CA Embedded Entitlements Manager

Manuel de mise en oeuvre

r8.4 SP3

Produits CA référencés

Ce document contient des références aux produits CA suivants :

- CA® Embedded Entitlements Manager (CA EEM)
- CA® Directory
- CA® SiteMinder® Web Access Manager (CA SiteMinder)
- CA® Identity Manager
- CA® Security Command Center
- CA® Integrated Threat Management
- CA® Enterprise Log Manager

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.

Table des matières

Chapitre 1 : Introduction 9

Présentation 9
Fonctions 9
Fonctionnalités 10
Accès client 11
Magasin de données pris en charge 11

Chapitre 2 : Installation sous Windows 13

Présentation de l'installation 13
Installation du serveur 14
Liste de contrôle de configuration de l'assistant 14
Non-affichage de l'écran du chemin du JRE dans l'assistant d'installation 15
    Définition du paramètre Javahome 15
Installation du serveur à l'aide de l'assistant d'installation 16
Mise à niveau du serveur 17
Démarrage du serveur 18
Activation de l'accessibilité dans le serveur CA EEM 19
Suppression du serveur 20
Installer SDK 20
Démarrage du kit de développement logiciel 21
Suppression du kit de développement logiciel 21
Paramètres d'installation du serveur 21
Installation du serveur CA EEM en mode silencieux 23
    Création du fichier de réponse 24
    Exécution de la commande spécifiant le fichier de réponse 24
Suppression du serveur CA EEM en mode silencieux 25

Chapitre 3 : Installation sous Linux et UNIX 27

Présentation de l'installation 27
Installation du serveur 28
Mise à niveau du serveur 29
Suppression du serveur 29
Installation du kit de développement logiciel 30
Démarrage du SDK de CA EEM 30
Suppression du kit de développement logiciel 31
Paramètres du script d'installation du serveur 32

Installation du serveur en mode silencieux 34
Suppression du serveur CA EEM en mode silencieux 34

Chapitre 4 : Configuration du SDK CA EEM 35

Nouveaux fichiers binaires nécessaires à la création d'applications à l'aide du SDK CA EEM 35
Création d'applications à l'aide des nouveaux fichiers binaires Java 36
Fichiers requis pour exécuter les applications utilisant le SDK C++ de CA EEM 37
Création d'applications à l'aide des nouveaux fichiers binaires C++ 38
Fichiers requis pour la création et l'exécution des applications utilisant le SDK C# CA EEM 39
Mise en package du SDK C# de CA EEM dans les applications 39
Configuration du SDK CA EEM 39
A propos du fichier eiam.config 40
Activation de la journalisation iTechnology de SDK 43
Avant la configuration du SDK Java de CA EEM en mode FIPS uniquement 43
Configuration du SDK C++ de CA EEM en mode FIPS uniquement 44
Configuration du SDK C# de CA EEM en mode FIPS uniquement 45
Définition des informations SafeContext 45
Configuration du SDK Java CA EEM à l'aide de SafeConfigurator 46
Configuration du SDK CA EEM C++ 47
Initialisez le SDK C# de CA EEM 48

Chapitre 5 : Prise en charge de la norme FIPS 140-2 49

Présentation de la norme FIPS 140-2 49
Modes de sécurité pris en charge dans CA EEM 50
Configuration du serveur CA EEM en mode FIPS uniquement 51
Conditions requises pour la configuration du serveur CA EEM en mode FIPS uniquement. 51
Opérations préalables à la configuration de CA EEM en mode FIPS uniquement 52
Configuration du serveur CA EEM en mode FIPS uniquement. 52
Vérification du mode FIPS du serveur CA EEM 53
Communication entre le serveur CA EEM et les répertoires LDAP externes 54
Configuration de CA EEM pour l'utilisation des certificats de serveur dans un périphérique PKCS#11 54
Configuration de CA EEM pour le stockage des certificats de serveur dans un périphérique PKCS#11 55
Configuration de votre application en mode FIPS uniquement 56
Convertissez les certificats P12 utilisés par votre application en certificats PEM. 57
Initialisez le SDK de CA EEM en mode FIPS uniquement. 59

