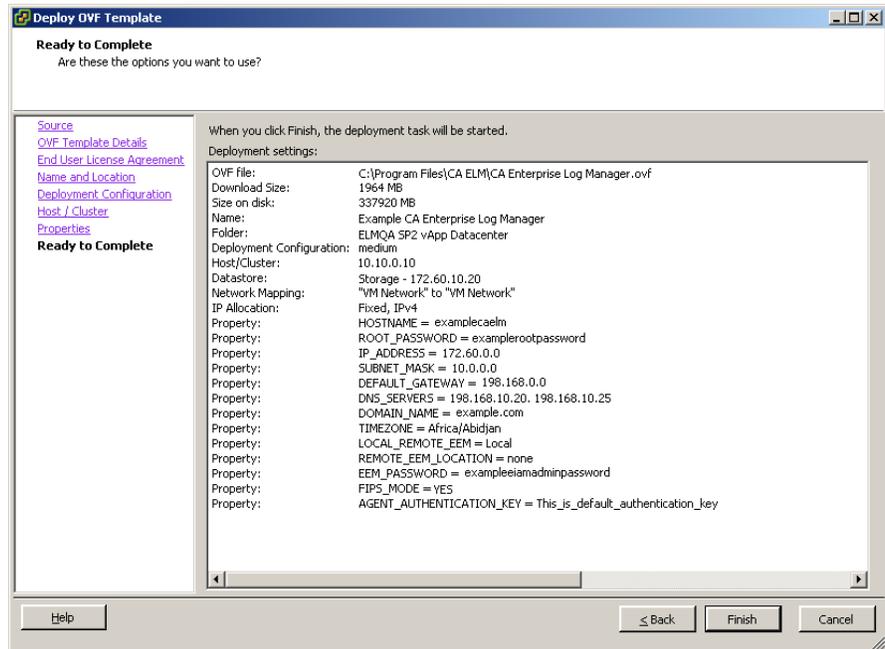
- A. Host Name:** Enter name of this host machine. Value: examplecaelm
- B. Root Password:** Enter root password of this machine. Value: examplerootpassword
- C. IP Address:** Enter IP address of this machine. Value: 172.160.0.0
- D. Subnet Mask:** Enter the subnet mask. Value: 10.0.0.0
- E. Default Gateway:** Enter the IP address of the default gateway. Value: 198.168.0.0
- F. DNS Servers:** Enter a list of the IP addresses for your DNS servers. Use a comma to separate the IP addresses of the DNS servers. Value: 198.168.10.20, 198.168.10.25
- G. Domain Name:** Enter the domain name of this machine. Value: example.com
- H. Time Zone:** Choose the time zone. Value: Africa/Abidjan

At the bottom of the window, there are buttons for "Help", "Back", "Next", and "Cancel".



Le Ready to Complete (Prêt pour la finalisation) s'ouvre. Cette page contient un récapitulatif des informations indiquées aux pages précédentes.

17. Vérifiez ces informations, puis cliquez sur Finish (Terminer).



Le message Opening VI target (Cible VI en cours d'ouverture) s'affiche. Le statut de déploiement du dispositif virtuel s'affiche. Si l'installation s'est correctement effectuée, le dispositif virtuel figurera sous le magasin de données sélectionné dans le volet gauche.

18. (Facultatif) Si vous voulez modifier les informations saisies, procédez comme suit :
 - a. Cliquez sur Précédent dans la fenêtre Deploy OVF Model jusqu'à accéder à la page correspondante.
 - b. Effectuez les modifications nécessaires.
 - c. Cliquez plusieurs fois sur Suivant dans la fenêtre Deploy OVF jusqu'à accéder à la page Ready to Complete.

Définition des paramètres de paravirtualisation et de ressources

Après l'importation du modèle OVF, définissez manuellement les paramètres de paravirtualisation et de ressource pour améliorer les performances du serveur CA Enterprise Log Manager provisionné.

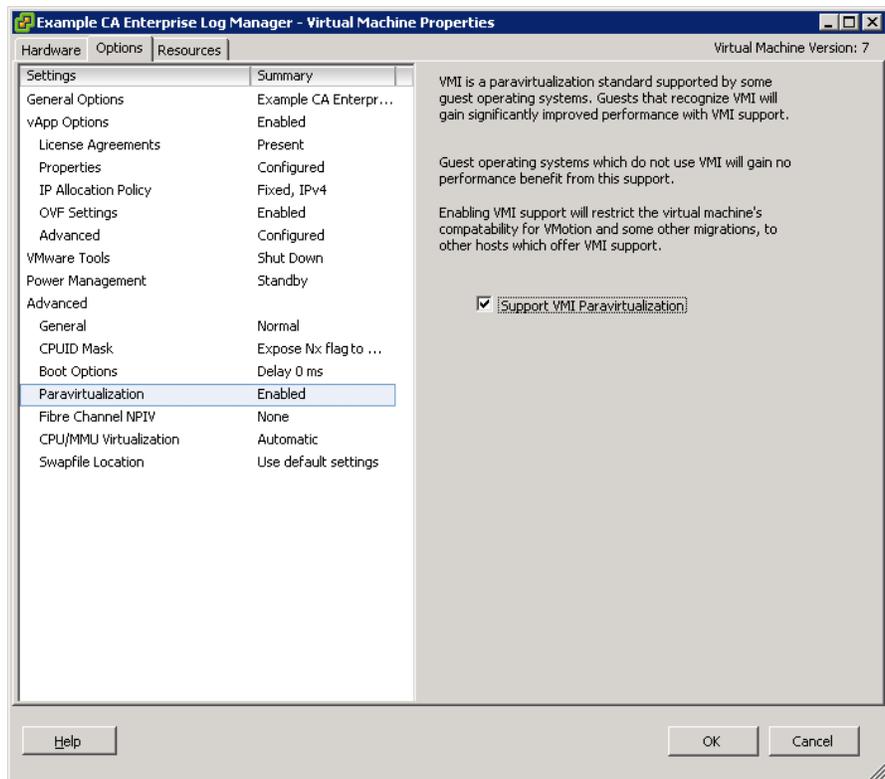
Remarque : Vérifiez que le lecteur de CD/DVD est défini sur (Client Device) Unités du client.

Pour définir les paramètres de paravirtualisation et de ressources :

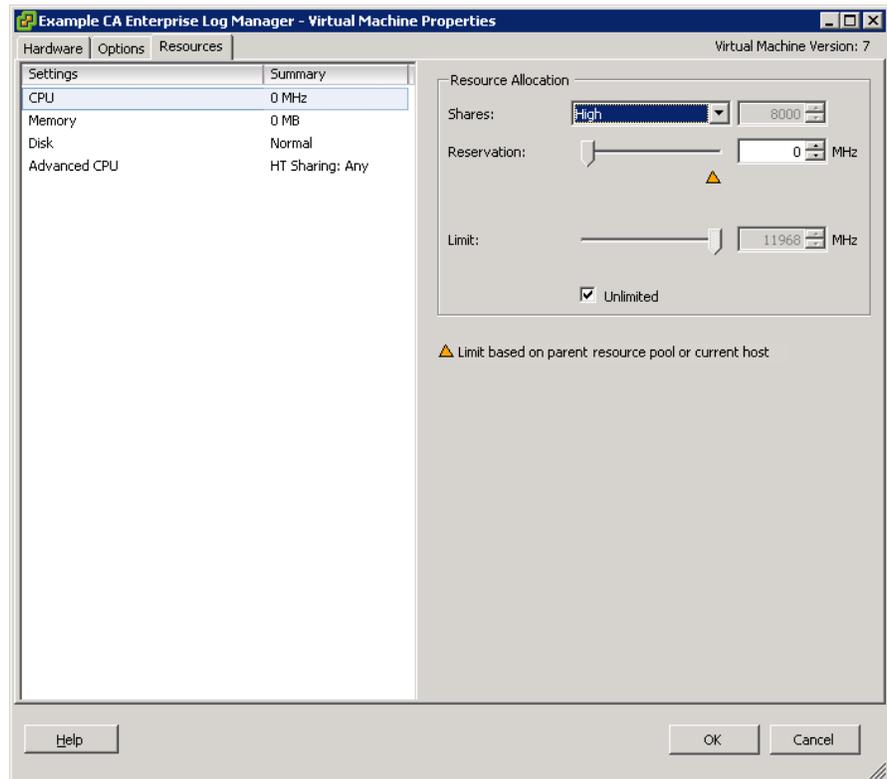
1. Cliquez avec le bouton droit de la souris sur le nouveau dispositif virtuel CA Enterprise Log Manager situé dans le volet gauche et cliquez sur Edit Settings (Modifier les paramètres).

La fenêtre <CA Enterprise Log Manager Virtual Appliance name> - Virtual Machine Properties (Propriétés de l'ordinateur virtuel <CA Enterprise Log Manager nom application virtuelle> s'affiche.

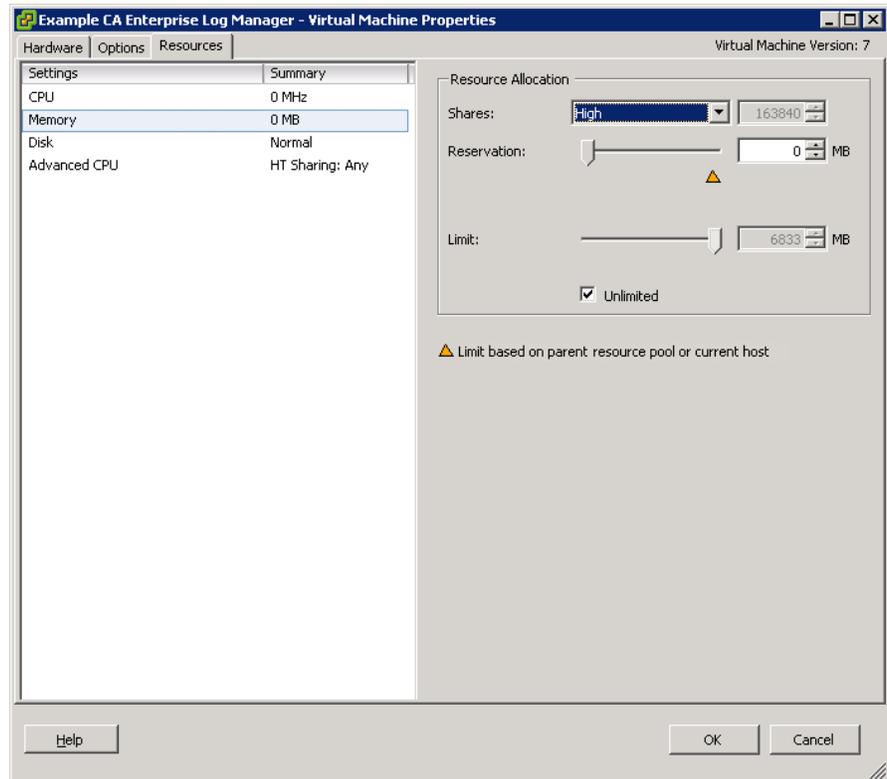
2. Cliquez sur l'onglet Option dans la fenêtre.
3. Sélectionnez le paramètre Paravirtualization situé dans le volet gauche, puis l'option Support VMI Paravirtualization (Prise en charge de la paravirtualization VMI) située dans le volet droit.



4. Cliquez sur l'onglet Resources (Ressources) dans la fenêtre.
5. Sélectionnez l'option CPU (UC) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



- Sélectionnez l'option Memory (Mémoire) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



- Cliquez sur OK.
- Remarque :** Pour plus d'informations sur la paravirtualization, visitez le site Web www.vmware.com.

Démarrez le serveur CA Enterprise Log Manager provisionné.

Ceci est nécessaire à son exécution.

Pour démarrer un serveur CA Enterprise Log Manager :

1. Sélectionnez le nouveau serveur CA Enterprise Log Manager dans le volet gauche de la fenêtre de l'application VMware.
2. Cliquez sur l'option Power On (Démarrage) située sous l'onglet Basic Tasks of the Getting Started (Tâches de base du démarrage) dans le volet droit.

Le serveur CA Enterprise Log Manager est démarré.

Remarque : Vérifiez qu'un serveur CA Enterprise Log Manager principal est exécuté avant de démarrer un serveur CA Enterprise Log Manager secondaire.

Installation silencieuse d'un serveur CA Enterprise Log Manager :

Lors de l'installation silencieuse du dispositif virtuel, effectuez les tâches suivantes :

1. Appelez l'outil OVF.
2. Définissez les paramètres de paravirtualisation et ressources.
3. Démarrez le serveur CA Enterprise Log Manager provisionné.

Le tableau suivant décrit les paramètres utilisés pour le déploiement de CA Enterprise Log Manager à l'aide de l'outil OVF. Vous devez spécifier ces paramètres en tant qu'arguments de ligne de commande dans la ligne de commande.

Informations requises	Valeur	Commentaires
Paramètres spécifiques aux hôtes		

Informations requises	Valeur	Commentaires
HOSTNAME	<i>Nom d'hôte pour ce serveur CA Enterprise Log Manager</i> Exemple : CA-ELM1	Spécifiez le nom d'hôte de ce serveur en utilisant uniquement les caractères pris en charge par les hôtes. Les normes du secteur recommandent les lettres de A à Z (insensibles à la casse), les chiffres de 0 à 9 et le tiret, avec une lettre en premier caractère et un caractère alphanumérique en dernière position. N'utilisez pas le caractère de soulignement dans un nom d'hôte et ne lui ajoutez pas de nom de domaine. Remarque : Le nom d'hôte ne peut pas dépasser 15 caractères.
ROOT_PASSWORD	<i>nouveau mot de passe root</i>	Créez et confirmez un nouveau mot de passe root pour ce serveur.
IP_ADDRESS	<i>Adresse IPv4 correspondante</i>	Entrez une adresse IP valide pour ce serveur.
SUBNET_MASK	<i>Adresse IP correspondante</i>	Entrez un masque de sous-réseau valide à utiliser avec ce serveur.
DEFAULT_GATEWAY	<i>Adresse IP correspondante</i>	Entrez un masque de sous-réseau valide et une passerelle par défaut à utiliser avec ce serveur.
DNS_SERVERS	<i>Adresses IPv4 correspondantes</i>	Entrez une ou plusieurs adresses IP de serveur DNS à utiliser sur votre réseau. La liste est séparée par des virgules, sans espace entre les entrées. Si vos serveurs DNS utilisent l'adressage IPv6, entrez ces adresses avec ce format.
DOMAIN_NAME	<i>votre nom de domaine</i>	Entrez le nom de domaine complet au sein duquel opère le serveur, par exemple mycompany.com. Remarque : Le nom de domaine doit être enregistré auprès du serveur DNS (Domain Name Server) de votre réseau pour permettre la résolution du nom d'hôte vers l'adresse IP.
acceptAllEulas	Accepter	Acceptez le contrat de licence de CA pour poursuivre le provisionnement du serveur CA Enterprise Log Manager.

Informations requises	Valeur	Commentaires
deploymentOption	moyen ou grand	Si vous sélectionnez Moyenne, VMware indique 4 UC de 8 Go de mémoire RAM chacune. Si vous sélectionnez Large, VMware indique huit UC de 8 Go de mémoire RAM chacune.
TIMEZONE	<i>le fuseau horaire que vous souhaitez</i>	Sélectionnez le fuseau horaire dont dépend ce serveur.
Paramètres spécifiques aux applications		
LOCAL_REMOTE_EEM	Local pour le premier serveur installé (serveur de gestion) Distant pour chaque serveur supplémentaire	Indiquez si vous prévoyez d'utiliser un serveur CA EEM local ou distant. Pour un serveur CA Enterprise Log Manager de gestion, choisissez l'option locale. L'installation vous invite à créer un mot de passe pour le compte d'utilisateur EiamAdmin par défaut. Pour chaque serveur supplémentaire, choisissez l'option distante. L'installation vous invite à indiquer le nom du serveur de gestion. Que vous choisissiez l'option locale ou distante, vous devez utiliser l'ID et le mot de passe du compte EiamAdmin lors de la première connexion à chaque serveur CA Enterprise Log Manager.
REMOTE_EEM_LOCATION	<i>adresse IP ou nom d'hôte</i>	Entrez cette valeur uniquement si vous sélectionnez l'option de serveur distant. Entrez l'adresse IP ou le nom d'hôte du serveur CA Enterprise Log Manager de gestion installé en premier. Le nom d'hôte doit être enregistré auprès du serveur DNS. Si vous voulez utiliser un serveur CA EEM local, la valeur par défaut n'est Aucun .

Informations requises	Valeur	Commentaires
EEM_PASSWORD	<i>mot de passe du compte EiamAdmin</i>	<p>Enregistrez le mot de passe du compte d'administrateur par défaut, EiamAdmin.</p> <p>Votre serveur CA Enterprise Log Manager doit disposer de ces informations d'identification de compte pour la connexion initiale.</p> <p>Si vous installez le serveur de gestion, vous créez et confirmez ici un nouveau mot de passe EiamAdmin.</p> <p>Notez ce mot de passe, car vous l'utiliserez à nouveau lors de l'installation d'autres serveurs et agents CA Enterprise Log Manager.</p> <p>Remarque : Le mot de passe entré ici est également le mot de passe initial du compte caelmadmin par défaut, que vous utiliserez pour accéder directement au serveur CA Enterprise Log Manager via ssh.</p> <p>Si vous le souhaitez, vous pouvez créer d'autres comptes d'administrateur pour accéder aux fonctions CA EEM après l'installation.</p>
FIPS_MODE	Oui ou Non	<p>Spécifie si le dispositif virtuel doit être exécuté en mode FIPS ou non. Si vous choisissez un serveur CA EEM local, choisissez le mode de votre choix. Si vous choisissez un serveur CA EEM distant, choisissez le mode utilisé par ce serveur.</p>

Informations complémentaires :

[Ajout de serveurs virtuels à votre environnement](#) (page 341)

[Création d'un environnement complètement virtuel](#) (page 365)

[Déploiement rapide de serveurs virtuels](#) (page 391)

Appel de l'outil OVF à partir d'une ligne de commande

Remarque : Avant d'effectuer l'installation silencieuse, installez l'outil OVF 1.0.0.0. Pour plus d'informations sur l'outil OVF, consultez le manuel *VMware's OVF Tool User Guide* ou visitez le site Web www.vmware.com.

Vous devez transférer les paramètres de configuration en tant qu'arguments de ligne de commande pour appeler l'outil OVF.

Remarque : Nous vous recommandons vivement d'utiliser une configuration de déploiement moyenne pour effectuer le provisionnement d'un serveur de collecte, mais une configuration de déploiement grande pour le provisionnement d'un serveur de gestion ou de génération de rapports. Nous vous recommandons également d'utiliser la méthode de déploiement lourd comme indiqué dans la documentation VMware.

Pour appeler l'outil OVF à partir d'une ligne de commande :

1. Ouvrez l'invite de commande sur l'ordinateur où le client VMware vSphere est installé.
2. Exécutez la commande suivante pour appeler l'outil OVF :

```
ovftool -dm=thick --acceptAllEulas --name=value --deploymentOption=value --  
prop:ROOT_PASSWORD=value --prop:LOCAL_REMOTE_EEM=value --  
prop:REMOTE_EEM_LOCATION=value --prop:EEM_PASSWORD=value --  
prop:FIPS_MODE=value --prop:IP_ADDRESS=value --prop:SUBNET_MASK=value --  
prop:HOSTNAME=value --prop:DEFAULT_GATEWAY=value --prop:DNS_SERVERS=value --  
prop:DOMAIN_NAME=value --prop:TIMEZONE=value <OVF_Name.ovf>  
vi://username:password@hostname_of_VMware_vSphere_Client/Datacenter/host/host  
name
```

Le message Opening VI target (Cible VI en cours d'ouverture) s'affiche. Le statut de déploiement du serveur CA Enterprise Log Manager s'affiche. Si l'installation s'est correctement effectuée, le serveur CA Enterprise Log Manager figurera sous le magasin de données sélectionné dans le volet gauche.

Remarque : Si une valeur de propriété contient des espaces, placez-la entre apostrophes doubles ("). Par exemple, si le nom OVF est CA ELM, entrez la valeur comme suit : "CA ELM.ovf". Pour plus d'informations sur l'outil OVF, consultez le Manuel de l'Utilisateur *OVF Tool User Guide*.

Exemple

```
ovftool -dm=thick --acceptAllEulas --name="example_server" --  
deploymentOption=medium --prop:ROOT_PASSWORD="example_password" --  
prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none --  
prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.0.0 --  
prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_server1" --  
prop:DEFAULT_GATEWAY=198,168.0,0 --prop:DNS_SERVERS=198.168.10.20.198.168.10.25 -  
-prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA  
ELM\CA Enterprise Log Manager.ovf"  
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0  
"
```

Définition des paramètres de paravirtualisation et de ressources

Après l'importation du modèle OVF, définissez manuellement les paramètres de paravirtualisation et de ressource pour améliorer les performances du serveur CA Enterprise Log Manager provisionné.

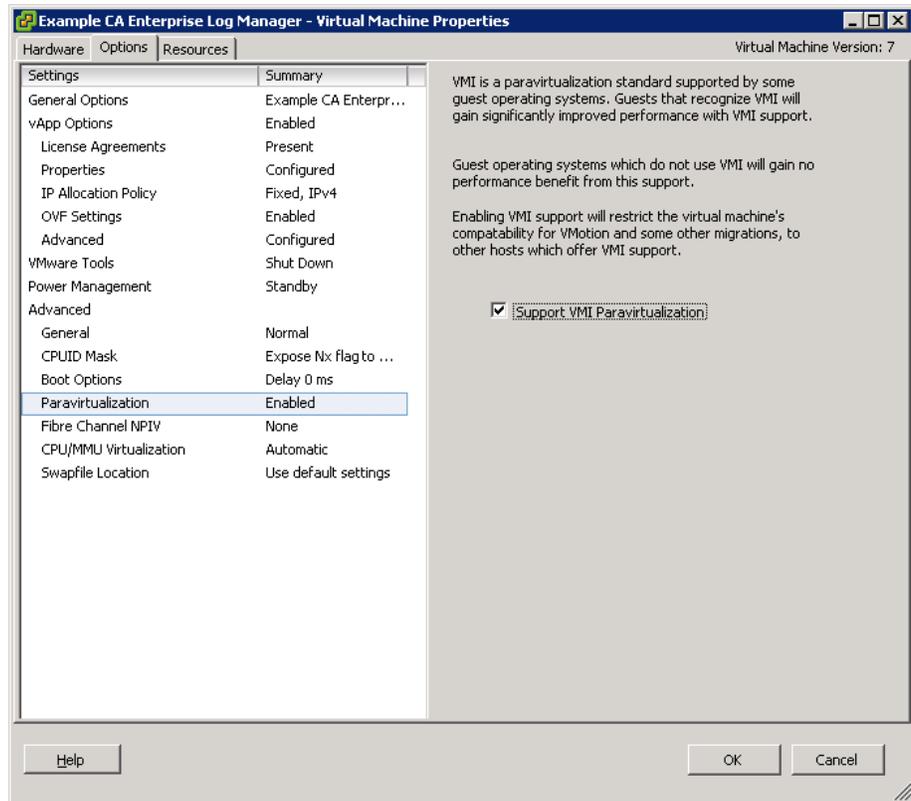
Remarque : Vérifiez que le lecteur de CD/DVD est défini sur (Client Device) Unités du client.

Pour définir les paramètres de paravirtualisation et de ressources :

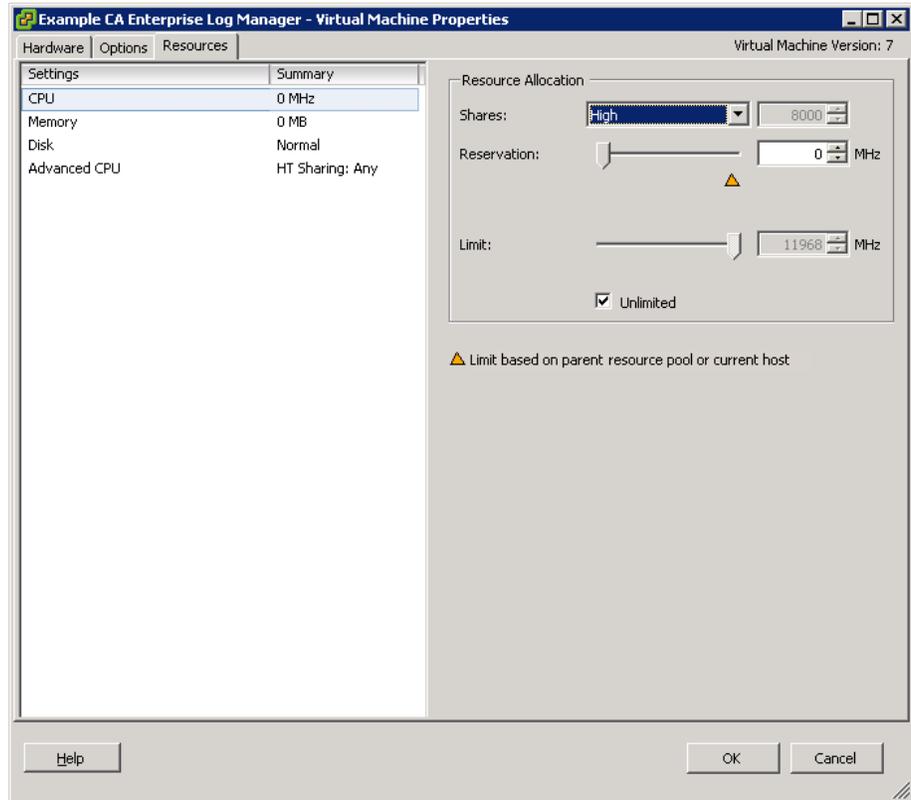
1. Cliquez avec le bouton droit de la souris sur le nouveau dispositif virtuel CA Enterprise Log Manager situé dans le volet gauche et cliquez sur Edit Settings (Modifier les paramètres).

La fenêtre <CA Enterprise Log Manager Virtual Appliance name> - Virtual Machine Properties (Propriétés de l'ordinateur virtuel <CA Enterprise Log Manager nom application virtuelle> s'affiche.

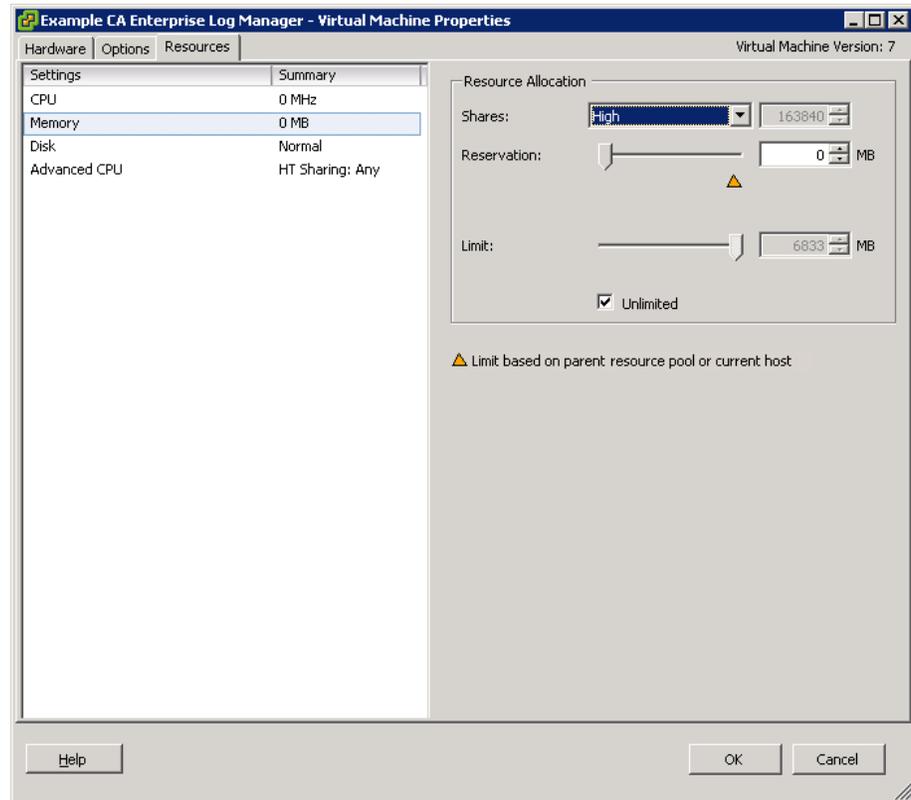
2. Cliquez sur l'onglet Option dans la fenêtre.
3. Sélectionnez le paramètre Paravirtualization situé dans le volet gauche, puis l'option Support VMI Paravirtualization (Prise en charge de la paravirtualization VMI) située dans le volet droit.



4. Cliquez sur l'onglet Resources (Ressources) dans la fenêtre.
5. Sélectionnez l'option CPU (UC) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



6. Sélectionnez l'option Memory (Mémoire) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



7. Cliquez sur OK.
8. **Remarque** : Pour plus d'informations sur la paravirtualization, visitez le site Web www.vmware.com.

Démarrez le serveur CA Enterprise Log Manager provisionné.

Ceci est nécessaire à son exécution.

Pour démarrer un serveur CA Enterprise Log Manager :

1. Sélectionnez le nouveau serveur CA Enterprise Log Manager dans le volet gauche de la fenêtre de l'application VMware.
2. Cliquez sur l'option Power On (Démarrage) située sous l'onglet Basic Tasks of the Getting Started (Tâches de base du démarrage) dans le volet droit.

Le serveur CA Enterprise Log Manager est démarré.

Remarque : Vérifiez qu'un serveur CA Enterprise Log Manager principal est exécuté avant de démarrer un serveur CA Enterprise Log Manager secondaire.

Vérification de l'installation d'un serveur CA Enterprise Log Manager virtuel

Lors du démarrage du serveur CA Enterprise Log Manager provisionné, une URL permettant d'accéder à CA Enterprise Log Manager s'affiche dans l'onglet Console de la fenêtre Client VMware vSphere. Utilisez cette URL et les informations d'identification par défaut suivantes pour accéder à CA Enterprise Log Manager :

Nom de l'utilisateur par défaut : EiamAdmin

Mot de passe par défaut : mot de passe saisi lors de la procédure d'installation du serveur CA Enterprise Log Manager

Informations complémentaires :

[Ajout de serveurs virtuels à votre environnement](#) (page 341)

[Création d'un environnement complètement virtuel](#) (page 365)

[Déploiement rapide de serveurs virtuels](#) (page 391)

Création d'un environnement complètement virtuel

Si vous n'avez pas encore implémenté un environnement CA Enterprise Log Manager, vous pouvez créer un environnement entièrement virtuel de collecte de journaux. Ce scénario suppose de disposer d'un nombre suffisant de serveurs physiques disponibles, tous dotés d'un groupe de quatre processeurs au minimum, pour installer chacun des serveurs CA Enterprise Log Manager souhaités.

Installez un serveur CA Enterprise Log Manager comme serveur de gestion. Lors de la configuration, n'envoyez pas les journaux d'événements à ce serveur et ne l'utilisez pas pour générer des rapports. En configurant ainsi votre environnement, vous conservez le débit de collecte des journaux d'événements requis par la production d'une entreprise.

En général, vous installez deux serveurs CA Enterprise Log Manager dotés de quatre processeurs en lieu et place de chacun des serveurs de dispositifs normalement installés en cas d'utilisation de matériel certifié (les serveurs de dispositifs comptent huit processeurs au minimum).

Le processus suivi pour créer un dispositif virtuel comprend les procédures ci-après.

1. Téléchargez le package de dispositif virtuel.
2. Installez un serveur virtuel CA Enterprise Log Manager pour disposer des fonctions de gestion.
3. Installez un ou plusieurs serveurs virtuels pour la collecte et la génération de rapports.
4. Configurez les serveurs virtuels conformément à la section sur l'installation d'un serveur CA Enterprise Log Manager.

Important : Si vous voulez effectuer le provisionnement d'un serveur CA Enterprise Log Manager à l'aide du dispositif virtuel, le nom d'instance d'application du serveur CA Enterprise Log Manager principal doit être CAELM.

Téléchargez le package de dispositif virtuel.

L'image de distribution du dispositif virtuel de CA Enterprise Log Manager est disponible à partir du support en ligne du lien de téléchargement. Vous devez télécharger cinq fichiers :

- Le fichier Manifest
- Le fichier .ovf
- Trois fichiers de disque virtuel

Installation manuelle d'un serveur CALM

Lors de l'installation manuelle du dispositif virtuel, effectuez les tâches suivantes :

1. Déployez un modèle OVF.
2. Définissez les paramètres Paravirtualization et Resource.
3. Démarrez le serveur CA Enterprise Log Manager provisionné.

Déploiement d'un modèle OVF

Vous pouvez spécifier les propriétés du dispositif virtuel dans un modèle OVF. VMware utilise ce modèle pour effectuer le provisionnement d'un serveur CA Enterprise Log Manager. Utilisez le Client VMware vSphere pour déployer le modèle OVF.

Remarque : Les captures d'écran qui figurent dans les procédures suivantes contiennent des exemples de données à titre indicatif. Ces captures d'écran concernent le Client VMware vSphere 4.0.0. Nous vous recommandons de spécifier des données propres à votre environnement.

Pour déployer un modèle OVF :

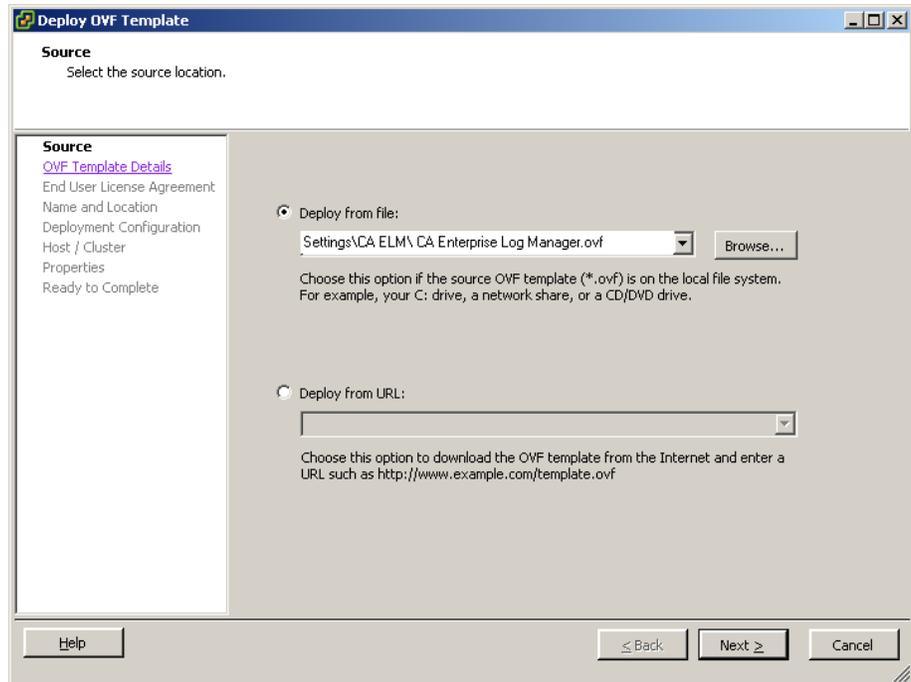
1. Cliquez sur Démarrer, Tous les programmes, Client VMware vSphere sur l'ordinateur où le Client VMware vSphere est installé.
La boîte de dialogue VMware vSphere Client s'ouvre.
2. Dans le champ IP address/Name (Adresse IP/Nom), saisissez l'adresse IP ou le nom d'hôte du serveur VMware vSphere auquel vous souhaitez vous connecter.
3. Entrez les informations d'identification dans les champs User name (nom d'utilisateur) et Password (mot de passe).
4. Cliquez sur Logon (connexion).
La fenêtre de l'application s'ouvre.
5. Sélectionnez l'emplacement où vous voulez effectuer le provisionnement d'un serveur CA Enterprise Log Manager sous un centre de données dans le volet gauche.
6. Cliquez sur File (Fichier), puis sur Deploy OVF Template (Déployer le modèle OVF).

La fenêtre Deploy OVF Template (Déployer le modèle OVF) s'affiche. Par défaut, cette fenêtre affiche la page Source. Saisissez l'emplacement du modèle OVF dans cette page.

Remarque : Les pages affichées dans la fenêtre Deploy OVF Template peuvent varier selon la version de Client VMware vSphere et des paramètres utilisés. Pour plus d'informations sur le déploiement d'un modèle OVF, visitez le site Web www.vmware.com.

7. Sélectionnez l'option Deploy from file (Déployer à partir du fichier) et cliquez sur Parcourir pour sélectionner l'emplacement du modèle OVF.
8. Accédez à l'emplacement du modèle OVF à partir de la boîte de dialogue Open (Ouvrir), sélectionnez le modèle OVF et cliquez sur Open.

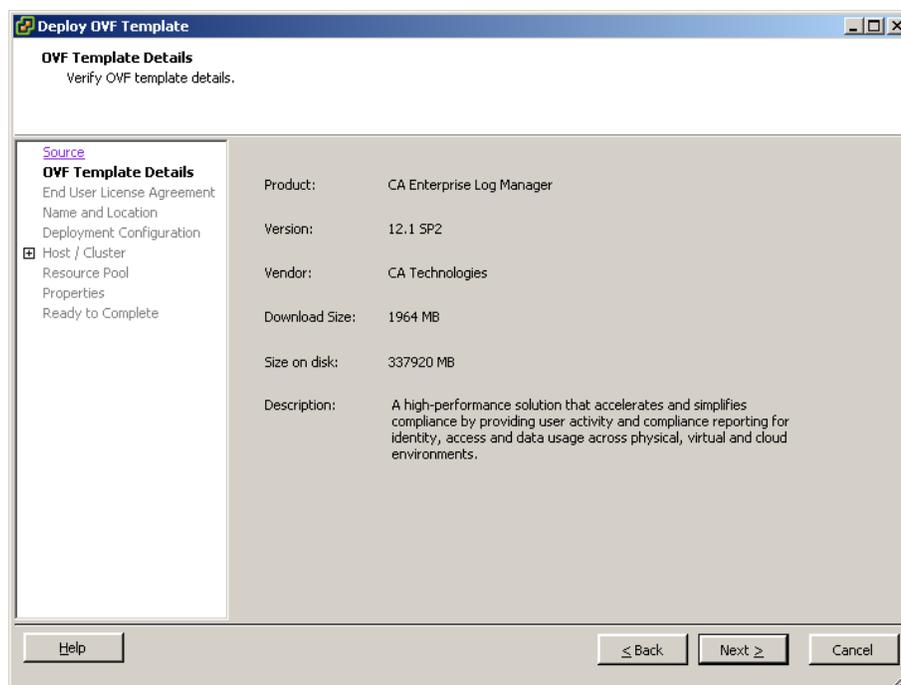
Le chemin d'accès de l'emplacement du modèle OVF s'affiche dans le champ Deploy from file (Déployer à partir du fichier).



9. Cliquez sur Suivant.

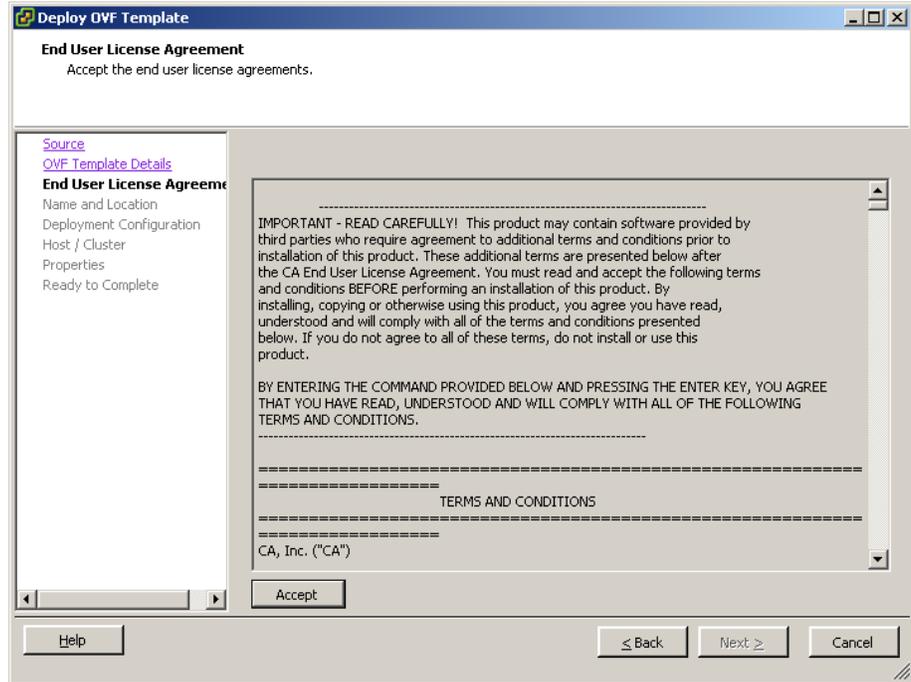
La page OVF Template Details (Informations du modèle OVF) s'ouvre. Cette page contient les informations stockées dans le modèle OVF, tels que la taille de téléchargement, la taille de disque disponible et le nom des fournisseurs.

10. Vérifiez que le serveur VMware dispose de 350 Go minimum d'espace disque, puis cliquez sur Suivant.



La page End User License Agreement (Contrat de licence de l'utilisateur final) s'affiche. Cette page contient le contrat de licence de produits tiers. Vous devez accepter ce contrat de licence pour installer CA Enterprise Log Manager.

11. Lisez le contrat de licence.

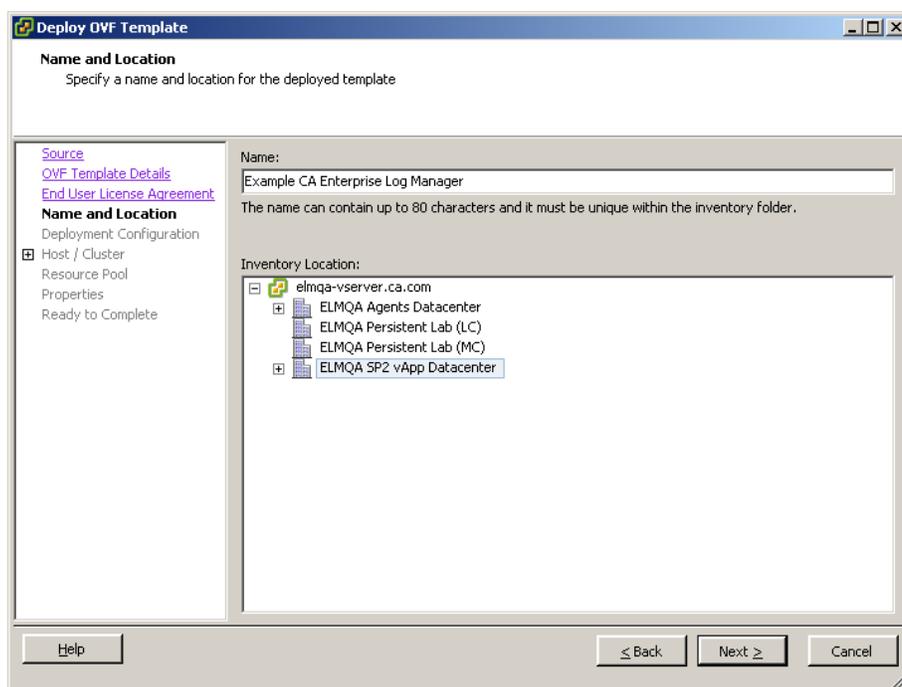


12. Cliquez sur Accept (Accepter), puis sur Suivant.

La page Name and Location (Nom et emplacement) s'ouvre. Elle permet d'ajouter un nom pour identifier le serveur CA Enterprise Log Manager et de spécifier le centre de données où vous voulez effectuer le provisionnement de ce serveur.

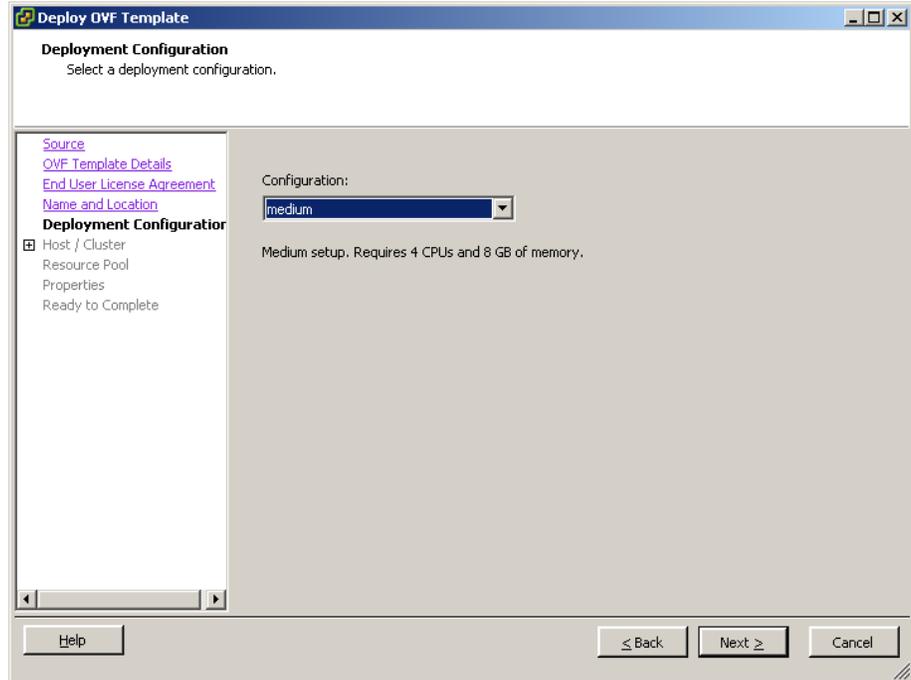
13. Saisissez le nom du serveur CA Enterprise Log Manager dans le champ Nom, sélectionnez le centre de données dans la liste Inventory Location (Emplacement de l'inventaire), puis cliquez sur Suivant.