Chapitre 6 : Sauvegarde et restauration du serveur CA EEM 61

Sauvegarde du système de fichiers 61

Sauvegarde des fichiers et dossiers du serveur CA EEM 62
Procédures de restauration 63
Démarrage du service iGateway. 63
Arrêt du service iGateway 63

Chapitre 7 : Sauvegarde des données CA EEM stockées dans CA Directory 65

Introduction à la terminologie CA Directory 65
Utilisation de DXtools 66
Variable d'environnement DXHOME 66
Codes de sortie de DXtools 66
Sauvegarde des données CA Directory 68
Connexion à une console DSA locale 68
Vidage en ligne du magasin de données 69
Commande dump dxgrid-db : copie instantanée cohérente d'un magasin de données 70
Utilisation d'un fichier LDIF pour sauvegarder et charger des données 71
Outil DXdumpdb : exportation des données d'un magasin de données vers un fichier LDIF 72
Restauration des données CA Directory 73
Outil DXloaddb : chargement d'un magasin de données à partir d'un fichier LDIF 73

Chapitre 8 : Configuration du basculement 77

Basculement 77
Basculement du magasin de données d'application 78
Configuration du basculement du magasin de données d'application 79
Basculement du serveur CA EEM 83
Configuration des fichiers CA EEM 84

Chapitre 9 : Fédération d'artefacts 87

Activation de la fédération d'artefacts 87

Chapitre 10 : Intégration avec CA SiteMinder 89

Intégration de CA SiteMinder dans CA EEM 89
Configuration de la journalisation côté serveur CA EEM pour les modules CA SiteMinder 90

Chapitre 11 : Journalisation du SDK CA EEM 91

A propos des fichiers de configuration de l'enregistreur 92
Annexeur 92
Annexeur dans eiam.log4net.config 94
Enregistreur 96
Enregistreur racine 97

Configuration des fichiers de l'enregistreur 98
Exemple d'un fichier eiam.log4cxx.config 98
Exemple de fichier eiam.log4net.config 100
Exemple de fichier eiam.lo4j.config 102

Chapitre 12 : Configuration de la prise en charge d'un serveur de répertoire externe 105

Configuration d'un répertoire externe avec CA EEM 105
Configuration du serveur CA EEM pour l'échappement des barres obliques dans les noms de domaine renvoyés par les répertoires externes 107
Configuration de la prise en charge d'un basculement de répertoire externe 107
Connexion aux serveurs LDAP via TLS 108
Connexion à des serveurs LDAP via SSL 108
Connexion de CA EEM à un serveur LDAP via SSL 109
Configuration des connexions SSL 109
Configuration du serveur LDAP pour utiliser des certificats SSL 109
Activation de SSL dans le serveur CA EEM 110

Chapitre 13 : Configuration de la prise en charge d'un grand nombre de stratégies 111

Prise en charge d'un grand nombre de stratégies 111
Configuration d'autres paramètres du serveur CA EEM sur AIX 111
Configuration du client 112
Configuration du client pour tous les systèmes d'exploitation 112

Chapitre 14 : Archivage des événements 113

Présentation 113
Utilitaire de dégivrage des fichiers de base de données sauvegardée 114
Syntaxe de l'utilitaire SEM 115
Dégivrage des fichiers de base de données sauvegardée 116

Chapitre 1 : Introduction

Ce chapitre traite des sujets suivants :

Présentation (page 9)
Fonctions (page 9)
Fonctionnalités (page 10)
Accès client (page 11)
Magasin de données pris en charge (page 11)

Présentation

CA Embedded Entitlements Manager (CA EEM) permet aux applications de partager des services communs d'autorisation, d'authentification et de gestion des stratégies d'accès.

Fonctions

CA EEM propose un ensemble de services de sécurité. Les services de sécurité suivants sont disponibles.