Remarque : Par défaut, le nom spécifié dans le modèle OVF s'affiche dans le champ Nom.



La page Deployment Configuration (Configuration du déploiement) s'affiche. Elle permet de spécifier le mode de configuration du serveur CA Enterprise Log Manager pour lequel vous voulez effectuer le provisionnement.

14. Dans la liste déroulante Configuration, sélectionnez Moyenne ou Grande, puis cliquez sur Suivant.

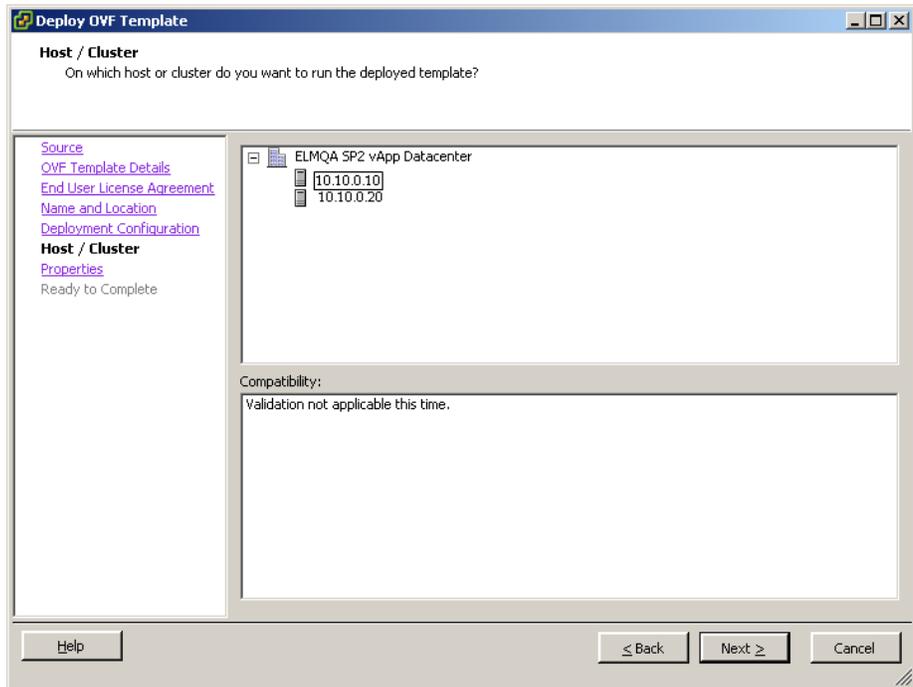


Si vous sélectionnez Moyenne, VMware indique 4 UC de 8 Go de mémoire RAM chacune. Si vous sélectionnez Large, VMware indique huit UC de 8 Go de mémoire RAM chacune.

Remarque : Nous vous recommandons vivement d'utiliser une configuration de déploiement moyenne pour effectuer le provisionnement d'un serveur de collecte, mais une configuration de déploiement importante pour le provisionnement d'un serveur de gestion ou de génération de rapports.

La page Host / Cluster (Hôte / Cluster) s'ouvre. Elle s'affiche uniquement si vous n'avez pas sélectionné le pool de ressources avant l'importation du modèle OVF. Cette page contient le centre de données sélectionné et ses clusters disponibles. Spécifiez l'emplacement des clusters sous le centre de données où vous voulez effectuer le provisionnement du serveur CA Enterprise Log Manager.

15. Sélectionnez un cluster sous le centre de données, puis cliquez sur Suivant.



La page Propriétés (Propriétés)s'ouvre. Cette page contient les paramètres de l'hôte et de CA Enterprise Log Manager.

16. Indiquez des valeurs dans chaque champ relatives aux informations collectées dans la feuille de calcul Installation, puis cliquez sur Suivant.

Deploy OVF Template

Properties
Customize the software solution for this deployment.

Source
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Host / Cluster](#)
Properties
Ready to Complete

A. Host Name
Enter name of this host machine.
examplecaelm

B. Root Password
Enter root password of this machine.
examplerootpassword

C. IP Address
Enter IP address of this machine.
172.160.0.0

D. Subnet Mask
Enter the subnet mask.
10.0.0.0

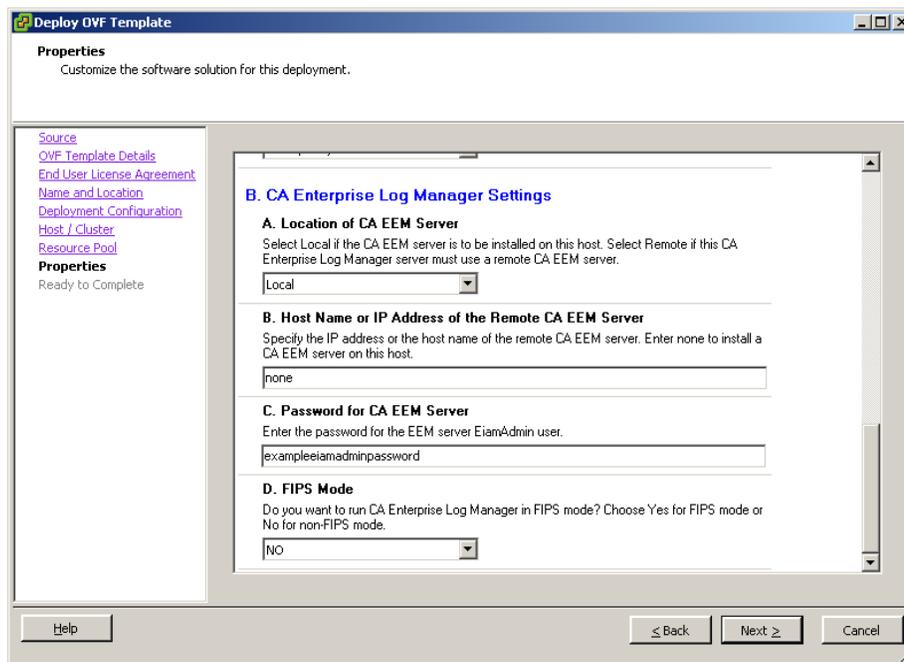
E. Default Gateway
Enter the IP address of the default gateway.
198.168.0.0

F. DNS Servers
Enter a list of the IP addresses for your DNS servers. Use a comma to separate the IP addresses of the DNS servers.
198.168.10.20, 198.168.10.25

G. Domain Name
Enter the domain name of this machine.
example.com

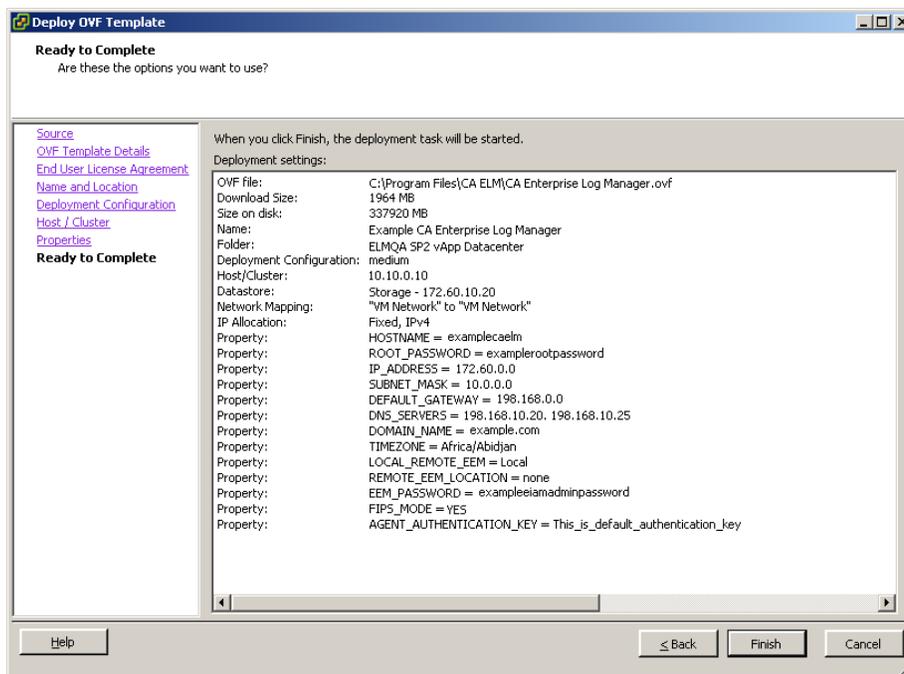
H. Time Zone
Choose the time zone.
Africa/Abidjan

Help < Back Next > Cancel



Le Ready to Complete (Prêt pour la finalisation) s'ouvre. Cette page contient un récapitulatif des informations indiquées aux pages précédentes.

17. Vérifiez ces informations, puis cliquez sur Finish (Terminer).



Le message Opening VI target (Cible VI en cours d'ouverture) s'affiche. Le statut de déploiement du dispositif virtuel s'affiche. Si l'installation s'est correctement effectuée, le dispositif virtuel figurera sous le magasin de données sélectionné dans le volet gauche.

18. (Facultatif) Si vous voulez modifier les informations saisies, procédez comme suit :
 - a. Cliquez sur Précédent dans la fenêtre Deploy OVF Model jusqu'à accéder à la page correspondante.
 - b. Effectuez les modifications nécessaires.
 - c. Cliquez plusieurs fois sur Suivant dans la fenêtre Deploy OVF jusqu'à accéder à la page Ready to Complete.

Définition des paramètres de paravirtualisation et de ressources

Après l'importation du modèle OVF, définissez manuellement les paramètres de paravirtualisation et de ressource pour améliorer les performances du serveur CA Enterprise Log Manager provisionné.

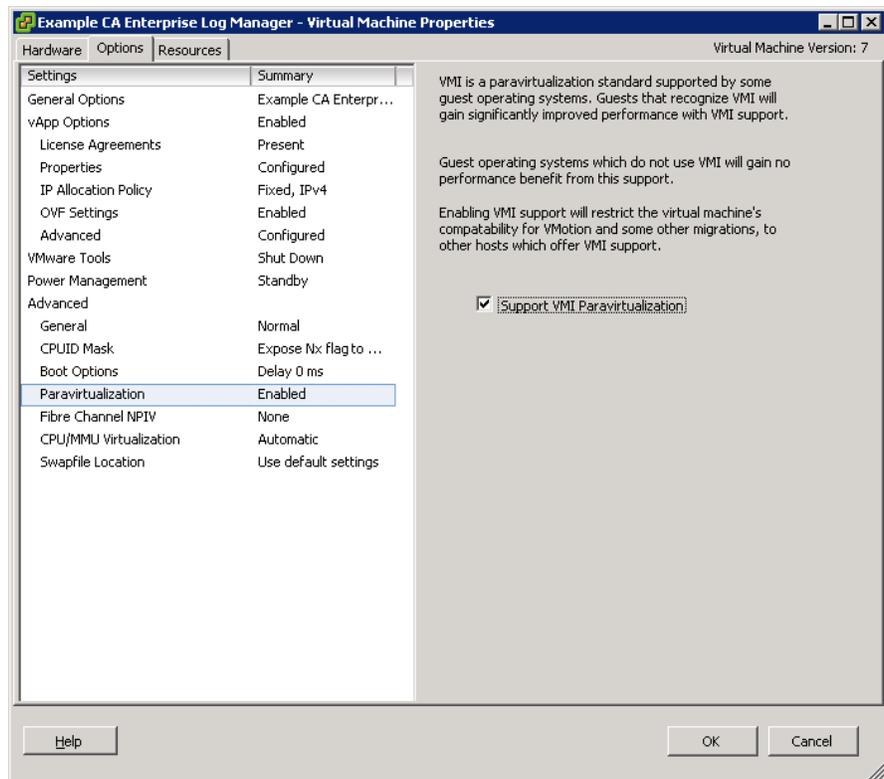
Remarque : Vérifiez que le lecteur de CD/DVD est défini sur (Client Device) Unités du client.

Pour définir les paramètres de paravirtualisation et de ressources :

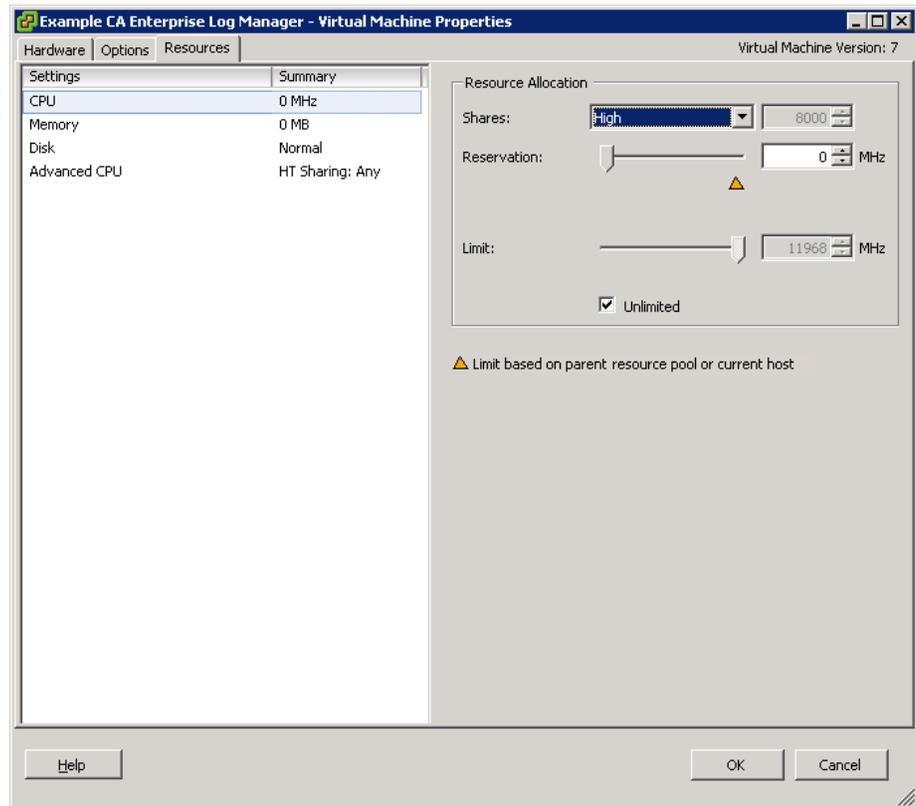
1. Cliquez avec le bouton droit de la souris sur le nouveau dispositif virtuel CA Enterprise Log Manager situé dans le volet gauche et cliquez sur Edit Settings (Modifier les paramètres).

La fenêtre <CA Enterprise Log Manager Virtual Appliance name> - Virtual Machine Properties (Propriétés de l'ordinateur virtuel <CA Enterprise Log Manager nom application virtuelle> s'affiche.

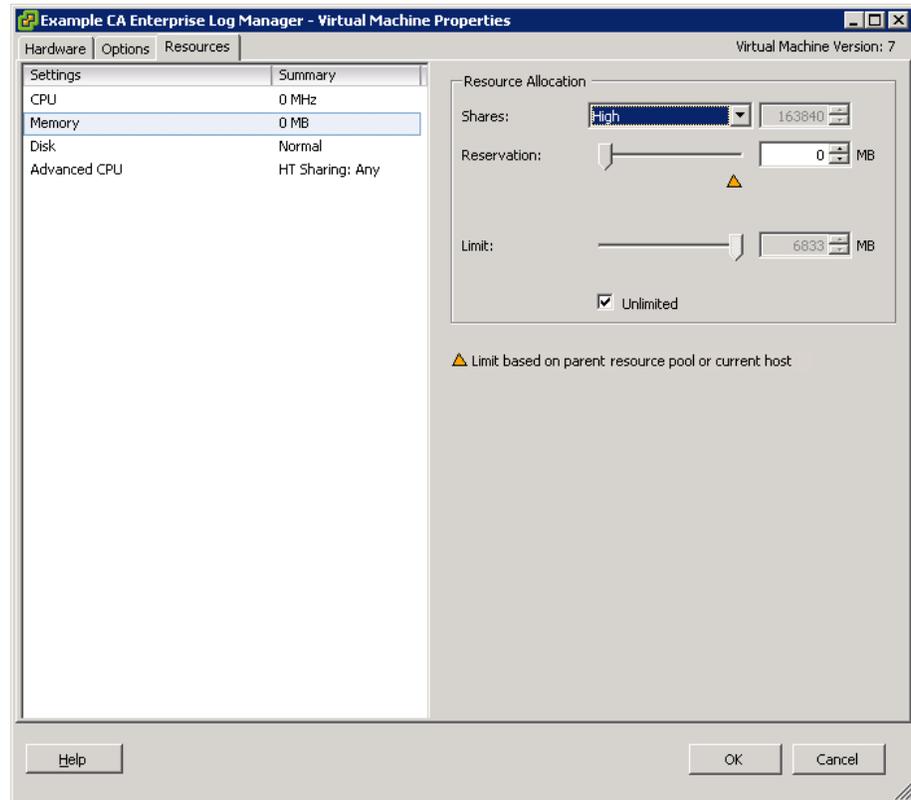
2. Cliquez sur l'onglet Option dans la fenêtre.
3. Sélectionnez le paramètre Paravirtualization situé dans le volet gauche, puis l'option Support VMI Paravirtualization (Prise en charge de la paravirtualization VMI) située dans le volet droit.



4. Cliquez sur l'onglet Resources (Ressources) dans la fenêtre.
5. Sélectionnez l'option CPU (UC) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



6. Sélectionnez l'option Memory (Mémoire) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



7. Cliquez sur OK.
8. **Remarque** : Pour plus d'informations sur la paravirtualization, visitez le site Web www.vmware.com.

Démarrez le serveur CA Enterprise Log Manager provisionné.

Ceci est nécessaire à son exécution.

Pour démarrer un serveur CA Enterprise Log Manager :

1. Sélectionnez le nouveau serveur CA Enterprise Log Manager dans le volet gauche de la fenêtre de l'application VMware.
2. Cliquez sur l'option Power On (Démarrage) située sous l'onglet Basic Tasks of the Getting Started (Tâches de base du démarrage) dans le volet droit.

Le serveur CA Enterprise Log Manager est démarré.

Remarque : Vérifiez qu'un serveur CA Enterprise Log Manager principal est exécuté avant de démarrer un serveur CA Enterprise Log Manager secondaire.

Installation silencieuse d'un serveur CA Enterprise Log Manager :

Lors de l'installation silencieuse du dispositif virtuel, effectuez les tâches suivantes :

1. Appelez l'outil OVF.
2. Définissez les paramètres de paravirtualisation et ressources.
3. Démarrez le serveur CA Enterprise Log Manager provisionné.

Le tableau suivant décrit les paramètres utilisés pour le déploiement de CA Enterprise Log Manager à l'aide de l'outil OVF. Vous devez spécifier ces paramètres en tant qu'arguments de ligne de commande dans la ligne de commande.

Informations requises	Valeur	Commentaires
Paramètres spécifiques aux hôtes		

Informations requises	Valeur	Commentaires
HOSTNAME	<i>Nom d'hôte pour ce serveur CA Enterprise Log Manager</i> Exemple : CA-ELM1	Spécifiez le nom d'hôte de ce serveur en utilisant uniquement les caractères pris en charge par les hôtes. Les normes du secteur recommandent les lettres de A à Z (insensibles à la casse), les chiffres de 0 à 9 et le tiret, avec une lettre en premier caractère et un caractère alphanumérique en dernière position. N'utilisez pas le caractère de soulignement dans un nom d'hôte et ne lui ajoutez pas de nom de domaine. Remarque : Le nom d'hôte ne peut pas dépasser 15 caractères.
ROOT_PASSWORD	<i>nouveau mot de passe root</i>	Créez et confirmez un nouveau mot de passe root pour ce serveur.
IP_ADDRESS	<i>Adresse IPv4 correspondante</i>	Entrez une adresse IP valide pour ce serveur.
SUBNET_MASK	<i>Adresse IP correspondante</i>	Entrez un masque de sous-réseau valide à utiliser avec ce serveur.
DEFAULT_GATEWAY	<i>Adresse IP correspondante</i>	Entrez un masque de sous-réseau valide et une passerelle par défaut à utiliser avec ce serveur.
DNS_SERVERS	<i>Adresses IPv4 correspondantes</i>	Entrez une ou plusieurs adresses IP de serveur DNS à utiliser sur votre réseau. La liste est séparée par des virgules, sans espace entre les entrées. Si vos serveurs DNS utilisent l'adressage IPv6, entrez ces adresses avec ce format.
DOMAIN_NAME	<i>votre nom de domaine</i>	Entrez le nom de domaine complet au sein duquel opère le serveur, par exemple mycompany.com. Remarque : Le nom de domaine doit être enregistré auprès du serveur DNS (Domain Name Server) de votre réseau pour permettre la résolution du nom d'hôte vers l'adresse IP.
acceptAllEulas	Accepter	Acceptez le contrat de licence de CA pour poursuivre le provisionnement du serveur CA Enterprise Log Manager.

Informations requises	Valeur	Commentaires
deploymentOption	moyen ou grand	Si vous sélectionnez Moyenne, VMware indique 4 UC de 8 Go de mémoire RAM chacune. Si vous sélectionnez Large, VMware indique huit UC de 8 Go de mémoire RAM chacune.
TIMEZONE	<i>le fuseau horaire que vous souhaitez</i>	Sélectionnez le fuseau horaire dont dépend ce serveur.
Paramètres spécifiques aux applications		
LOCAL_REMOTE_EEM	Local pour le premier serveur installé (serveur de gestion) Distant pour chaque serveur supplémentaire	Indiquez si vous prévoyez d'utiliser un serveur CA EEM local ou distant. Pour un serveur CA Enterprise Log Manager de gestion, choisissez l'option locale. L'installation vous invite à créer un mot de passe pour le compte d'utilisateur EiamAdmin par défaut. Pour chaque serveur supplémentaire, choisissez l'option distante. L'installation vous invite à indiquer le nom du serveur de gestion. Que vous choisissiez l'option locale ou distante, vous devez utiliser l'ID et le mot de passe du compte EiamAdmin lors de la première connexion à chaque serveur CA Enterprise Log Manager.
REMOTE_EEM_LOCATION	<i>adresse IP ou nom d'hôte</i>	Entrez cette valeur uniquement si vous sélectionnez l'option de serveur distant. Entrez l'adresse IP ou le nom d'hôte du serveur CA Enterprise Log Manager de gestion installé en premier. Le nom d'hôte doit être enregistré auprès du serveur DNS. Si vous voulez utiliser un serveur CA EEM local, la valeur par défaut n'est Aucun .

Informations requises	Valeur	Commentaires
EEM_PASSWORD	<i>mot de passe du compte EiamAdmin</i>	<p>Enregistrez le mot de passe du compte d'administrateur par défaut, EiamAdmin.</p> <p>Votre serveur CA Enterprise Log Manager doit disposer de ces informations d'identification de compte pour la connexion initiale.</p> <p>Si vous installez le serveur de gestion, vous créez et confirmez ici un nouveau mot de passe EiamAdmin.</p> <p>Notez ce mot de passe, car vous l'utiliserez à nouveau lors de l'installation d'autres serveurs et agents CA Enterprise Log Manager.</p> <p>Remarque : Le mot de passe entré ici est également le mot de passe initial du compte caelmadmin par défaut, que vous utiliserez pour accéder directement au serveur CA Enterprise Log Manager via ssh.</p> <p>Si vous le souhaitez, vous pouvez créer d'autres comptes d'administrateur pour accéder aux fonctions CA EEM après l'installation.</p>
FIPS_MODE	Oui ou Non	<p>Spécifie si le dispositif virtuel doit être exécuté en mode FIPS ou non. Si vous choisissez un serveur CA EEM local, choisissez le mode de votre choix. Si vous choisissez un serveur CA EEM distant, choisissez le mode utilisé par ce serveur.</p>

Informations complémentaires :

[Ajout de serveurs virtuels à votre environnement](#) (page 341)

[Création d'un environnement complètement virtuel](#) (page 365)

[Déploiement rapide de serveurs virtuels](#) (page 391)

Appel de l'outil OVF à partir d'une ligne de commande

Remarque : Avant d'effectuer l'installation silencieuse, installez l'outil OVF 1.0.0.0. Pour plus d'informations sur l'outil OVF, consultez le manuel *VMware's OVF Tool User Guide* ou visitez le site Web www.vmware.com.

Vous devez transférer les paramètres de configuration en tant qu'arguments de ligne de commande pour appeler l'outil OVF.

Remarque : Nous vous recommandons vivement d'utiliser une configuration de déploiement moyenne pour effectuer le provisionnement d'un serveur de collecte, mais une configuration de déploiement grande pour le provisionnement d'un serveur de gestion ou de génération de rapports. Nous vous recommandons également d'utiliser la méthode de déploiement lourd comme indiqué dans la documentation VMware.

Pour appeler l'outil OVF à partir d'une ligne de commande :

1. Ouvrez l'invite de commande sur l'ordinateur où le client VMware vSphere est installé.
2. Exécutez la commande suivante pour appeler l'outil OVF :

```
ovftool -dm=thick --acceptAllEulas --name=value --deploymentOption=value --  
prop:ROOT_PASSWORD=value --prop:LOCAL_REMOTE_EEM=value --  
prop:REMOTE_EEM_LOCATION=value --prop:EEM_PASSWORD=value --  
prop:FIPS_MODE=value --prop:IP_ADDRESS=value --prop:SUBNET_MASK=value --  
prop:HOSTNAME=value --prop:DEFAULT_GATEWAY=value --prop:DNS_SERVERS=value --  
prop:DOMAIN_NAME=value --prop:TIMEZONE=value <OVF_Name.ovf>  
vi://username:password@hostname_of_VMware_vSphere_Client/Datacenter/host/host  
name
```

Le message Opening VI target (Cible VI en cours d'ouverture) s'affiche. Le statut de déploiement du serveur CA Enterprise Log Manager s'affiche. Si l'installation s'est correctement effectuée, le serveur CA Enterprise Log Manager figurera sous le magasin de données sélectionné dans le volet gauche.

Remarque : Si une valeur de propriété contient des espaces, placez-la entre apostrophes doubles (""). Par exemple, si le nom OVF est CA ELM, entrez la valeur comme suit : "CA ELM.ovf". Pour plus d'informations sur l'outil OVF, consultez le Manuel de l'Utilisateur *OVF Tool User Guide*.

Exemple

```
ovftool -dm=thick --acceptAllEulas --name="example_server" --  
deploymentOption=medium --prop:ROOT_PASSWORD="example_password" --  
prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none --  
prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.0.0 --  
prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_server1" --  
prop:DEFAULT_GATEWAY=198,168.0,0 --prop:DNS_SERVERS=198.168.10.20.198.168.10.25 -  
-prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA  
ELM\CA Enterprise Log Manager.ovf"  
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0  
"
```

Définition des paramètres de paravirtualisation et de ressources

Après l'importation du modèle OVF, définissez manuellement les paramètres de paravirtualisation et de ressource pour améliorer les performances du serveur CA Enterprise Log Manager provisionné.

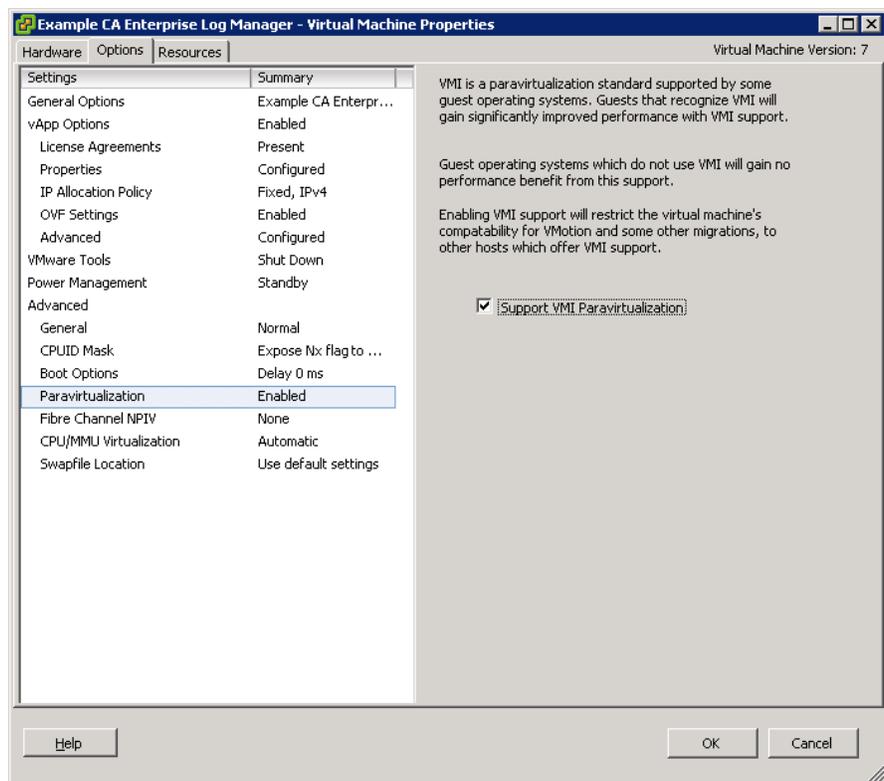
Remarque : Vérifiez que le lecteur de CD/DVD est défini sur (Client Device) Unités du client.

Pour définir les paramètres de paravirtualisation et de ressources :

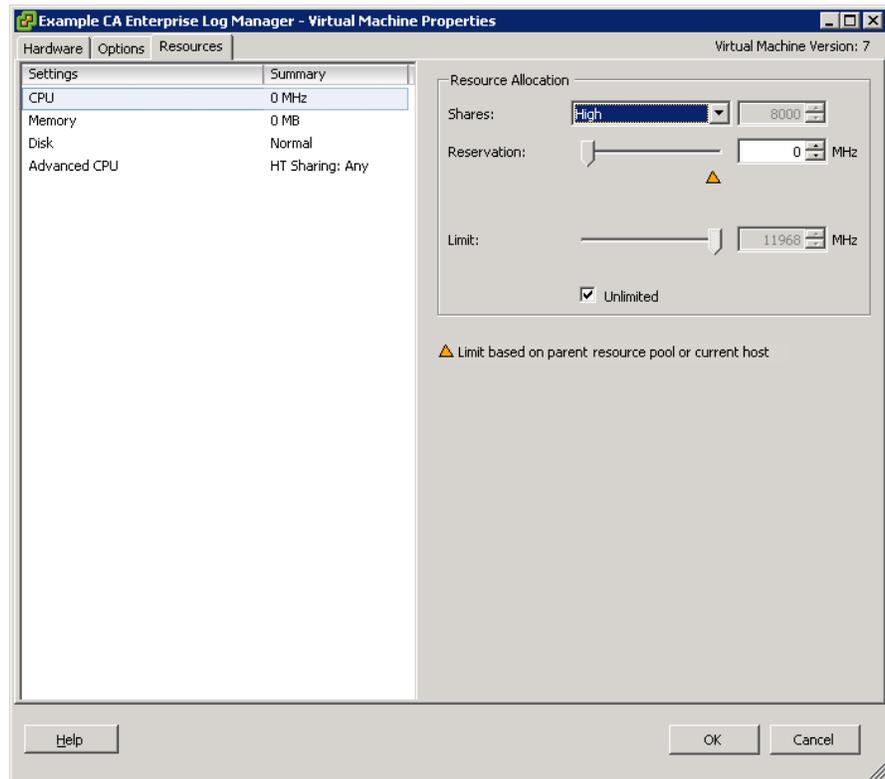
1. Cliquez avec le bouton droit de la souris sur le nouveau dispositif virtuel CA Enterprise Log Manager situé dans le volet gauche et cliquez sur Edit Settings (Modifier les paramètres).

La fenêtre <CA Enterprise Log Manager Virtual Appliance name> - Virtual Machine Properties (Propriétés de l'ordinateur virtuel <CA Enterprise Log Manager nom application virtuelle> s'affiche.

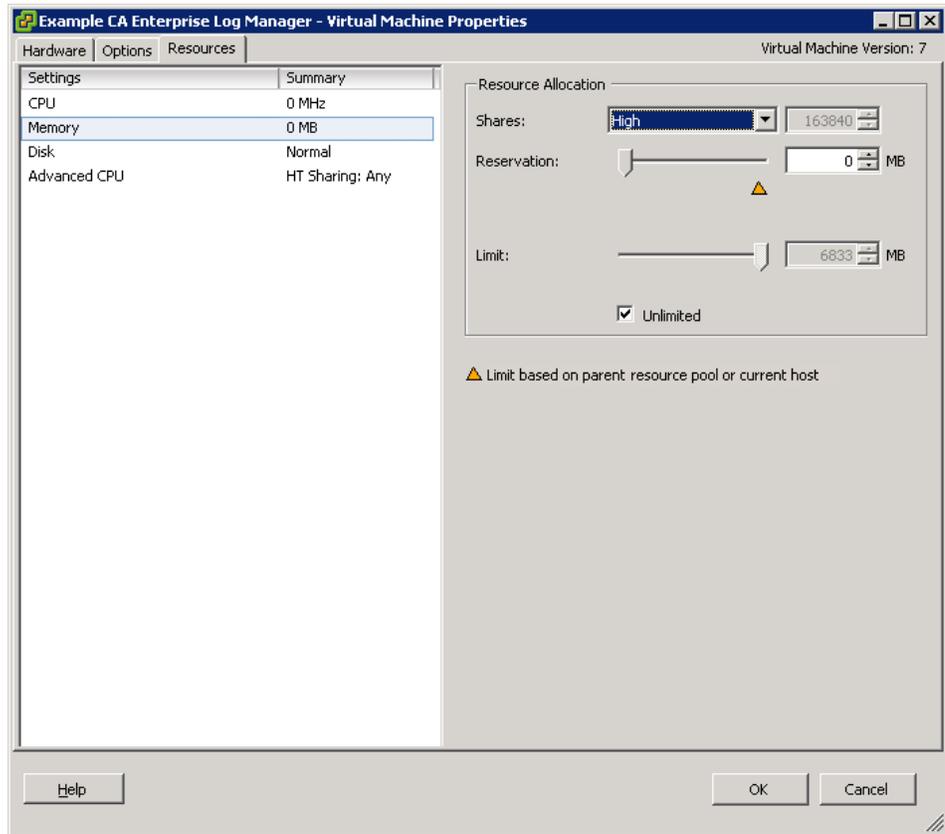
2. Cliquez sur l'onglet Option dans la fenêtre.
3. Sélectionnez le paramètre Paravirtualization situé dans le volet gauche, puis l'option Support VMI Paravirtualization (Prise en charge de la paravirtualization VMI) située dans le volet droit.



4. Cliquez sur l'onglet Resources (Ressources) dans la fenêtre.
5. Sélectionnez l'option CPU (UC) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



- Sélectionnez l'option Memory (Mémoire) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



- Cliquez sur OK.
- Remarque :** Pour plus d'informations sur la paravirtualization, visitez le site Web www.vmware.com.

Démarrez le serveur CA Enterprise Log Manager provisionné.

Ceci est nécessaire à son exécution.

Pour démarrer un serveur CA Enterprise Log Manager :

1. Sélectionnez le nouveau serveur CA Enterprise Log Manager dans le volet gauche de la fenêtre de l'application VMware.
2. Cliquez sur l'option Power On (Démarrage) située sous l'onglet Basic Tasks of the Getting Started (Tâches de base du démarrage) dans le volet droit.

Le serveur CA Enterprise Log Manager est démarré.

Remarque : Vérifiez qu'un serveur CA Enterprise Log Manager principal est exécuté avant de démarrer un serveur CA Enterprise Log Manager secondaire.

Vérification de l'installation d'un serveur CA Enterprise Log Manager virtuel

Lors du démarrage du serveur CA Enterprise Log Manager provisionné, une URL permettant d'accéder à CA Enterprise Log Manager s'affiche dans l'onglet Console de la fenêtre Client VMware vSphere. Utilisez cette URL et les informations d'identification par défaut suivantes pour accéder à CA Enterprise Log Manager :

Nom de l'utilisateur par défaut : EiamAdmin

Mot de passe par défaut : mot de passe saisi lors de la procédure d'installation du serveur CA Enterprise Log Manager

Informations complémentaires :

[Ajout de serveurs virtuels à votre environnement](#) (page 341)

[Création d'un environnement complètement virtuel](#) (page 365)

[Déploiement rapide de serveurs virtuels](#) (page 391)

Déploiement rapide de serveurs virtuels

La procédure de déploiement rapide d'un serveur CA Enterprise Log Manager virtuel à des fins de collecte comporte les étapes ci-après.

1. Téléchargez le package de dispositif virtuel CA Enterprise Log Manager.
2. Effectuez une installation silencieuse d'un serveur CA Enterprise Log Manager.
3. Configurez les serveurs virtuels conformément à la section sur l'installation d'un serveur CA Enterprise Log Manager.

Important : Si vous voulez effectuer le provisionnement d'un serveur CA Enterprise Log Manager à l'aide du dispositif virtuel, le nom d'instance d'application du serveur CA Enterprise Log Manager principal doit être CAELM.

Téléchargez le package de dispositif virtuel.

L'image de distribution du dispositif virtuel de CA Enterprise Log Manager est disponible à partir du support en ligne du liens de téléchargement. Vous devez télécharger cinq fichiers :

- Le fichier Manifest
- Le fichier .ovf
- Trois fichiers de disque virtuel

Installation silencieuse d'un serveur CA Enterprise Log Manager :

Lors de l'installation silencieuse du dispositif virtuel, effectuez les tâches suivantes :

1. Appelez l'outil OVF.
2. Définissez les paramètres de paravirtualisation et ressources.
3. Démarrez le serveur CA Enterprise Log Manager provisionné.

Le tableau suivant décrit les paramètres utilisés pour le déploiement de CA Enterprise Log Manager à l'aide de l'outil OVF. Vous devez spécifier ces paramètres en tant qu'arguments de ligne de commande dans la ligne de commande.

Informations requises	Valeur	Commentaires
-----------------------	--------	--------------

Paramètres spécifiques aux hôtes

Informations requises	Valeur	Commentaires
HOSTNAME	<i>Nom d'hôte pour ce serveur CA Enterprise Log Manager</i> Exemple : CA-ELM1	Spécifiez le nom d'hôte de ce serveur en utilisant uniquement les caractères pris en charge par les hôtes. Les normes du secteur recommandent les lettres de A à Z (insensibles à la casse), les chiffres de 0 à 9 et le tiret, avec une lettre en premier caractère et un caractère alphanumérique en dernière position. N'utilisez pas le caractère de soulignement dans un nom d'hôte et ne lui ajoutez pas de nom de domaine. Remarque : Le nom d'hôte ne peut pas dépasser 15 caractères.
ROOT_PASSWORD	<i>nouveau mot de passe root</i>	Créez et confirmez un nouveau mot de passe root pour ce serveur.
IP_ADDRESS	<i>Adresse IPv4 correspondante</i>	Entrez une adresse IP valide pour ce serveur.
SUBNET_MASK	<i>Adresse IP correspondante</i>	Entrez un masque de sous-réseau valide à utiliser avec ce serveur.
DEFAULT_GATEWAY	<i>Adresse IP correspondante</i>	Entrez un masque de sous-réseau valide et une passerelle par défaut à utiliser avec ce serveur.
DNS_SERVERS	<i>Adresses IPv4 correspondantes</i>	Entrez une ou plusieurs adresses IP de serveur DNS à utiliser sur votre réseau. La liste est séparée par des virgules, sans espace entre les entrées. Si vos serveurs DNS utilisent l'adressage IPv6, entrez ces adresses avec ce format.
DOMAIN_NAME	<i>votre nom de domaine</i>	Entrez le nom de domaine complet au sein duquel opère le serveur, par exemple mycompany.com. Remarque : Le nom de domaine doit être enregistré auprès du serveur DNS (Domain Name Server) de votre réseau pour permettre la résolution du nom d'hôte vers l'adresse IP.
acceptAllEulas	Accepter	Acceptez le contrat de licence de CA pour poursuivre le provisionnement du serveur CA Enterprise Log Manager.

Informations requises	Valeur	Commentaires
deploymentOption	moyen ou grand	Si vous sélectionnez Moyenne, VMware indique 4 UC de 8 Go de mémoire RAM chacune. Si vous sélectionnez Large, VMware indique huit UC de 8 Go de mémoire RAM chacune.
TIMEZONE	<i>le fuseau horaire que vous souhaitez</i>	Sélectionnez le fuseau horaire dont dépend ce serveur.
Paramètres spécifiques aux applications		
LOCAL_REMOTE_EEM	Local pour le premier serveur installé (serveur de gestion) Distant pour chaque serveur supplémentaire	Indiquez si vous prévoyez d'utiliser un serveur CA EEM local ou distant. Pour un serveur CA Enterprise Log Manager de gestion, choisissez l'option locale. L'installation vous invite à créer un mot de passe pour le compte d'utilisateur EiamAdmin par défaut. Pour chaque serveur supplémentaire, choisissez l'option distante. L'installation vous invite à indiquer le nom du serveur de gestion. Que vous choisissiez l'option locale ou distante, vous devez utiliser l'ID et le mot de passe du compte EiamAdmin lors de la première connexion à chaque serveur CA Enterprise Log Manager.
REMOTE_EEM_LOCATION	<i>adresse IP ou nom d'hôte</i>	Entrez cette valeur uniquement si vous sélectionnez l'option de serveur distant. Entrez l'adresse IP ou le nom d'hôte du serveur CA Enterprise Log Manager de gestion installé en premier. Le nom d'hôte doit être enregistré auprès du serveur DNS. Si vous voulez utiliser un serveur CA EEM local, la valeur par défaut n'est Aucun .

Informations requises	Valeur	Commentaires
EEM_PASSWORD	<i>mot de passe du compte EiamAdmin</i>	<p>Enregistrez le mot de passe du compte d'administrateur par défaut, EiamAdmin.</p> <p>Votre serveur CA Enterprise Log Manager doit disposer de ces informations d'identification de compte pour la connexion initiale.</p> <p>Si vous installez le serveur de gestion, vous créez et confirmez ici un nouveau mot de passe EiamAdmin.</p> <p>Notez ce mot de passe, car vous l'utiliserez à nouveau lors de l'installation d'autres serveurs et agents CA Enterprise Log Manager.</p> <p>Remarque : Le mot de passe entré ici est également le mot de passe initial du compte caelmadmin par défaut, que vous utiliserez pour accéder directement au serveur CA Enterprise Log Manager via ssh.</p> <p>Si vous le souhaitez, vous pouvez créer d'autres comptes d'administrateur pour accéder aux fonctions CA EEM après l'installation.</p>
FIPS_MODE	Oui ou Non	<p>Spécifie si le dispositif virtuel doit être exécuté en mode FIPS ou non. Si vous choisissez un serveur CA EEM local, choisissez le mode de votre choix. Si vous choisissez un serveur CA EEM distant, choisissez le mode utilisé par ce serveur.</p>

Informations complémentaires :

[Ajout de serveurs virtuels à votre environnement](#) (page 341)

[Création d'un environnement complètement virtuel](#) (page 365)

[Déploiement rapide de serveurs virtuels](#) (page 391)

Appel de l'outil OVF à l'aide de scripts

Remarque : Avant d'effectuer l'installation silencieuse, installez l'outil OVF 4.0.0. Pour plus d'informations sur l'outil OVF, consultez le manuel *VMware's OVF Tool User Guide* ou visitez le site Web www.vmware.com.

Vous pouvez installer plusieurs serveurs CA Enterprise Log Manager à la fois ; pour ce faire, vous devez créer et exécuter des scripts contenant les commandes qui appellent l'outil OVF. Vous pouvez utiliser le langage de script de votre choix pour la création de scripts.

Pour appeler l'outil OVF à l'aide de scripts :

1. Créez un script pour appeler l'outil OVF.
2. Ouvrez l'invite de commande sur l'ordinateur où le client VMware vSphere est installé.
3. Accédez à l'emplacement de stockage du script.
4. Exécutez le script.

Le message Opening VI target (Cible VI en cours d'ouverture) s'affiche. Le statut de déploiement de chaque serveur CA Enterprise Log Manager s'affiche. Si l'installation s'est correctement effectuée, les serveurs CA Enterprise Log Manager figureront sous le magasin de données sélectionné dans le volet gauche.

Exemple 1 : Script de commande pour la création d'un serveur CA Enterprise Log Manager principal et d'un serveur CA Enterprise Log Manager secondaire

```
REM Primary CA Enterprise Log Manager Server
ovftool -dm=thin --acceptAllEulas --name="example_primaryserver" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password" --
prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none --
prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=YES --prop:IP_ADDRESS=172.162.0.0 --
prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_primary_server" --
prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25 --
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA
ELM\CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

```
REM Secondary CA Enterprise Log Manager Server
```

```
ovftool -dm=thin --acceptAllEulas --name="example_secondaryserver" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password1" --
prop:LOCAL_REMOTE_EEM="Remote" --prop:REMOTE_EEM_LOCATION="example_primaryserver"
--prop:EEM_PASSWORD="calmr12" --prop:FIPS_MODE="Yes" --
prop:IP_ADDRESS="172.168.10.10" --prop:SUBNET_MASK="10.0.10.10" --
prop:HOSTNAME="example_secondary_server" --prop:DEFAULT_GATEWAY="198.168.10.30" -
--prop:DNS_SERVERS="198.168.20.20,198.168.20.25" --prop:DOMAIN_NAME="example.com"
--prop:TIMEZONE="Asia/Kolkata" "C:\Program Files\CA ELM\CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

Exemple 2 : Script de commande pour la création d'un serveur de gestion et de deux serveurs de collecte

```
REM CA Enterprise Log Manager Management Server
ovftool -dm=thin --acceptAllEulas --name="example_managementserver" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password" --
prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none --
prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.0.0 --
prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_management_server" --
prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25 -
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA
ELM\CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

```
REM CA Enterprise Log Manager Collection Server 1
ovftool -dm=thin --acceptAllEulas --name="example_collectionserver1" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password1" --
prop:LOCAL_REMOTE_EEM=Remote --
prop:REMOTE_EEM_LOCATION="example_managementserver" --prop:EEM_PASSWORD=calmr12 -
--prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.10.10 --prop:SUBNET_MASK=10.0.10.10
--prop:HOSTNAME="example_collection_server1" --prop:DEFAULT_GATEWAY=198.168.10.30
--prop:DNS_SERVERS=198.168.20.20,198.168.20.25 --prop:DOMAIN_NAME=example.com --
prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA ELM\CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

```
REM CA Enterprise Log Manager Collection Server 2
```

```
ovftool -dm=thin --acceptAllEulas --name="example_collectionserver2" --  
deploymentOption=medium --prop:ROOT_PASSWORD="example_password2" --  
prop:LOCAL_REMOTE_EEM=Remote --  
prop:REMOTE_EEM_LOCATION="example_managementserver" --prop:EEM_PASSWORD=ca1mr12 -  
-prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.10.30 --prop:SUBNET_MASK=10.0.10.40  
--prop:HOSTNAME="example_collection_server2" --prop:DEFAULT_GATEWAY=198.168.10.40  
--prop:DNS_SERVERS=198.168.30.30,198.168.30.25 --prop:DOMAIN_NAME=example.com --  
prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA ELM\CA Enterprise Log  
Manager.ovf"  
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0  
"
```

Définition des paramètres de paravirtualisation et de ressources

Après l'importation du modèle OVF, définissez manuellement les paramètres de paravirtualisation et de ressource pour améliorer les performances du serveur CA Enterprise Log Manager provisionné.

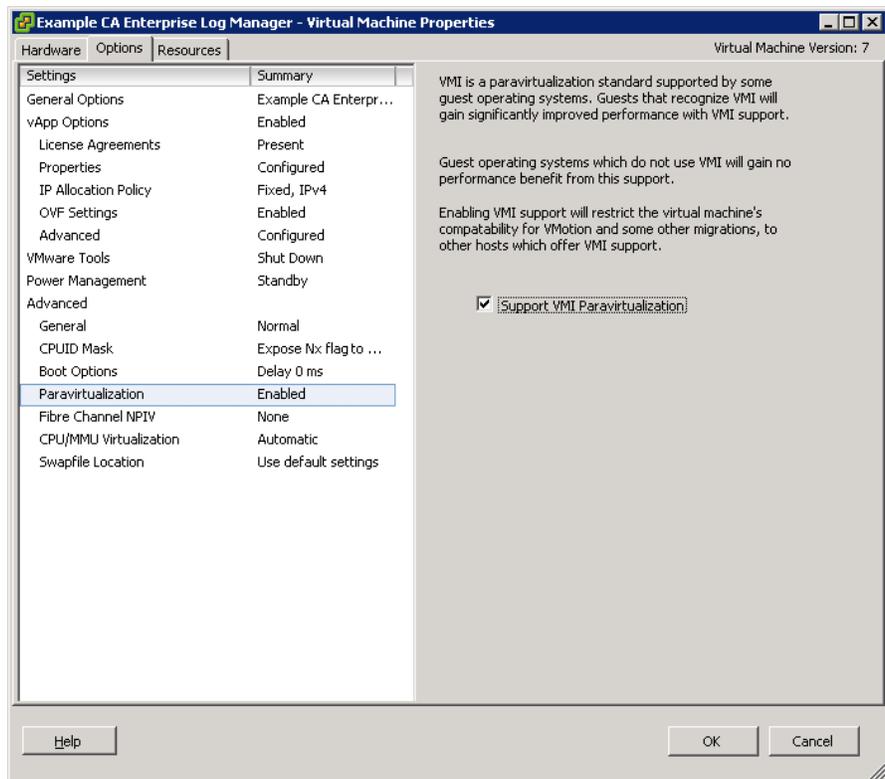
Remarque : Vérifiez que le lecteur de CD/DVD est défini sur (Client Device) Unités du client.

Pour définir les paramètres de paravirtualisation et de ressources :

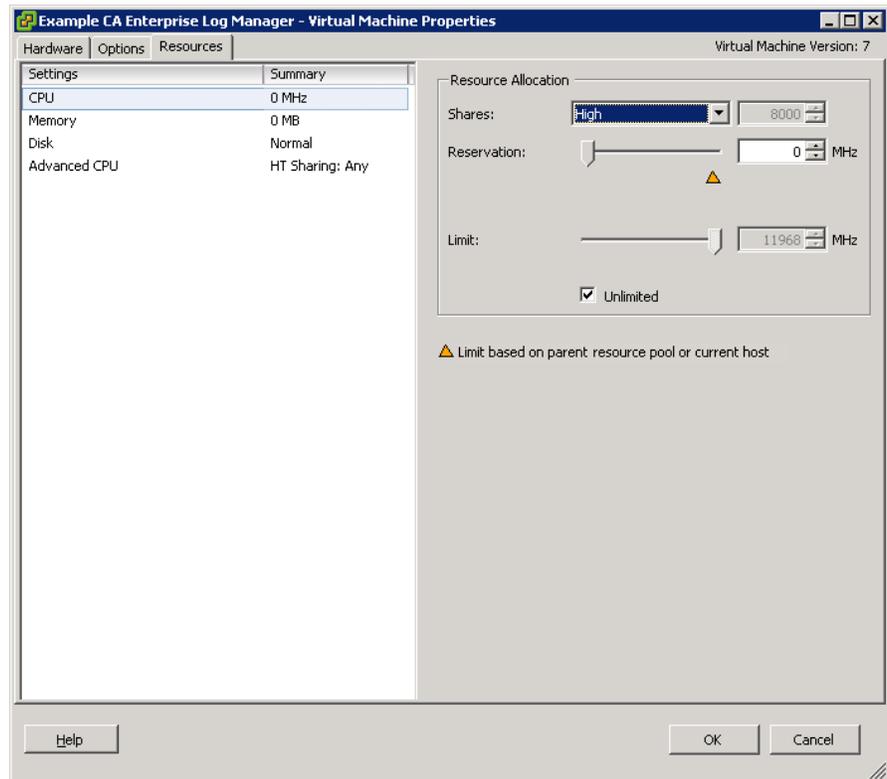
1. Cliquez avec le bouton droit de la souris sur le nouveau dispositif virtuel CA Enterprise Log Manager situé dans le volet gauche et cliquez sur Edit Settings (Modifier les paramètres).

La fenêtre <CA Enterprise Log Manager Virtual Appliance name> - Virtual Machine Properties (Propriétés de l'ordinateur virtuel <CA Enterprise Log Manager nom application virtuelle> s'affiche.

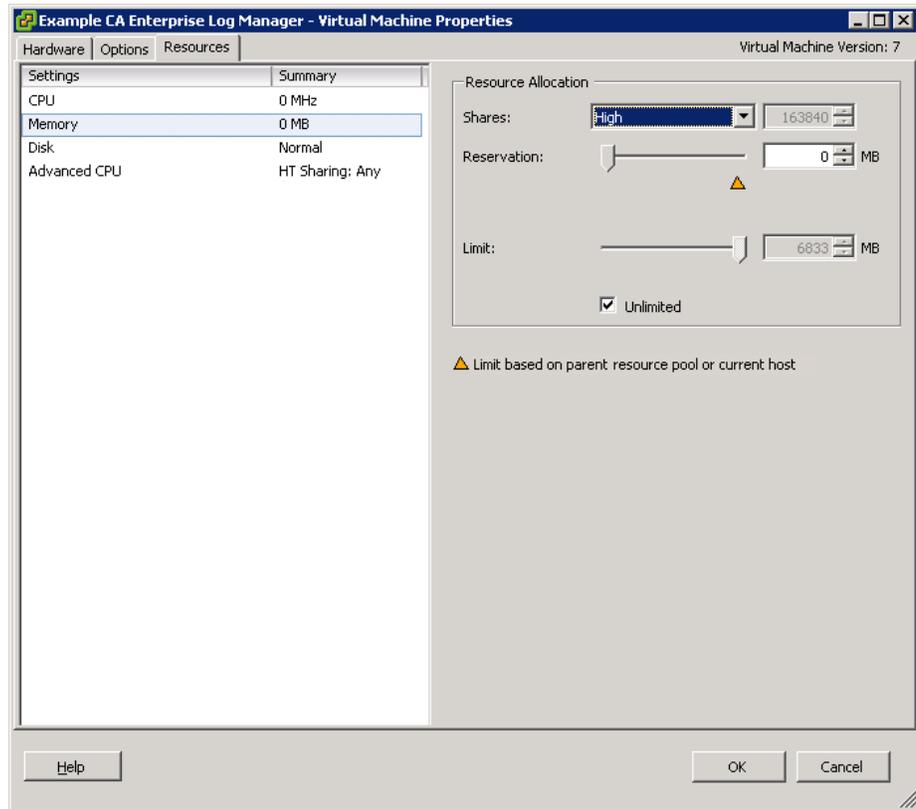
2. Cliquez sur l'onglet Option dans la fenêtre.
3. Sélectionnez le paramètre Paravirtualization situé dans le volet gauche, puis l'option Support VMI Paravirtualization (Prise en charge de la paravirtualization VMI) située dans le volet droit.



4. Cliquez sur l'onglet Resources (Ressources) dans la fenêtre.
5. Sélectionnez l'option CPU (UC) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



6. Sélectionnez l'option Memory (Mémoire) sous la colonne Settings (Paramètres), puis dans la liste déroulante Shares (Partages) située dans la section Resource Allocation (Allocation de ressources) sélectionnez High (Elevé).



7. Cliquez sur OK.
8. **Remarque** : Pour plus d'informations sur la paravirtualization, visitez le site Web www.vmware.com.

Démarrez le serveur CA Enterprise Log Manager provisionné.

Ceci est nécessaire à son exécution.

Pour démarrer un serveur CA Enterprise Log Manager :

1. Sélectionnez le nouveau serveur CA Enterprise Log Manager dans le volet gauche de la fenêtre de l'application VMware.
2. Cliquez sur l'option Power On (Démarrage) située sous l'onglet Basic Tasks of the Getting Started (Tâches de base du démarrage) dans le volet droit.

Le serveur CA Enterprise Log Manager est démarré.

Remarque : Vérifiez qu'un serveur CA Enterprise Log Manager principal est exécuté avant de démarrer un serveur CA Enterprise Log Manager secondaire.

Vérification de l'installation d'un serveur CA Enterprise Log Manager virtuel

Lors du démarrage du serveur CA Enterprise Log Manager provisionné, une URL permettant d'accéder à CA Enterprise Log Manager s'affiche dans l'onglet Console de la fenêtre Client VMware vSphere. Utilisez cette URL et les informations d'identification par défaut suivantes pour accéder à CA Enterprise Log Manager :

Nom de l'utilisateur par défaut : EiamAdmin

Mot de passe par défaut : mot de passe saisi lors de la procédure d'installation du serveur CA Enterprise Log Manager

Informations complémentaires :

[Ajout de serveurs virtuels à votre environnement](#) (page 341)

[Création d'un environnement complètement virtuel](#) (page 365)

[Déploiement rapide de serveurs virtuels](#) (page 391)

Tâches de post-installation

Après le démarrage d'un serveur CA Enterprise Log Manager, vous pouvez effectuer les opérations suivantes :

- Changement de type de clavier
- Ajout d'un serveur NTP

Changement de type de clavier

Par défaut, un serveur CA Enterprise Log Manager provisionné utilise le clavier standard américain. Vous pouvez utiliser le type de clavier de votre choix en modifiant le paramètre de langue nationale.

Pour changer le type de clavier :

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur root.

2. Exécutez la commande ci-dessous.

```
vi /etc/sysconfig/keyboard
```

Le fichier s'ouvre en mode d'édition. Les informations du type de clavier existants s'affichent.

3. Remplacez U.S.A. dans la valeur KEYTABLE par le paramètre de langue nationale que vous souhaitez.

Par exemple, pour utiliser un clavier britannique, entrez KEYTABLE="UK" pour la valeur KEYTABLE.

Remarque : Pour plus d'informations sur les paramètres de langue, reportez-vous à la documentation sur l'installation RHEL.

4. Enregistrez et fermez le fichier.

5. Redémarrez l'ordinateur.

Le type de clavier est modifié.

Ajout d'un serveur NTP

Nous vous recommandons vivement d'ajouter un serveur NTP pour mettre à jour la date et l'heure du serveur CA Enterprise Log Manager.

Pour ajouter un serveur NTP :

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur root.

2. Exécutez les commandes suivantes.

```
crontab -e
```

```
00 0 * * * /usr/sbin/ntpdate NTPserver_hostname
```

Un job cron est ajouté.

3. Enregistrez les modifications et quittez la console.

Le serveur NTP est ajouté.

Chapitre 9 : Glossaire

accès aux données

L'*accès aux données* est un type d'autorisation octroyé à l'ensemble de CA Enterprise Log Manager par le biais de la stratégie d'accès aux données par défaut, pour la classe de ressource CALM. Tous les utilisateurs ont accès à toutes les données, hormis celles dont l'accès est restreint par des filtres.

Accès ODBC et JDBC

L'*accès ODBC et JDBC* aux magasins de journaux d'événements CA Enterprise Log Manager prend en charge l'utilisation des données d'événements par un grand nombre de produits tiers, notamment la génération de rapports d'événements personnalisés à l'aide d'outils de génération de rapports tiers, la corrélation d'événements à l'aide de moteurs de corrélation et l'évaluation d'événements à l'aide de produits de détection d'intrusion et de programmes malveillants. Les systèmes Windows utilisent ODBC ; les systèmes UNIX ou Linux utilisent JDBC.

adaptateurs CA

Les *adaptateurs CA* constituent un groupe d'écouteurs qui reçoit des événements provenant de composants CA Audit tels que les clients CA Audit, les iRecorders et les SAPI Recorders, ainsi que les sources qui transmettent des événements de manière native via iTechnology.

agent

Un *agent* est un service générique, configuré avec des connecteurs chargés de collecter les événements bruts à partir d'une source d'événement unique, puis de les envoyer à CA Enterprise Log Manager pour traitement. Chaque CA Enterprise Log Manager dispose d'un agent intégré. De plus, vous pouvez installer un agent sur un point de collecte distant et collecter des événements sur des hôtes où l'installation d'agents est impossible. Vous pouvez également installer un agent sur l'hôte où s'exécutent les sources d'événement et bénéficier des possibilités d'application de règles de suppression et de chiffrement des transmissions vers CA Enterprise Log Manager.

agent par défaut

L'*agent par défaut* est l'agent intégré installé avec le serveur CA Enterprise Log Manager. Vous pouvez le configurer pour collecter directement des événements Syslog ainsi que des événements provenant de différentes sources non Syslog, par exemple CA Access Control r12 SP1, le service de certificats Microsoft Active Directory et les bases de données Oracle9i.

ajustement d'événement

L'*ajustement d'événement* est le processus par lequel une chaîne d'événement brut collecté est analysée en champs d'événement et mappée vers des champs CEG. Les utilisateurs peuvent exécuter des requêtes afin d'afficher les données d'événement ajusté ainsi obtenues. L'ajustement d'événement est l'étape qui suit la collecte des événements et qui précède leur stockage.

alerte d'action

Une *alerte d'action* est un job de requête planifié qui peut être utilisé pour détecter les violations de stratégie, les tendances d'utilisation, les schémas de connexion et d'autres actions d'événement nécessitant une attention à court terme. Par défaut, lorsque les requêtes d'une alerte renvoient des résultats, ces derniers sont affichés sur la page Alertes CA Enterprise Log Manager et ajoutés à un flux RSS. Lorsque vous planifiez une alerte, vous pouvez indiquer des destinations supplémentaires, y compris une adresse électronique, un processus de sortie d'événement/d'alerte CA IT PAM et des interruptions SNMP.

analyse

Le terme *analyse* (parfois analyse de message ou décomposition) désigne le processus d'extraction de données d'unités brutes et de conversion en paires de valeurs clés. L'analyse s'effectue sur la base d'un fichier XMP. Cette étape, qui précède le mappage de données, fait partie du processus d'intégration qui convertit les événements bruts collectés auprès d'une source d'événement en événements ajustés que vous pouvez consulter.

analyse (décomposition) d'un journal

L'*analyse (décomposition) d'un journal* est le processus qui permet d'extraire les données d'un journal, pour que les valeurs ainsi analysées (décomposées) puissent être utilisées lors des étapes suivantes du processus de gestion du journal.

analyse de fichiers XMP

L'*analyse de fichiers XMP* est le processus réalisé par l'utilitaire d'analyse de message pour rechercher tous les événements contenant chaque chaîne pré-associée, pour chaque événement associé, en décomposant l'événement en jetons à l'aide du premier filtre trouvé, qui utilise la même chaîne pré-associée.

analyse de mappage

L'*analyse de mappage* est une étape de l'Assistant de fichier de mappage, qui vous permet de tester et de modifier un fichier de mappage de données. Des exemples d'événement sont testés par rapport au fichier de mappage de données et les résultats sont validés avec la CEG.

analyse de message

L'*analyse de message* est le processus consistant à appliquer des règles à l'analyse d'un journal d'événements bruts, afin d'obtenir des informations pertinentes, telles que l'horodatage, l'adresse IP et le nom d'utilisateur. Les règles d'analyse utilisent la correspondance de caractères pour localiser un texte d'événement spécifique et le relier aux valeurs sélectionnées.

analyse des journaux

L'*analyse des journaux* est l'étude des entrées de journal, qui permet d'identifier les événements pertinents. Si les journaux ne sont pas analysés opportunément, leur valeur est considérablement réduite.

AppObjects

Les *AppObjects* (Application Objects), ou objets d'application, sont des ressources spécifiques à un produit ; ils sont stockés dans CA EEM sous l'instance d'application d'un produit donné. Pour l'instance d'application CAELM, ces ressources incluent le contenu des rapports et requêtes, les jobs planifiés pour les rapports et alertes, les configurations et le contenu des agents, les configurations de service, d'adaptateur et d'intégration, les fichiers de mappage de données et d'analyse de message, ainsi que les règles de suppression et de récapitulation.

archivage automatique

L'*archivage automatique* est un processus configurable qui permet d'automatiser le transfert des bases de données d'archivage entre deux serveurs. Lors de la première phase de l'archivage automatique, le serveur de collecte envoie les bases de données nouvellement archivées au serveur de rapports, à la fréquence que vous avez prédéfinie. Lors de la seconde phase, le serveur de rapports envoie les anciennes bases de données au serveur de stockage distant, pour un stockage à long terme, ce qui évite d'avoir à effectuer la sauvegarde et le transfert manuellement. Pour effectuer un archivage automatique, vous devez configurer une authentification sans mot de passe entre le serveur source et le serveur de destination.

archivage de journaux

L'*archivage de journaux* est le processus se déroulant lorsque la base de données chaude atteint sa taille maximale, auquel cas une compression au niveau des lignes est effectuée et la base passe de "l'état chaud" à "l'état tiède". Les administrateurs peuvent sauvegarder manuellement les bases de données tièdes, avant que le délai de suppression automatique ne soit écoulé, puis exécuter l'utilitaire LMArchive pour enregistrer le nom des sauvegardes. Ces informations sont alors disponibles à la consultation, via la requête d'archivage.

assistant de fichier d'analyse

L'*Assistant de fichier d'analyse* est une fonction CA Enterprise Log Manager que les administrateurs utilisent pour créer, modifier et analyser les fichiers d'analyse de message extensibles (XMP), stockés sur le serveur de gestion CA Enterprise Log Manager. Pour personnaliser l'analyse des données d'événements entrants, vous devez modifier les chaînes et filtres pré-associés. Les nouveaux fichiers, comme les fichiers modifiés, s'affichent dans l'Explorateur de collecte de journaux, la Bibliothèque d'ajustement d'événement, les fichiers d'analyse et le dossier Utilisateur.

Authentification ssh non interactive

L'authentification *non interactive* permet de déplacer des fichiers d'un serveur à un autre sans avoir à saisir de phrase secrète. Avant de configurer l'archivage automatique ou d'utiliser le script `restore-ca-elm.sh`, définissez l'authentification non interactive du serveur source vers le serveur de destination.

balise

Une *balise* est un terme ou une expression clé, qui sert à identifier les requêtes ou rapports appartenant au même regroupement pertinent. Les balises permettent d'effectuer des recherches basées sur les regroupements pertinents. Le terme balise désigne également le nom de ressource utilisé dans une stratégie octroyant à l'utilisateur le droit de créer une balise.

bases de données archivées

Les *bases de données archivées* sur un serveur CA Enterprise Log Manager donné incluent : toutes les bases de données tièdes disponibles pour requête, mais nécessitant une sauvegarde manuelle avant expiration ; toutes les bases de données froides ; toutes les bases de données enregistrées comme restaurées à partir d'une sauvegarde.

bibliothèque d'ajustement d'événement

La *bibliothèque d'ajustement d'événement* est l'espace de stockage qui contient les intégrations, les fichiers de mappage et d'analyse, ainsi que les règles de suppression et de récapitulation, prédéfinis et définis par l'utilisateur.

bibliothèque d'analyse de message

La *bibliothèque d'analyse de message* est une bibliothèque qui accepte les événements provenant des files d'attente d'écouteur et qui utilise des expressions régulières pour marquer les chaînes en paires nom/valeur.

bibliothèque de la requête

La *bibliothèque de la requête* est la bibliothèque dans laquelle sont stockées toutes les requêtes, les balises de requête et les filtres d'invite, prédéfinis et définis par l'utilisateur.

bibliothèque de rapports

La *bibliothèque de rapports* est la bibliothèque dans laquelle sont stockés tous les rapports, les balises de rapports, les rapports générés et les jobs de rapports planifiés, prédéfinis et définis par l'utilisateur.

CA Enterprise Log Manager

CA Enterprise Log Manager est une solution qui vous permet de collecter des journaux à partir de sources d'événement très dispersées et de différents types, de contrôler la conformité avec les requêtes et les rapports, et de conserver des enregistrements des bases de données de journaux compressés stockées à long terme sur un système externe.

CA IT PAM

CA IT PAM est l'acronyme de CA IT Process Automation Manager. Le rôle de ce produit CA est d'automatiser les processus que vous définissez. *CA Enterprise Log Manager* utilise deux processus : la création d'un processus de sortie de l'événement/de l'alerte pour un produit local, par exemple *CA Service Desk*, et la génération dynamique de listes qui peuvent être importées sous la forme de valeurs à clés. L'intégration requiert *CA IT PAM* r2.1.

CA Spectrum

CA Spectrum est un produit de gestion des défaillances réseau qui peut être intégré à *CA Enterprise Log Manager* pour être utilisé comme destination des alertes envoyées sous la forme d'interruptions SNMP.

CAELM

CAELM est le nom de l'instance d'application que *CA EEM* utilise pour *CA Enterprise Log Manager*. Pour accéder à la fonctionnalité *CA Enterprise Log Manager* dans *CA Embedded Entitlements Manager*, saisissez l'URL https://<adresse_ip>:5250/spin/eiam/eiam.csp, sélectionnez *CAELM* comme nom d'application, puis saisissez le mot de passe de l'utilisateur *EiamAdmin*.

caelmadmin

Le nom d'utilisateur et le mot de passe *caelmadmin* sont les informations d'identification nécessaires pour accéder au système d'exploitation du dispositif logiciel. L'ID d'utilisateur *caelmadmin* est créé lors de l'installation de ce système d'exploitation. Durant l'installation du composant logiciel, l'installateur doit spécifier le mot de passe du compte de superutilisateur *CA EEM*, *EiamAdmin*. Le même mot de passe est affecté au compte *caelmadmin*. Nous recommandons que l'administrateur du serveur se connecte via *ssh* en tant qu'utilisateur *caelmadmin* et modifie ce mot de passe par défaut. Bien que l'administrateur ne puisse pas se connecter via *ssh* en tant que *root*, il peut basculer sur le compte *root* (*su root*) si nécessaire.

caelmservice

caelmservice est un compte de service qui permet d'exécuter iGateway et les services CA EEM locaux en tant qu'utilisateur non root. Le compte caelmservice est utilisé pour installer les mises à jour du système d'exploitation téléchargées avec les mises à jour d'abonnement.

calendrier

Un *calendrier* est un moyen de limiter la durée d'application d'une stratégie d'accès. Une stratégie permet aux identités spécifiées d'effectuer les actions indiquées sur la ressource spécifiée durant le laps de temps déterminé.

CALM

CALM est une classe de ressource prédéfinie qui inclut les ressources CA Enterprise Log Manager suivantes : Alerte, ArchiveQuery, calmTag, Données, EventGrouping, Intégration et Rapport. Les actions autorisées pour cette ressource sont : Annotation (Rapports), Création (Alerte, calmTag, EventGrouping, Intégration et Rapport), Dataaccess (Données), Exécution (ArchiveQuery) et Planification (Alerte, Rapport).

calmTag

calmTag est un attribut nommé de l'AppObject utilisé lors de la création d'une stratégie de portée afin de limiter l'accès aux requêtes et rapports appartenant à certaines balises. Tous les rapports et requêtes sont des objets d'application (AppObjects) et ont calmTag comme attribut (à ne pas confondre avec la balise de ressource).

catalogue

Le *catalogue* est la base de données stockée sur chaque CA Enterprise Log Manager, qui consigne l'état des bases de données archivées et joue le rôle d'index de haut niveau pour l'ensemble des bases de données. Les informations d'état (tiède, froid ou dégivré) sont conservées pour toutes les bases de données ayant jamais transité par ce CA Enterprise Log Manager, ainsi que toutes celles ayant été restaurées sur ce CA Enterprise Log Manager en tant que base de données dégivrée. La fonction d'indexation s'étend à toutes les bases de données chaudes et tièdes contenues dans le magasin de journaux d'événements de ce CA Enterprise Log Manager.

catalogue d'archive

Voir catalogue.

catégories d'événement

Les *catégories d'événement* sont les balises utilisées par CA Enterprise Log Manager pour classer les événements selon leur fonction, avant de les insérer dans le magasin d'événements.

Certificats

Les *certificats* prédéfinis utilisés par CA Enterprise Log Manager sont CAELMCert.cer et CAELM_AgentCert.cer. Tous les services CA Enterprise Log Manager utilisent CAELMCert.cer pour communiquer avec le serveur de gestion. Tous les agents utilisent CAELM_AgentCert.cer pour communiquer avec leur serveur de collecte.

Champs CEG

Les *champs CEG* sont des étiquettes utilisées pour normaliser la présentation des champs d'événements bruts provenant de sources d'événement hétérogènes. Lors de l'ajustement d'événement, CA Enterprise Log Manager analyse les messages d'événements bruts dans une série de paires nom-valeur, puis mappe les noms des événements bruts avec les champs CEG standard. L'ajustement crée des paires nom-valeur composées des champs CEG et des valeurs issues de l'événement brut. En d'autres termes, au cours de l'ajustement des événements bruts, les différentes étiquettes utilisées dans les événements bruts correspondant au même objet de données ou élément de réseau sont converties au même nom de champ CEG. Les champs CEG sont mappés aux OID de la MIB utilisée pour les interruptions SNMP.

client d'abonnement

Un *client d'abonnement* est un serveur CA Enterprise Log Manager qui récupère les mises à jour de contenu auprès d'un autre serveur CA Enterprise Log Manager, appelé serveur proxy d'abonnement. Les clients d'abonnement interrogent le serveur proxy d'abonnement configuré de manière régulière et planifiée, et ils récupèrent les nouvelles mises à jour disponibles, le cas échéant. Après récupération des mises à jour, le client installe les composants téléchargés.

collecte d'événements

La *collecte d'événements* est un processus permettant de lire la chaîne d'événement brut à partir d'une source d'événement et de l'envoyer au CA Enterprise Log Manager configuré. La collecte est suivie d'un ajustement d'événement.

collecte directe de journaux

La *collecte directe de journaux* est la technique de collecte de journaux sans agent intermédiaire entre la source d'événement et le logiciel CA Enterprise Log Manager.

collecteur SAPI

Le *collecteur SAPI* est un adaptateur CA qui reçoit des événements provenant de clients CA Audit. Les envois des clients CA Audit reposent sur l'action Collecteur, qui propose le basculement intégré. Les administrateurs configurent le collecteur SAPI CA Audit avec, par exemple, les fichiers de mappage de données et les chiffres sélectionnés.

Compatibilité avec la norme FIPS 140-2

L'expression "*compatible avec la FIPS 140-2*" désigne un produit pouvant *facultativement* utiliser des bibliothèques cryptographiques conformes à la FIPS et des algorithmes pour chiffrer et déchiffrer des données sensibles. CA Enterprise Log Manager est un produit de collecte de journaux compatible avec la FIPS, car vous pouvez choisir d'exécuter en mode FIPS ou en mode non FIPS.

composants de visualisation

Les *composants de visualisation* sont des options disponibles pour l'affichage des données de rapport, par exemple une table, un graphique (en courbes, à barres, à colonnes, à secteurs) ou une visionneuse d'événements.

compte

Un *compte* est un utilisateur global qui est également un utilisateur d'applications CALM. Une même personne peut posséder plusieurs comptes, chacun disposant d'un rôle personnalisé différent.

configuration enregistrée

Une *configuration enregistrée* est une configuration stockée avec les valeurs d'attributs d'accès aux données provenant d'une intégration pouvant être utilisée comme modèle lors de la création d'une nouvelle intégration.

configuration globale

La *configuration globale* est un ensemble de paramètres qui s'appliquent à tous les serveurs CA Enterprise Log Manager utilisant le même serveur de gestion.

Conformité à la norme FIPS 140-2

L'expression "*conforme à la FIPS 140-2*" désigne un produit qui par défaut utilise *uniquement* des algorithmes de chiffrement certifiés par un laboratoire accrédité de test des modules cryptographiques (CMT). CA Enterprise Log Manager peut utiliser des modules cryptographiques basés sur les bibliothèques BSAFE Crypto-C ME et Crypto-J certifiées RSA en mode FIPS, mais ne pourra peut-être pas le faire par défaut.

connecteur

Un *connecteur* est une intégration ciblant une source d'événement spécifique, configurée sur un agent donné. Un agent peut charger en mémoire plusieurs connecteurs, similaires ou non. Le connecteur permet de collecter les événements bruts à partir d'une source d'événement et d'effectuer une transmission régulée (sur règle) des événements convertis vers un magasin de journaux d'événements, où ils seront insérés dans la base de données chaude. Les intégrations prêtes à l'emploi permettent une collecte optimisée à partir d'une large gamme de sources d'événement, notamment des systèmes d'exploitation, des bases de données, des serveurs Web, des pare-feu et de nombreux types d'applications de sécurité. Vous pouvez définir entièrement un connecteur pour une source d'événement interne ou utiliser une intégration comme modèle.

Contenu d'une interruption SNMP

Une *interruption SNMP* se compose de paires nom-valeur, chaque nom étant un OID (identificateur d'objet) et chaque valeur une valeur renvoyée par l'alerte planifiée. Les résultats de requête renvoyés par une alerte d'action contiennent des champs CEG ainsi que leurs valeurs. L'interruption SNMP est renseignée en substituant un OID à chaque champ CEG utilisé pour le nom de la paire nom-valeur. Le mappage de chaque champ avec un OID est stocké dans la MIB. L'interruption SNMP inclut uniquement les paires nom-valeur des champs que vous avez sélectionnés lorsque de la configuration de l'alerte.

cumul d'événements

Le *cumul d'événements* est le processus par lequel des entrées de journal similaires sont regroupées en une entrée unique, contenant un compteur d'occurrences d'événement. Les règles de récapitulation définissent le regroupement des événements.

dégel

Le *dégel* est le processus qui consiste à faire passer une base de données de l'état froid à l'état dégivré. Cette opération est réalisée par CA Enterprise Log Manager lorsque l'utilitaire LMArchive l'avertit qu'une base de données froide connue a été restaurée. Si la base de données froide n'est pas restaurée sur son CA Enterprise Log Manager original, l'utilitaire LMArchive n'est pas utilisé et aucun dégel n'est requis ; la fonction de recatalogage ajoute la base de données restaurée en tant que base de données tiède.

Destinations d'une interruption SNMP

Lorsque vous planifiez une alerte d'action, vous avez la possibilité d'ajouter plusieurs *destinations pour l'interruption SNMP*. Chacune d'entre elles est définie par une adresse IP et un numéro de port. Généralement, la destination est un NOC ou un serveur de gestion tel que CA Spectrum ou CA NSM. Une interruption SNMP est envoyée aux destinations configurées lorsque les requêtes d'un job d'alerte planifié renvoient des résultats.

détecteur de journaux

Un *détecteur de journaux* est un composant d'intégration conçu pour lire un type de journal spécifique, comme une base de données, Syslog, un fichier ou SNMP. Les détecteurs de journaux peuvent être réutilisés. Généralement, les utilisateurs ne créent pas de détecteur de journaux personnalisé.

Dispositif logiciel

Un *dispositif logiciel* est un package logiciel entièrement fonctionnel qui contient le logiciel, le système d'exploitation sous-jacent et tous les packages de dépendants. Il s'installe dans le matériel fourni par l'utilisateur final en démarrant le support d'installation du dispositif logiciel.

dossier

Un *dossier* est un emplacement de répertoire que le serveur de gestion CA Enterprise Log Manager utilise pour stocker les types d'objet CA Enterprise Log Manager. Vous référencez des dossiers dans des stratégies de portée afin de permettre ou d'interdire à certains utilisateurs d'accéder au type d'objet spécifié.

éléments d'intégration

Les *éléments d'intégration* incluent un détecteur, une aide à la configuration, un fichier d'accès aux données, un ou plusieurs fichiers d'analyse de message (XMP) et un ou plusieurs fichiers de mappage de données.

enregistrement de journal

Un *enregistrement de journal* est un enregistrement d'audit individuel.

enregistrements d'audit

Les *enregistrements d'audit* contiennent les événements de sécurité de type tentatives d'authentification, accès aux fichiers et modifications apportées aux stratégies de sécurité, comptes d'utilisateur ou droits d'utilisateur. Les utilisateurs Administrator spécifient les types d'événement à auditer et ce qui doit être journalisé.

entrée de journal

Une *entrée de journal* est, dans un journal, l'emplacement contenant des informations sur un événement spécifique qui s'est produit sur un système ou un réseau donné.

état chaud d'une base de données

L'*état chaud* correspond à une base de données du magasin de journaux d'événements, où sont insérés de nouveaux événements. Lorsqu'une base de données chaude atteint sa taille maximale prédéfinie sur le serveur de collecte, elle est compressée, cataloguée et déplacée sur un système de stockage non compressé sur le serveur de rapports. De plus, tous les serveurs stockent les nouveaux événements d'autosurveillance dans une base de données chaude.

état dégivré d'une base de données

L'*état dégivré* est l'état qualifiant une base de données qui a été restaurée dans le répertoire d'archivage après l'exécution de l'utilitaire LMArchive par l'administrateur pour indiquer à CA Enterprise Log Manager que la base de données a été restaurée. Les bases de données dégivrées sont conservées pendant le nombre d'heures configuré pour la stratégie d'exportation. Vous pouvez effectuer des requêtes sur des journaux d'événements dans les bases de données chaudes, tièdes et dégivrées.

état froid d'une base de données

L'*état froid* s'applique à une base de données tiède lorsqu'un administrateur exécute l'utilitaire LMArchive pour avertir CA Enterprise Log Manager que la base de données a été sauvegardée. Les administrateurs doivent sauvegarder les bases de données tièdes et exécuter cet utilitaire avant que ces bases de données ne soient supprimées. En effet, une base de données tiède est automatiquement supprimée lorsque son ancienneté dépasse la valeur Nbre max. de jours d'archivage définie ou lorsque le seuil Espace disque d'archivage est atteint, dès que l'une de ces deux conditions est remplie. Vous pouvez interroger la base de données d'archivage pour identifier les bases de données dont l'état est tiède ou froid.

état tiède d'une base de données

L'*état tiède* correspond à une base de données chaude de journaux d'événements, qui est déplacée lorsque sa taille atteint la limite maximale spécifiée (Nombre maximum de lignes) ou lorsqu'un recatalogage est effectué après restauration d'une base de données froide dans un nouveau magasin de journaux d'événements. Les bases de données tièdes sont conservées dans le magasin de journaux d'événements jusqu'à ce que leur ancienneté (en jours) dépasse la valeur configurée pour le paramètre Nbre max. de jours d'archivage. Vous pouvez effectuer des requêtes sur des journaux d'événements dans les bases de données chaudes, tièdes et dégivrées.

états de base de données

Les *états d'une base de données* incluent "chaude" pour une base de données de nouveaux événements, "tiède" pour une base de données d'événements compressés, "froide" pour une base de données sauvegardée et "dégivrée" pour une base de données restaurée dans le magasin de journaux d'événements où elle avait été sauvegardée. Vous pouvez lancer une requête sur les bases de données chaudes, tièdes et dégivrées. Toutes les requêtes d'archivage affichent les informations relatives aux bases de données froides.

événement ajusté

Un *événement ajusté* contient les données d'événements mappés ou analysés, dérivées d'événements bruts ou récapitulés. CA Enterprise Log Manager réalise le mappage et l'analyse pour permettre les recherches sur les données stockées.

événement brut

Un *événement brut* correspond aux informations déclenchées par un événement natif envoyé par un agent de surveillance au collecteur Log Manager. L'événement brut est souvent présenté sous la forme d'une chaîne Syslog ou d'une paire nom/valeur. Il est possible d'examiner un événement sous sa forme brute dans CA Enterprise Log Manager.

événement d'autosurveillance

Un *événement d'autosurveillance* est un événement journalisé par CA Enterprise Log Manager. Ce type d'événement est automatiquement généré sur la base d'actes effectués par l'utilisateur et de fonctions réalisées par différents modules, tels que les services et les écouteurs. Pour consulter le rapport précisant les détails des événements d'autosurveillance des opérations SIM, sélectionnez un serveur de rapports et ouvrez l'onglet Événements d'autosurveillance.

événement distant

Un *événement distant* est un événement impliquant deux ordinateurs hôtes distincts, la source et la destination. Un événement distant est de type 2, sur les quatre types d'événement utilisés dans la grammaire commune aux événements.

événement enregistré

Un *événement enregistré* contient les données d'un événement brut ou ajusté, après son intégration dans la base de données. Les événements bruts sont toujours enregistrés, sauf s'ils sont supprimés ou récapitulés, comme des événements ajustés. Ces informations sont stockées et peuvent être interrogées.

événement local

Un *événement local* est un événement impliquant une entité unique, où la source et la destination de l'événement correspondent au même ordinateur hôte. Un événement local est de type 1, sur les quatre types d'événement utilisés dans la grammaire commune aux événements.

événement natif

Un *événement natif* constitue l'état ou l'action déclenchant un événement brut. Les événements natifs sont reçus et analysés/mappés, le cas échéant, puis transmis en tant qu'événements bruts ou ajustés. Un échec d'authentification est un événement natif.

événement observé

Un *événement observé* est un événement impliquant une source, une destination et un agent, où l'événement est observé et enregistré par un agent de collecte d'événements.

événement RSS

Un *événement RSS* est un événement généré par CA Enterprise Log Manager pour transmettre une alerte d'action à des produits et utilisateurs tiers. L'événement est un récapitulatif de chaque résultat d'alerte d'action et un lien vers le fichier de résultat. La durée d'un flux RSS donné peut être configurée.

événements

Dans CA Enterprise Log Manager, les *événements* sont des enregistrements de journal générés par chaque source d'événement spécifiée.

event_action

event_action est le champ de quatrième niveau et spécifique à l'événement, utilisé par la grammaire commune aux événements (CEG) pour la normalisation des événements. Il décrit les actions communes. Les types d'action d'événement (*event_action*) incluent par exemple : Lancement d'un processus, Arrêt d'un processus et Erreur d'application.

event_category

event_category est le champ de deuxième niveau et spécifique à l'événement, utilisé par la grammaire commune aux événements (CEG) pour la normalisation des événements. Il permet une classification plus approfondie des événements, avec une valeur *ideal_model* spécifique. Les types de catégories d'événement (*event_category*) incluent : Sécurité opérationnelle, Gestion des identités, Gestion de la configuration, Accès aux ressources et Accès au système.

event_class

event_class est le champ de troisième niveau et spécifique à l'événement, utilisé par la grammaire commune aux événements (CEG) pour la normalisation des événements. Il permet une classification plus approfondie des événements, avec une valeur *event_category* spécifique.

explorateur d'agent

L'*Explorateur d'agent* est l'espace de stockage qui contient les paramètres de configuration d'un agent. Les agents peuvent être installés sur un point de collecte ou sur un terminal où il existe des sources d'événement.

fédération hiérarchique

Une *fédération hiérarchique* de serveurs CA Enterprise Log Manager est une topologie qui établit une relation hiérarchique entre les serveurs. Dans sa forme la plus simple, le serveur 2 est un enfant du serveur 1, mais le serveur 1 n'est pas un enfant du serveur 2. La relation est donc unilatérale. Une fédération hiérarchique peut posséder de nombreux niveaux de relation parent-enfant et un seul serveur parent peut avoir de nombreux serveurs enfants. Une requête fédérée renvoie ses résultats depuis le serveur sélectionné et ses enfants.

fédération maillée

Une *fédération maillée* de serveurs CA Enterprise Log Manager est une topologie qui établit une relation de parité entre les serveurs. Dans sa forme la plus simple, le serveur 2 est un enfant du serveur 1 et le serveur 1 est un enfant du serveur 2. Une paire de serveurs maillée a une relation bilatérale. Une fédération maillée peut être définie pour qu'un grand nombre de serveurs soient les pairs les uns des autres. Une requête fédérée renvoie ses résultats depuis le serveur sélectionné et tous ses pairs.

fichier d'analyse de message (XMP, Message Parsing File)

Un *fichier d'analyse de message (XMP)* est un fichier XML associé à un type de source d'événement spécifique, qui applique des règles d'analyse. Les règles d'analyse décomposent les données pertinentes d'un événement brut collecté, afin d'obtenir des paires nom/valeur qui sont ensuite transmises au fichier de mappage de données à des fins de traitement. Ce type de fichier est utilisé dans toutes les intégrations, ainsi que dans les connecteurs, qui sont eux-mêmes basés sur des intégrations. Dans le cas d'adaptateurs CA, les fichiers XMP peuvent également être appliqués au serveur CA Enterprise Log Manager.

fichiers de mappage de données

Les *fichiers de mappage des données* sont des fichiers XML utilisant la grammaire commune aux événements (CEG) de CA pour transformer des événements d'un format source en un format conforme CEG pouvant être stocké à des fins de rapport et d'analyse dans le magasin de journaux d'événements. Un fichier de mappage de données doit être créé pour chaque nom de journal pour que les données d'événement puissent être stockées. L'utilisateur peut modifier une copie du fichier de mappage de données et l'appliquer à un connecteur spécifié.

filtrage d'événements

Le *filtrage d'événements* est le processus de tri des événements sur la base de filtres CEG.

filtre

Un *filtre* est un moyen permettant de limiter les requêtes sur le magasin de journaux d'événements.

filtre d'accès

Un *filtre d'accès* est un filtre que l'administrateur peut définir pour contrôler les données d'événement pouvant être consultées par les utilisateurs ou groupes ne détenant pas le rôle Administrator. Un filtre d'accès peut, par exemple, limiter les données que des identités spécifiées peuvent afficher dans un rapport. Les filtres d'accès sont automatiquement convertis en stratégies d'obligation.

filtre global

Un *filtre global* est un ensemble de critères que vous pouvez spécifier pour limiter les éléments présentés dans tous les rapports. Par exemple, un filtre global pour les 7 derniers jours renvoie les événements générés au cours des sept derniers jours écoulés.

filtre local

Un *filtre local* est un ensemble de critères que vous pouvez spécifier lors de la consultation d'un rapport, pour limiter les données affichées dans ce rapport en cours.

FIPS mode

Le *mode FIPS* est un paramètre qui requiert que les serveurs et agents CA Enterprise Log Manager utilisent des modules cryptographiques certifiés FIPS par RSA pour le chiffrement. Le paramètre alternatif est le mode non-FIPS.

gestion des agents

La *gestion des agents* est le processus logiciel qui contrôle l'ensemble des agents associés à l'ensemble de CA Enterprise Log Manager fédérés. Ce processus authentifie les agents avec lesquels il communique.

gestion des droits

La *gestion des droits* est la méthode qui permet de contrôler ce que les utilisateurs sont autorisés à faire une fois authentifiés et connectés à l'interface CA Enterprise Log Manager. Ceci implique des stratégies d'accès associées à des rôles affectés aux utilisateurs. Ces rôles, ou groupes d'utilisateurs d'applications, et stratégies d'accès peuvent être prédéfinis ou définis par l'utilisateur. La gestion des droits est assurée par le magasin d'utilisateurs interne du système CA Enterprise Log Manager.

gestion des journaux de sécurité informatique

La *gestion des journaux de sécurité informatique* est définie par le National Institute of Standards and Technology (NIST) comme étant le "processus permettant de générer, de transmettre, de stocker, d'analyser et d'éliminer les données des journaux de sécurité des ordinateurs".

grammaire commune aux événements (CEG)

La *grammaire commune aux événements* est le cadre qui propose un format standard utilisé par CA Enterprise Log Manager pour convertir les événements à l'aide de fichiers d'analyse et de mappage, avant de les stocker dans le magasin de journaux d'événements. La CEG utilise des champs communs et normalisés pour définir les événements de sécurité provenant de plates-formes et de produits différents. Les événements ne pouvant faire l'objet d'une analyse ou d'un mappage sont stockés en tant qu'événements bruts.

groupe d'agents

Un *groupe d'agents* est une balise que les utilisateurs peuvent appliquer aux agents sélectionnés, qui permet d'appliquer simultanément une configuration à plusieurs agents et de récupérer les rapports basés sur les groupes. Un agent donné peut appartenir à un seul groupe à la fois. Les groupes d'agents sont basés sur des critères définis par l'utilisateur, comme la région géographique ou l'importance.

groupe d'applications

Un *groupe d'applications* est un groupe spécifique à un produit, pouvant être affecté à un utilisateur global. Les groupes d'applications (ou rôles) prédéfinis pour CA Enterprise Log Manager sont Administrator, Analyst et Auditor. Ces groupes d'applications sont disponibles uniquement pour les utilisateurs CA Enterprise Log Manager ; ils ne peuvent pas être affectés aux utilisateurs d'autres produits enregistrés sur le même serveur CA EEM. Des groupes d'applications définis par l'utilisateur doivent être ajoutés à la stratégie d'accès aux applications CALM par défaut, pour que les utilisateurs de ces groupes puissent accéder à CA Enterprise Log Manager.

groupe d'utilisateurs

Un *groupe d'utilisateurs* peut être un groupe d'applications, un groupe global ou un groupe dynamique. Les groupes d'applications CA Enterprise Log Manager prédéfinis sont les rôles Administrator, Analyst et Auditor. Les utilisateurs CA Enterprise Log Manager peuvent faire partie des groupes globaux par le biais d'appartenances distinctes de CA Enterprise Log Manager. Les groupes dynamiques sont définis par l'utilisateur et créés via une stratégie de groupe dynamique.

groupe d'utilisateurs dynamique

Un *groupe d'utilisateurs dynamique* est composé d'utilisateurs globaux qui partagent un ou plusieurs attributs communs. Un groupe d'utilisateurs dynamique est créé par le biais d'une stratégie de groupe d'utilisateurs dynamique particulière dans laquelle le nom de la ressource est le nom du groupe d'utilisateurs dynamique et l'appartenance repose sur un ensemble de filtres configurés sur les attributs d'utilisateur et de groupe.

groupe global

Un *groupe global* est un groupe partagé sur les instances d'application enregistrées auprès du même serveur de gestion CA Enterprise Log Manager. N'importe quel utilisateur peut être affecté à un ou plusieurs groupes globaux. Des stratégies d'accès peuvent être définies avec les groupes globaux en tant qu'identités, afin d'autoriser ou d'interdire à ces dernières d'effectuer certaines actions sur les ressources sélectionnées.

ideal_model

ideal_model correspond à la technologie exprimant l'événement. Il s'agit du premier champ de la grammaire commune aux événements (CEG) dans la hiérarchie des champs utilisés pour la normalisation et la classification des événements. Les types de modèles idéaux (*ideal_model*) incluent : Antivirus, DBMS, Pare-feu, Système d'exploitation et Serveur Web. Les produits de pare-feu Check Point, Cisco PIX et Netscreen/Juniper peuvent être normalisés en saisissant la valeur "Pare-feu" dans le champ *ideal_model*.

identité

Dans CA Enterprise Log Manager, une *identité* est un utilisateur ou un groupe autorisé à accéder à l'instance d'application CAELM et à ses ressources. Pour tout produit CA, une identité peut être un utilisateur global, un utilisateur d'applications, un groupe global, un groupe d'applications ou un groupe dynamique.

installateur

L'*installateur* est la personne qui se charge d'installer le dispositif logiciel et les agents. Lors de la procédure d'installation, les noms d'utilisateur caelmadmin et EiamAdmin sont créés et le mot de passe spécifié pour EiamAdmin est affecté à caelmadmin. Les informations d'identification de caelmadmin sont requises pour le premier accès au système d'exploitation ; celles de EiamAdmin sont nécessaires pour le premier accès au logiciel CA Enterprise Log Manager et pour l'installation des agents.

instance d'application

Une *instance d'application* est un espace commun dans le référentiel CA EEM, où sont stockés tous les utilisateurs, groupes, contenus, stratégies d'autorisation et configurations. En général, tous les serveurs CA Enterprise Log Manager d'une entreprise utilisent la même instance d'application (par défaut, CAELM). Vous pouvez installer des serveurs CA Enterprise Log Manager avec différentes instances d'application, mais seuls les serveurs partageant la même instance d'application peuvent être fédérés. Les serveurs configurés pour utiliser le même serveur CA EEM avec différentes instances d'application partagent uniquement le magasin d'utilisateurs, les stratégies de mots de passe et les groupes globaux. Les différents produits CA ont des instances d'application par défaut différentes.

intégration

L'*intégration* est une méthode permettant de traiter les événements non classés en événements ajustés, pour pouvoir les afficher dans les requêtes et les rapports. L'intégration est mise en oeuvre avec un ensemble d'éléments qui permettent à un connecteur et un agent donnés de collecter les événements à partir d'un ou de plusieurs types de source d'événement, puis de les envoyer à CA Enterprise Log Manager. Cet ensemble d'éléments inclut le détecteur de journaux ainsi que les fichiers XMP et de mappage de données, conçus pour être lus à partir d'un produit spécifique. Les intégrations permettant de traiter les événements Syslog et les événements WMI sont des exemples d'intégrations prédéfinies. Vous pouvez créer des intégrations personnalisées pour permettre le traitement d'événements non classés.

invite

Une *invite* est un type de requête spécial qui affiche des résultats en fonction de la valeur que vous saisissez et des champs CEG que vous sélectionnez. Les lignes sont uniquement renvoyées pour les événements dont la valeur saisie apparaît dans au moins un des champs CEG sélectionnés.

jeton d'analyse de message (ELM)

Un *jeton d'analyse de message* est un modèle réutilisable servant à la création de la syntaxe d'expression régulière utilisée lors de l'analyse de message CA Enterprise Log Manager. A chaque jeton sont associés un nom, un type et une chaîne d'expression régulière.

journal

Un *journal* est un enregistrement d'audit, ou message enregistré, concernant un événement ou un ensemble d'événements. Un journal peut afficher différents types : journal d'audit, journal de transaction, journal d'intrusion, journal de connexion, enregistrement des performances système, journal des activités utilisateur ou alerte.

Liaison de variable

Une *liaison de variable* est une liaison de variable SNMP. Chaque liaison de variable est formée d'un OID, d'un type, et d'une valeur. Les liaisons de variable s'ajoutent à une MIB personnalisée.

liste de contrôle d'accès d'identité

Une *liste de contrôle d'accès d'identité* vous permet de spécifier différentes actions que chaque identité sélectionnée peut exécuter sur les ressources indiquées. Par exemple, avec une liste de contrôle d'accès d'identité, vous pouvez préciser qu'une identité donnée peut créer des rapports et qu'une autre peut planifier et annoter des rapports. La liste de contrôle d'accès d'identité diffère de la liste de contrôle d'accès classique dans le sens où elle est centrée sur l'identité, et non sur la ressource.

magasin de journaux d'événements

Le *magasin de journaux d'événements* est un composant du serveur CA Enterprise Log Manager, dans lequel les événements entrants sont stockés dans des bases de données. Les bases de données du magasin de journaux d'événements doivent être sauvegardées et déplacées manuellement vers un système de stockage distant de journaux, avant le délai de suppression configuré. Les bases de données archivées peuvent être restaurées dans un magasin de journaux d'événements.

magasin d'utilisateurs

Un *magasin d'utilisateurs* est le référentiel contenant les informations et stratégies de mots de passe d'utilisateurs globaux. Par défaut, le magasin d'utilisateurs CA Enterprise Log Manager est le référentiel local, mais il peut être configuré pour faire référence à CA SiteMinder ou à un répertoire LDAP pris en charge, comme Microsoft Active Directory, Sun One ou Novell eDirectory. Quelle que soit la configuration du magasin d'utilisateurs, le référentiel local sur le serveur de gestion contient des informations spécifiques aux applications concernant les utilisateurs, comme leur rôle et les stratégies d'accès associées.

mappage de données

Le *mappage de données* est un processus consistant à mapper les paires de valeurs clés vers la CEG. Le mappage de données s'effectue sur la base d'un fichier de mappage de données.

mappages de fonctions

Les *mappages de fonctions* constituent une partie facultative du fichier de mappage de données pour une intégration produit. Ils servent à renseigner un champ de la grammaire commune aux événements lorsque la valeur requise ne peut être extraite directement de la source d'événement. Tous les mappages de fonctions se composent d'un nom de champ CEG, d'une valeur de champ de classe ou prédéfinie, ainsi que de la fonction utilisée pour obtenir ou calculer la valeur.

MIB (base de données d'informations de gestion)

La *MIB (base de données d'informations de gestion)* pour CA Enterprise Log Manager, CA-ELM.MIB, doit être importée et compilée par chaque produit devant recevoir des alertes sous la forme d'interruptions SNMP depuis CA Enterprise Log Manager. La MIB indique l'origine de chaque identificateur d'objet numérique (OID) utilisé dans un message d'interruption SNMP accompagnée d'une description de l'objet de données ou de l'élément de réseau en question. Dans la MIB pour les interruptions SNMP envoyées par CA Enterprise Log Manager, la description de chaque objet de données est destinée au champ CEG associé. La MIB permet de s'assurer que toutes les paires nom-valeur transmises dans une interruption SNMP sont correctement interprétées au niveau de la destination.

MIB personnalisée

Une *MIB personnalisée* est une MIB créée pour une alerte d'action envoyée vers une destination d'interruption SNMP (par exemple, CA NSM). L'ID d'interruption personnalisée spécifié dans l'alerte d'action implique l'existence d'une MIB personnalisée associée définissant les champs CEG sélectionnés envoyés sous forme d'interruption.

mises à jour d'abonnement

Les *mises à jour d'abonnement* correspondent aux fichiers binaires et non binaires mis à disposition par le serveur d'abonnement CA. Les fichiers binaires sont des mises à jour du module produit, généralement installées sur les systèmes CA Enterprise Log Manager. Les fichiers non binaires, ou mises à jour de contenu, sont enregistrés sur le serveur de gestion.

mises à jour du contenu

Les *mises à jour de contenu* constituent la partie non binaire des mises à jour d'abonnement et elles sont enregistrées sur le serveur de gestion CA Enterprise Log Manager. Les mises à jour de contenu incluent les fichiers XMP, les fichiers de mappage de données, les mises à jour de configuration pour les modules CA Enterprise Log Manager et les mises à jour de clé publique.

Mode non FIPS

Le *mode non FIPS* est un paramètre par défaut qui permet aux serveurs et agents CA Enterprise Log Manager d'utiliser une combinaison de techniques de chiffrement, dont certaines ne sont pas conformes à la FIPS. Le paramètre alternatif est le mode non FIPS.

module (à télécharger)

Un *module* est un groupement logique de mises à jour de composant, mis à disposition des utilisateurs en téléchargement, sur la base d'un abonnement. Un module peut contenir des mises à jour de fichier binaire, de contenu, ou les deux. Par exemple, tous les rapports sont réunis dans un même module ; toutes les mises à jour de fichier binaire de sponsor sont regroupées dans un autre module. CA définit le contenu de chaque module.

module d'abonnement

Le *module d'abonnement* est le service qui permet de télécharger automatiquement les mises à jour d'abonnement à partir du serveur d'abonnement CA et de les distribuer à tous les serveurs et agents CA Enterprise Log Manager. Les paramètres globaux s'appliquent aux serveurs CA Enterprise Log Manager locaux ; les paramètres locaux indiquent notamment si le serveur est un proxy hors ligne, un proxy en ligne ou un client d'abonnement.

module d'extension d'événements iTech

Le *module d'extension d'événements iTech* est un adaptateur CA qu'un administrateur peut configurer à l'aide de fichiers de mappage sélectionnés. Il reçoit des événements provenant d'iRecorders, de CA EEM, d'iTechnology ou de tout produit capable d'envoyer des événements via iTechnology.

NIST

Le *National Institute of Standards and Technology (NIST)* est l'agence technologique fédérale américaine qui propose des recommandations dans une publication intitulée "*Special Publication 800-92 Guide to Computer Security Log Management*" (en anglais), qui ont servi de base pour CA Enterprise Log Manager.

nom d'utilisateur EiamAdmin

EiamAdmin est le nom de superutilisateur par défaut affecté au programme d'installation des serveurs CA Enterprise Log Manager. Lors de l'installation du premier logiciel CA Enterprise Log Manager, le programme d'installation crée un mot de passe pour ce compte de superutilisateur, sauf si un serveur CA EEM distant existe déjà. Dans ce cas, le programme d'installation doit entrer le mot de passe existant. Une fois le dispositif logiciel installé, le programme d'installation ouvre un navigateur à partir d'une station de travail, entre l'URL de CA Enterprise Log Manager et se connecte en tant qu'utilisateur EiamAdmin avec le mot de passe associé. Ce premier utilisateur configure le magasin d'utilisateurs, crée les stratégies de mots de passe et crée le premier compte d'utilisateur doté du rôle Administrator. L'utilisateur EiamAdmin peut également effectuer n'importe quelle opération contrôlée par CA EEM.

Norme FIPS 140-2

La *norme FIPS 140-2* est la norme fédérale de traitement de l'information (Federal Information Processing Standard). Cette norme fédérale spécifie les configurations requises de sécurité pour des modules cryptographiques utilisés dans un système de sécurité protégeant des informations sensibles mais non classifiées. La norme fournit quatre niveaux qualitatifs et d'amélioration de la sécurité visant à couvrir une vaste gamme d'applications et d'environnements potentiels.

OID (identificateur d'objet)

L'*OID (identificateur d'objet)* est l'identifiant numérique unique d'un objet de données apparié à une valeur dans un message d'interruption SNMP. Chaque OID utilisé dans une interruption SNMP envoyée par CA Enterprise Log Manager est mappé à un champ CEG dans la MIB. La syntaxe d'un OID mappé à un champ CEG est la suivante : 1.3.6.1.4.1.791.9845.x.x.x, où 791 est le numéro d'entreprise de CA et 9845 est l'identifiant produit de CA Enterprise Log Manager.

point de collecte

Un *point de collecte* est un serveur sur lequel un agent est installé ; sur le réseau, ce serveur est proche de tous les serveurs contenant les sources d'événements associées aux connecteurs de son agent.

pozFolder

pozFolder est un attribut d'AppObject, dont la valeur correspond à l'emplacement parent de l'AppObject. L'attribut et la valeur *pozFolder* sont utilisés dans les filtres de stratégies d'accès, qui restreignent l'accès aux ressources telles que les rapports, les requêtes et les configurations.

processus de sortie de l'événement/de l'alerte

Le *processus de sortie de l'événement/de l'alerte* est un processus CA IT PAM qui invoque un produit tiers pour répondre aux données d'alerte configurées dans CA Enterprise Log Manager. Vous pouvez sélectionner Processus CA IT PAM comme destination lorsque vous planifiez un job d'alerte. Lorsqu'une alerte déclenche l'exécution du processus CA IT PAM, CA Enterprise Log Manager envoie les données d'alerte CA IT PAM, lesquelles sont ensuite transférées par CA IT PAM avec leurs propres paramètres de traitement au produit tiers dans le cadre du processus de sortie de l'événement/de l'alerte.

profil

Un *profil* est un ensemble facultatif et configurable de filtres de données et de balises, qui peut être spécifique à un produit, à une technologie ou à une catégorie donnée. Le filtre de balise d'un produit, par exemple, limite les balises répertoriées à la balise du produit sélectionné. Les filtres de données d'un produit affichent uniquement les données pour le produit spécifié dans les rapports que vous générez, les alertes que vous planifiez et les résultats de requête que vous affichez. Une fois créé le profil de votre choix, vous pouvez le configurer de manière à ce qu'il soit appliqué dès que vous vous connectez au système. Si vous créez plusieurs profils, vous pouvez appliquer un profil différent à différentes activités, lors d'une même session. Des filtres prédéfinis sont livrés avec les mises à jour d'abonnement.

proxies d'abonnement (pour le client)

Les *proxies d'abonnement pour le client* définissent la liste des proxies d'abonnement que le client contacte de manière circulaire pour obtenir les mises à jour du système d'exploitation et du logiciel CA Enterprise Log Manager. Si un proxy est occupé, le suivant sur la liste est contacté. Si tous les proxies sont indisponibles et que le client est en ligne, le proxy d'abonnement par défaut est utilisé.

proxies d'abonnement (pour les mises à jour de contenu)

Les *proxies d'abonnement pour les mises à jour de contenu* sont les proxies d'abonnement choisis pour mettre à jour le serveur de gestion CA Enterprise Log Manager avec les mises à jour de contenu téléchargées sur le serveur d'abonnement CA. Il est recommandé de configurer plusieurs proxies, à des fins de redondance.

proxy d'abonnement (en ligne)

Un *proxy d'abonnement en ligne* est un serveur CA Enterprise Log Manager doté d'un accès à Internet et chargé de récupérer les mises à jour d'abonnement auprès du serveur d'abonnement CA, de manière régulière et planifiée. Un proxy d'abonnement en ligne donné peut être inclus dans la liste des proxies pour un ou plusieurs clients, qui contactent les proxies répertoriés de manière circulaire afin de demander les mises à jour de fichiers binaires. S'il est configuré pour le faire, un proxy en ligne donné peut envoyer les nouvelles mises à jour de contenu et de configuration au serveur de gestion, sauf si cela a déjà été fait par un autre proxy. Le répertoire des mises à jour d'abonnement d'un proxy en ligne sélectionné est utilisé comme source pour copier les mises à jour sur les proxies d'abonnement hors ligne.

proxy d'abonnement (hors ligne)

Un *proxy d'abonnement hors ligne* est un serveur CA Enterprise Log Manager qui obtient les mises à jour d'abonnement par une copie de répertoire manuelle (à l'aide de scp) depuis un proxy d'abonnement en ligne. Les proxies d'abonnement hors ligne peuvent être configurés pour télécharger les mises à jour de fichiers binaires sur les clients qui les demandent et pour envoyer la dernière version des mises à jour de contenu au serveur de gestion, si celui-ci ne l'a pas déjà reçue. Les proxies d'abonnement hors ligne n'ont pas besoin d'accès à Internet.

proxy d'abonnement (par défaut)

Le *proxy d'abonnement par défaut* est généralement le serveur CA Enterprise Log Manager installé en premier ; il peut également s'agir du serveur CA Enterprise Log Manager principal. Ce serveur sert également de proxy d'abonnement en ligne et doit, par conséquent, être doté d'un accès à Internet. Si aucun autre proxy d'abonnement en ligne n'est défini, ce serveur obtient les mises à jour d'abonnement auprès du serveur d'abonnement CA, puis télécharge les mises à jour de fichiers binaires sur tous les clients et envoie les mises à jour de contenu à CA EEM. Si d'autres proxies sont définis, le serveur obtient tout de même les mises à jour d'abonnement, mais il est contacté par les clients uniquement lorsque aucune liste de proxies d'abonnement n'est configurée ou lorsque la liste configurée est épuisée.

rapport

Un *rapport* est une représentation graphique ou tabulaire des données de journal d'événements qui est générée en exécutant des requêtes prédéfinies ou personnalisées à l'aide de filtres. Les données peuvent être issues de bases de données chaudes, tièdes et dégivrées dans le magasin de journaux d'événements du serveur sélectionné et, sur demande, de ses serveurs fédérés.

rapports EPHI

Les *rapports EPHI* (Electronic Protected Health Information) sont des rapports relatifs à la sécurité HIPAA (Health Insurance Portability and Accountability Act). Ces rapports peuvent vous aider à démontrer que toutes les informations médicales associées aux patients et identifiables individuellement, qui sont créées, stockées et transmises de manière électronique, sont protégées.

recatalogage

Le *recatalogage* est une révision forcée du catalogue. Un recatalogage est requis uniquement lors de la restauration de données dans un magasin de journaux d'événements situé sur un serveur différent de celui sur lequel les données ont été générées. Par exemple, si vous avez désigné CA Enterprise Log Manager comme point de restauration pour l'examen des données sauvegardées, vous devez imposer un recatalogage de la base de données après l'avoir restaurée depuis son point de restauration désigné. Un recatalogage est exécuté automatiquement au redémarrage d'iGateway, si nécessaire. Recataloguer un seul fichier de base de données peut prendre plusieurs heures.

règles de récapitulation

Les *règles de récapitulation* sont des règles combinant certains événements natifs, d'un même type, en un seul événement ajusté. Par exemple, une règle de récapitulation peut être configurée pour remplacer par un seul événement de récapitulation jusqu'à 1 000 événements dupliqués, dont les adresses IP et les ports source et de destination sont identiques. De telles règles simplifient l'analyse des événements et réduisent le trafic associé aux journaux.

règles de suppression

Les *règles de suppression* sont des règles que vous configurez pour éviter que certains événements ajustés n'apparaissent dans vos rapports. Vous pouvez créer des règles de suppression permanentes afin de supprimer des événements de routine sans rapport avec des problèmes de sécurité ; vous pouvez également créer des règles temporaires afin de supprimer la journalisation d'événements planifiés tels que la création de nombreux utilisateurs.

règles de transfert d'événement

Les *règles de transfert d'événement* stipulent que les événements sélectionnés sont transférés à des produits tiers, par exemple ceux qui mettent les événements en corrélation, après leur sauvegarde dans le magasin des journaux d'événements.

requête

Une *requête* est un ensemble de critères utilisés pour effectuer une recherche dans les magasins de journaux d'événements du serveur CA Enterprise Log Manager actif et, le cas échéant, de ses serveurs fédérés. Une requête cible les bases de données chaudes, tièdes ou dégivrées spécifiées dans la clause *where* de la requête. Par exemple, si la clause *where* limite la requête aux événements pour lesquels *source_username="myname"* sur une période donnée et que seules dix des 1 000 bases de données contiennent des enregistrements répondant à ces critères, sur la base des informations fournies dans la base de données de catalogue, la requête sera exécutée uniquement sur ces dix bases de données. Une requête peut renvoyer 5 000 lignes de données au maximum. Tout utilisateur doté d'un rôle prédéfini peut exécuter une requête. Seuls les analystes et les administrateurs peuvent planifier une requête pour diffuser une alerte d'action, créer un rapport en sélectionnant les requêtes à inclure, ou encore créer une requête personnalisée à l'aide de l'assistant de conception de requête. Voir également requête d'archivage.

requête d'action

Une *requête d'action* est une requête prenant en charge une alerte d'action. Elle est exécutée de manière planifiée et récurrente, pour tester les conditions définies par l'alerte d'action à laquelle elle est associée.

requête d'archivage

Une *requête d'archivage* est une requête du catalogue utilisée pour identifier les bases de données froides devant être restaurées et dégivrées à des fins de requête. Une requête d'archivage diffère d'une requête normale dans le sens où elle cible les bases de données froides, tandis que les requêtes normales ciblent uniquement les bases chaudes, tièdes et dégivrées. Les administrateurs peuvent émettre une requête d'archivage grâce à l'option Requête de catalogue d'archive du sous-onglet Collecte de journaux, dans l'onglet Administration.

ressource d'application

Le terme *ressource d'application* correspond à toutes les ressources spécifiques à CA Enterprise Log Manager, sur lesquelles les stratégies d'accès CALM autorisent ou interdisent à des identités données d'effectuer certaines actions spécifiques à l'application, par exemple créer, planifier et modifier. Rapport, alerte et intégration sont des exemples de ressource d'application. Voir également ressource globale.

ressource globale

Une *ressource globale*, pour le produit CA Enterprise Log Manager, est une ressource partagée avec les autres applications CA. Vous pouvez créer des stratégies de portée pour les ressources globales. Utilisateur, stratégie et calendrier sont des exemples de ressource globale. Voir également ressource d'application.

rôle Administrator

Le *rôle Administrator* accorde aux utilisateurs la possibilité d'effectuer toutes les actions valides existantes sur l'ensemble des ressources CA Enterprise Log Manager. Seuls les utilisateurs Administrator sont autorisés à configurer les services et la collecte de journaux, ou encore à gérer les utilisateurs, les stratégies d'accès et les filtres d'accès.

rôle Analyst

Le *rôle Analyst* accorde aux utilisateurs la possibilité de créer et de modifier des requêtes et rapports personnalisés, de modifier et d'annoter les rapports, de créer des balises, ou encore de planifier des rapports et alertes d'action. Les utilisateurs Analyst peuvent également réaliser toutes les tâches du rôle Auditor.

rôle Auditor

Le *rôle Auditor* accorde aux utilisateurs l'accès aux rapports et à leurs données. Les utilisateurs Auditor peuvent afficher les rapports, la liste des modèles de rapport, la liste des jobs de rapports planifiés et la liste des rapports générés. Les utilisateurs Auditor peuvent planifier et annoter des rapports. Ils n'ont pas accès aux flux RSS (Rich Site Summary), à moins qu'aucune authentification ne soit requise pour l'affichage des alertes d'action.

rôle d'utilisateur

Un *rôle d'utilisateur* peut être un groupe d'utilisateurs d'applications prédéfini ou un groupe d'applications défini par l'utilisateur. Des rôles d'utilisateur personnalisés sont nécessaires lorsque les groupes d'applications prédéfinis (Administrator, Analyst et Auditor) ne sont pas suffisamment affinés pour refléter les attributions de tâches. Les rôles d'utilisateur personnalisés nécessitent des stratégies d'accès personnalisées et une modification des stratégies prédéfinies pour inclure le nouveau rôle.

routeur SAPI

Le *routeur SAPI* est un adaptateur CA qui reçoit les événements provenant des intégrations, de type Mainframe, et les renvoie au routeur CA Audit.

SafeObject

SafeObject est une classe de ressource prédéfinie dans CA EEM. Il s'agit de la classe de ressource à laquelle appartient AppObjects, stockée dans la portée de l'application. Les utilisateurs définissant des stratégies et des filtres permettant d'accéder aux AppObjects se réfèrent à cette classe de ressource.

SAPI Recorder

SAPI Recorder était la technologie utilisée pour envoyer les données à CA Audit, avant l'apparition d'iTechnology. SAPI signifie Submit API (Application Programming Interface) ou API de soumission. Les enregistreurs CA Audit pour CA ACF2, CA Top Secret, RACF, Oracle, Sybase et DB2 sont des exemples de SAPI Recorders.

serveur d'abonnement CA

Le *serveur d'abonnement CA* est la source des mises à jour d'abonnement de CA.

serveur d'alerte

Le *serveur d'alerte* sert à stocker les alertes d'action et les jobs d'alerte d'action.

serveur de collecte

Le *serveur de collecte* est un rôle attribué à un serveur CA Enterprise Log Manager. Le serveur de collecte ajuste les journaux d'événement entrants, les intègre à la base de données chaude, compresse celle-ci et en effectue un archivage automatique ou bien la copie sur le serveur de rapports associé. Le serveur de collecte compresse la base de données chaude lorsqu'elle atteint la taille maximale prédéfinie et effectue un archivage automatique selon le planning indiqué.

serveur de gestion

Le *serveur de gestion* est un rôle attribué au premier serveur CA Enterprise Log Manager installé. Ce serveur CA Enterprise Log Manager contient le référentiel chargé de stocker le contenu de tous ses serveurs CA Enterprise Log Manager, notamment les stratégies. Ce serveur correspond généralement au proxy d'abonnement par défaut. Bien que cela ne soit pas recommandé dans la plupart des environnements de production, le serveur de gestion peut prendre en charge tous les rôles.

serveur de point de restauration

Le *serveur de point de restauration* est un rôle attribué à un serveur CA Enterprise Log Manager. Pour étudier des événements sauvegardés, vous pouvez transférer des bases de données depuis le serveur de stockage distant jusqu'au serveur de point de restauration à l'aide d'un utilitaire, puis ajouter ces bases au catalogue et exécuter les requêtes de votre choix. Transférer des bases de données froides vers un point de restauration dédié est une alternative intéressante à la restauration de ces bases sur le serveur de rapports original.

serveur de rapports

Le *serveur de rapports* est le service qui stocke les informations de configuration, telles que le serveur de messagerie à utiliser lors de l'envoi des alertes par courriel, l'apparence des rapports enregistrés au format PDF, ainsi que la conservation des stratégies pour les rapports enregistrés sur le serveur de rapports et les alertes envoyées au flux RSS.

serveur de rapports

Le *serveur de rapports* est un rôle attribué à un serveur CA Enterprise Log Manager. Le serveur de rapports reçoit les bases de données tièdes archivées automatiquement en provenance d'un ou plusieurs serveurs de collecte. Il traite les requêtes, les rapports, ainsi que les alertes et les rapports planifiés.

serveur de stockage distant

Le *serveur de stockage distant* est un rôle attribué à un serveur qui reçoit les bases de données archivées automatiquement en provenance d'un ou plusieurs serveurs de rapports. Le serveur de stockage distant conserve les bases de données froides pendant le nombre d'années requis. L'hôte distant utilisé pour le stockage ne dispose généralement pas d'un système CA Enterprise Log Manager ou autre. Pour l'archivage automatique, configurez une authentification non interactive.

serveur ODBC

Le *serveur ODBC* est le service configuré qui définit le port utilisé pour les communications entre le client ODBC ou JDBC et le serveur CA Enterprise Log Manager et détermine si le chiffrement SSL est activé ou non.

serveur proxy HTTP

Un *serveur proxy HTTP* est un serveur proxy qui joue le rôle de pare-feu et empêche le trafic Internet de pénétrer dans l'entreprise ou de la quitter, hormis via le proxy. Le trafic sortant peut spécifier un ID et un mot de passe pour contourner le serveur proxy. L'utilisation d'un serveur proxy HTTP local dans la gestion de l'abonnement est configurable.

serveurs de fédération

Les *serveurs de fédération* sont des serveurs CA Enterprise Log Manager connectés les uns aux autres sur un réseau, afin de répartir la collecte des données de journal, tout en cumulant les données collectées à des fins de génération de rapports. Les serveurs de fédération peuvent être connectés selon une topologie hiérarchique ou maillée. Les rapports de données fédérées incluent celles provenant du serveur cible, ainsi que de ses enfants ou pairs, le cas échéant.

services

Les *services* CA Enterprise Log Manager sont le magasin de journaux d'événements, le serveur de rapports et l'abonnement. Les administrateurs configurent ces services au niveau global, où tous les paramètres s'appliquent à l'ensemble de CA Enterprise Log Manager par défaut. La plupart des paramètres globaux de services peuvent être remplacés au niveau local, pour CA Enterprise Log Manager donné.

SNMP

SNMP est l'acronyme de Simple Network Management Protocol (protocole simple de gestion de réseau), une norme ouverte de transmission de messages d'alerte sous la forme d'interruptions SNMP depuis un agent vers un ou plusieurs systèmes de gestion.

source d'événement

Une *source d'événement* est l'hôte à partir duquel un connecteur collecte des événements bruts. Une source d'événement peut contenir plusieurs magasins de journaux, tous accessibles via un connecteur différent. En général, le déploiement d'un nouveau connecteur implique la configuration de la source d'événement de sorte que l'agent puisse y accéder et lire les événements bruts à partir de l'un de ses magasins de journaux. Les événements bruts du système d'exploitation, des bases de données différentes et une variété d'applications de sécurité sont stockés séparément sur la source d'événement.

stockage des journaux d'événements

Le *stockage des journaux d'événements* est le résultat du processus d'archivage, lorsque l'utilisateur sauvegarde une base de données tiède, avertit CA Enterprise Log Manager en exécutant l'utilitaire LMArchive et déplace la base de données sauvegardée depuis le magasin de journaux d'événements jusqu'à l'emplacement de stockage à long terme.

stratégie d'accès

Une *stratégie d'accès* est une règle qui accorde ou refuse à une identité (utilisateur ou groupe d'utilisateurs) des droits d'accès à une ressource d'application. CA Enterprise Log Manager détermine si les stratégies s'appliquent à l'utilisateur concerné en faisant correspondre les identités, les ressources, les classes de ressources et en évaluant les filtres.

stratégie d'accès aux applications CALM

La *stratégie d'accès aux applications CALM* est une stratégie de portée de type Liste de contrôle d'accès, qui détermine qui peut se connecter au serveur CA Enterprise Log Manager. Par défaut, la connexion est autorisée pour les rôles Administrator [Groupe], Analyst [Groupe] et Auditor [Groupe].

stratégie de délégation

Une *stratégie de délégation* est une stratégie d'accès qui permet à un utilisateur de déléguer son autorité à un autre utilisateur, groupe d'applications, groupe global ou groupe dynamique. Vous devez supprimer explicitement les stratégies de délégation créées par un utilisateur supprimé ou désactivé.

stratégie de portée

Une *stratégie de portée* est un type de stratégie d'accès qui octroie ou interdit l'accès aux ressources stockées sur le serveur de gestion, notamment les AppObjects, les utilisateurs, les groupes, les dossiers et les stratégies. Une stratégie de portée définit les identités pouvant accéder aux ressources spécifiées.

stratégie d'obligation

Une *stratégie d'obligation* est une stratégie générée automatiquement lorsque vous créez un filtre d'accès. Vous ne pouvez pas créer, modifier ou supprimer directement une stratégie d'obligation. Vous devez plutôt créer, modifier ou supprimer le filtre d'accès correspondant.

suppression

La *suppression* est le processus de tri des événements sur la base de filtres CEG. La suppression s'effectue sur la base de fichiers SUP.

traitement des valeurs dynamiques

Un *traitement des valeurs dynamiques* est un processus CA IT PAM que vous pouvez invoquer pour renseigner ou mettre à jour la liste de valeurs d'une clé donnée utilisée dans des rapports ou des alertes. Vous fournissez le chemin d'accès au traitement des valeurs dynamiques lors de la configuration de CA IT PAM dans la liste des services de serveurs de rapports de l'onglet Administration. Vous cliquez sur Importer la liste des valeurs dynamiques dans la section Valeur associée aux valeurs clés sur la même page de l'interface utilisateur. L'invocation du traitement des valeurs dynamiques est l'une des trois méthodes qui vous permettent d'ajouter des valeurs à vos clés.

URL de CA Embedded Entitlements Manager

L'*URL de CA Embedded Entitlements Manager (CA EEM)* est : https://<adresse_ip>:5250/spin/eiam. Pour ouvrir une session, sélectionnez CAELM comme application et saisissez le mot de passe associé au nom d'utilisateur EiamAdmin.

URL de CA Enterprise Log Manager

L'*URL de CA Enterprise Log Manager* est : https://<adresse_ip>:5250/spin/calm. Pour ouvrir une session, saisissez le nom d'utilisateur défini pour votre compte par l'administrateur, puis le mot de passe associé. Vous pouvez également saisir le nom de superutilisateur par défaut, EiamAdmin, puis entrer le mot de passe associé.

URL du flux RSS pour l'abonnement

L'*URL du flux RSS pour l'abonnement* est un lien préconfiguré, utilisé par les serveurs proxy d'abonnement en ligne lors de la récupération des mises à jour d'abonnement. Cette URL est destinée au serveur d'abonnement CA.

URL du flux RSS pour les alertes d'action

L'*URL du flux RSS pour les alertes d'action* est : <https://{nomhôteelm}:5250/spin/calm/getActionQueryRssFeeds.csp>. A partir de cette URL, vous pouvez afficher les alertes d'action soumises à la configuration définie en termes de quantité et d'ancienneté maximales.

utilisateur d'application

Un *utilisateur d'application* est un utilisateur global auquel ont été attribués des détails au niveau de l'application. Les détails d'utilisateur d'application CA Enterprise Log Manager incluent le groupe d'utilisateurs et les éventuelles restrictions d'accès. Si le magasin d'utilisateurs est le référentiel local, les détails de l'utilisateur d'application incluent également les informations d'identification de connexion et les stratégies de mots de passe.

utilisateur EEM

L'*utilisateur EEM*, configuré dans la section Archivage automatique du Magasin de journaux d'événements, spécifie l'utilisateur autorisé à exécuter une requête d'archivage, à recataloguer la base de données d'archivage, à exécuter l'utilitaire LMArchive et à exécuter le script shell restore-ca-elm pour restaurer les bases de données d'archivage à des fins d'examen. Cet utilisateur doit posséder le rôle prédéfini Administrator ou un rôle personnalisé associé à une stratégie personnalisée qui autorise l'action Modifier sur la ressource Base de données.

utilisateur global

Un *utilisateur global* se compose des informations de compte d'utilisateur, à l'exclusion des données propres aux applications. Les détails de l'utilisateur global et les appartenances au groupe global sont partagés par l'ensemble des applications CA intégrant le magasin d'utilisateurs par défaut. Les détails de l'utilisateur global peuvent être stockés dans le référentiel intégré ou dans un répertoire externe.

utilitaire LMArchive

LMArchive est l'utilitaire de ligne de commande qui suit la sauvegarde et la restauration des bases de données d'archive vers le magasin de journaux d'événements d'un serveur CA Enterprise Log Manager. Utilisez LMArchive pour effectuer une requête sur la liste des fichiers de bases de données tièdes, prêts à être archivés. Après avoir sauvegardé la base de données répertoriée et l'avoir transférée sur un stockage à long terme (froid), utilisez LMArchive pour créer un enregistrement sur CA Enterprise Log Manager, indiquant que cette base de données a été sauvegardée. Suite à la restauration d'une base de données froide sur son CA Enterprise Log Manager d'origine, utilisez LMArchive pour notifier CA Enterprise Log Manager, qui place alors les fichiers de bases de données dans un état dégivré, accessible aux requêtes.

utilitaire LMSEOSImport

LMSEOSImport est un utilitaire de ligne de commande utilisé pour importer SEOSDATA, ou des événements existants, dans CA Enterprise Log Manager dans le cadre de la migration depuis le générateur de rapports, la visionneuse ou le collecteur d'Audit. L'utilitaire est pris en charge uniquement par Microsoft Windows et Sun Solaris Sparc.

utilitaire scp

La copie sécurisée *scp* (programme de copie de fichiers à distance) est un utilitaire UNIX qui permet de transférer des fichiers entre les ordinateurs UNIX d'un réseau. Cet utilitaire est fourni lors de l'installation CA Enterprise Log Manager, pour que vous puissiez transférer les fichiers de mise à jour d'abonnement depuis le proxy d'abonnement en ligne jusqu'au proxy d'abonnement hors ligne.

valeurs clés

Les *valeurs clés* sont des valeurs définies par l'utilisateur et affectées à une liste définie par l'utilisateur (groupe clé). Lorsqu'une requête utilise un groupe clé, les résultats de la recherche incluent les correspondances avec toutes les valeurs clés du groupe. Il existe plusieurs groupes clés prédéfinis ; certains contiennent des valeurs clés prédéfinies, utilisées dans les requêtes et rapports prédéfinis.

Index

A

- adaptateurs CA
 - configuration pour l'utilisation avec CA Audit - 251, 255
- agent par défaut
 - configuration d'un connecteur à l'aide du détecteur de journal OBDC - 216
 - configuration d'un connecteur à l'aide du détecteur de journal WinRM - 223
- agents
 - A propos de - 66
 - A propos des groupes d'agents - 67
 - affichage de l'état - 229
 - agent par défaut - 213
 - droits des comptes d'utilisateur - 67
 - installation - 211
 - planification pour - 63
- archivage
 - A propos des fichiers d'archive - 158
 - exemple - 175
- authentification non interactive
 - configuration de l'archivage automatique - 162
 - exemple de topologie en étoile - 164
 - exemple du plus simple cas d'utilisation - 173

B

- base de données de gestion CA (CA MDB)
 - magasin d'utilisateurs - 140
- bibliothèque d'ajustement d'événement
 - A propos de - 239
 - prise en charge de nouvelles sources d'événement - 240

C

- CA Audit
 - Configuration d'adaptateurs CA - 251
 - différences d'architecture - 243

- envoi d'événements à CA Enterprise Log Manager - 256
- modification de la stratégie r8 SP1 CR2 existante - 258
- modification de la stratégie r8 SP2 existante - 260
- Quand importer des événements - 261
- remarques pour les utilisateurs de - 243
- CA Embedded Entitlements Manager
 - définition - 32
- CA Enterprise Log Manager
 - fédération - 34
 - installation - 83
 - planification de l'architecture - 73
 - processus - 113
- collecte de journaux
 - instructions - 33
 - planification - 29
- compte caelmadmin
 - définition - 109
- comptes d'utilisateurs
 - ajout d'un groupe d'utilisateurs d'applications - 148
- configurations
 - configurations initiales du serveur - 108
- connecteurs
 - A propos des détecteurs de journaux - 69
 - affichage de l'état - 229
 - arrêt et redémarrage - 229

D

- détecteurs de journaux
 - A propos de - 69

E

- écouteur d'événements iTechnology
 - A propos de - 255
- espace disque
 - planification - 31
- événements d'autosurveillance
 - affichage - 88

exemples

- archivage automatique sur trois serveurs - 175
- collecte directe des journaux de base de données - 216
- collecte directe des journaux Windows - 223
- configuration d'abonnement avec six serveurs - 61

F

fédération

- à propos des requêtes et des rapports dans - 231
- carte de fédération - 35
- configuration - 235
- exemple de mappage de fédérations pour une grande entreprise - 37
- exemple de mappage de fédérations pour une moyenne entreprise - 39
- hiérarchique - 232
- maillée - 234
- planification - 34
- sélection de requêtes fédérées - 156

feuilles de calcul

- CA SiteMinder - 46
- répertoire LDAP externe - 44

filtres

- globaux et locaux - 155

G

gestion de l'abonnement

- exemple de configuration - 61

gestion des utilisateurs et des accès

- configuration du magasin d'utilisateurs - 140

I

importation

- événements SEOSDATA provenant de CA Audit - 263, 271

installation

- CA IT PAM avec CA EEM partagé - 299
- créer des DVD d'installation - 75
- de CA Enterprise Log Manager - 83
- dépannage - 127

Image du système d'exploitation personnalisé - 110

- Structure des répertoires par défaut - 110
- sur un système disposant de lecteurs SAN - 100

vérifier le serveur CA Enterprise Log Manager - 87

intégration à CA Audit

- Configuration d'adaptateurs CA - 251
- Envoi d'événements CA Audit à CA Enterprise Log Manager - 256
- importation d'événements SEOSDATA - 263
- présentation des architectures - 243
- Quand importer des événements - 261

intégrations

- A propos de - 67

L

Lecteurs SAN

- installation de CA Enterprise Log Manager avec des lecteurs activés - 107
- installation de CA Enterprise Log Manager avec des lecteurs désactivés - 101

M

magasin de journaux d'événements

- A propos de - 158
- A propos des fichiers d'archive - 158
- configuration - 157, 183
- paramètres de base - 181

magasin d'utilisateurs

- configuration comme CA-MDB - 140
- Feuille de calcul CA SiteMinder - 46
- Feuille de calcul du répertoire LDAP externe - 44
- planification - 42
- référence à CA SiteMinder - 142
- référence à un répertoire LDAP - 141

module d'extension

- module d'extension d'événements iTechnology - 255
- module d'extension d'événements module d'extension d'événements iTechnology - 255

P

planification

- dimensionnement - 70
- espace disque - 31
- fédération - 34
- intégration à CA Audit - 243
- magasin d'utilisateurs - 42
- récupération après sinistre - 311
- stratégies de mots de passe - 47

ports

- adaptateur réseau - 129
- pare-feu, pour les événements Syslog - 116

processus iGateway

- compte d'utilisateur pour le contrôle - 109
- contrôle - 84

R

récupération après sinistre

- planification - 311
- remplacement d'un serveur CA Enterprise Log Manager - 317
- restauration d'un serveur CA Embedded Entitlements Manager - 314
- restauration d'un serveur CA Enterprise Log Manager - 315
- sauvegarde d'un serveur CA Embedded Entitlements Manager - 312, 313
- sauvegarde d'un serveur CA Enterprise Log Manager - 315

règles de suppression

- effets - 71

rôles des serveurs

- dans les rapports fédérés - 37

rôles d'utilisateur

- attribution - 148

S

stratégies de mots de passe

- configuration - 144
- planification - 47

Syslog

- collecte définie - 63

T

tâches d'administration

- magasin d'utilisateurs - 140

U

utilitaire LMSeosImport

- à propos de l'utilitaire - 262
- copie sur le serveur d'outils de données Solaris - 264
- copie sur le serveur d'outils de données Windows - 265
- exemples de ligne de commande - 268
- importation à partir du serveur d'outils de données Solaris - 271
- Importation à partir d'une table SEOSDATA en temps réel - 262
- importation d'événements à partir du serveur d'outils de données Windows - 271
- options d'importation - 266
- Quand importer des événements - 261
- utilisation de la ligne de commande - 265