- Services de configuration
  - Enregistrement et annulation de l'enregistrement des instances d'application
  - Portée administrative des administrateurs d'applications
  - Délégation des droits administratifs
  - Gestion des utilisateurs et des groupes
- Services de sécurité d'administration
  - Gestion des stratégies d'accès, d'événement et d'obligation
  - Gestion des calendriers
- Services de sécurité d'exécution
  - Authentification des utilisateurs
  - Autorisation d'accès
  - Journalisation des événements de sécurité

Fonctionnalités

CA EEM comprend les fonctionnalités suivantes.

Général

- La fonctionnalité d'isolation des stratégies permet à chaque instance d'application enregistrée d'utiliser son propre espace pour stocker les données propres à l'application.
- SDK d'exécution disponible pour Java, C++ et C#
- SDK administratif disponible pour Java, C++ et C#
- Prise en charge de l'interface de ligne de commande pour les fonctions administratives (insertion/modification/suppression des objets) :
  - Exportation/importation XML
  - Vérifications d'exécution
  - Outils de migration
- Prise en charge de l'interface Web pour l'accès autonome ou contextuel au lancement
- Communications HTTP sécurisées
- Intégration à CA Security Command Center et à CA Audit pour la gestion des événements de sécurité
- Intégration à CA SiteMinder pour la récupération d'informations de groupe et d'utilisateur du magasin de données CA SiteMinder

Gestion des identités

- Attributs et utilisateurs globaux partagés pour toutes les applications
- Prise en charge des différents modes pour les utilisateurs globaux
  - Utilisateurs globaux internes, avec gestion complète des stratégies de mots de passe
  - Utilisateurs globaux externes à partir de serveurs de répertoire LDAP
  - Utilisateurs globaux externes à partir de CA Identity Manager
- Intégration à CA Identity Manager pour la gestion et l'attribution d'utilisateurs d'après leur rôle
- Prise en charge de l'exportation/importation de sessions mobiles pour les connexions uniques

Gestion des accès

- La gestion des accès couvre à la fois les listes de contrôle d'accès (ACL, Access Control List) et les stratégies d'entreprise.

- Le langage de stratégie permet d'utiliser les attributs d'utilisateur, de session, d'environnement et de ressource afin d'établir les décisions liées aux stratégies.
- Portée administrative intégrée de tous les objets
- Prise en charge intégrée pour l'administration déléguée
- Prise en charge intégrée pour les vérifications d'obligation personnalisées exigeant des actions spécifiques à l'application
  - Evaluation locale des vérifications d'autorisation en cours de processus
  - SDK et interface Web pour définir les stratégies d'accès, les listes ACL, les stratégies de portée administrative et l'autorité déléguée

Accès client

Vous pouvez accéder au serveur CA EEM via le Web standard ou à partir d'interfaces de services Web qui permettent une intégration tierce sans recourir au module client. Les interfaces sont :

- HTML et iTechnology pour la configuration et l'administration ;
- iTechnology pour la remise d'événement CA Audit.

iTechnology est une technologie CA basée sur des normes Web telles que HTTP, HTTPS, HTML, XML et SSL. Elle offre un environnement de création et de déploiement de services Web via Internet.

Magasin de données pris en charge

CA EEM prend en charge l'identification d'une source d'utilisateurs externes spécifique telle que Microsoft Active Directory. CA EEM stocke sa configuration et ses stratégies dans CA Directory, quel que soit l'emplacement de stockage des objets utilisateur.

Chapitre 2 : Installation sous Windows

Ce chapitre traite des sujets suivants :

Présentation de l'installation (page 13)
Installation du serveur (page 14)
Liste de contrôle de configuration de l'assistant (page 14)
Non-affichage de l'écran du chemin du JRE dans l'assistant d'installation (page 15)
Installation du serveur à l'aide de l'assistant d'installation (page 16)
Mise à niveau du serveur (page 17)
Démarrage du serveur (page 18)
Activation de l'accessibilité dans le serveur CA EEM (page 19)
Suppression du serveur (page 20)
Installer SDK (page 20)
Démarrage du kit de développement logiciel (page 21)
Suppression du kit de développement logiciel (page 21)
Paramètres d'installation du serveur (page 21)
Installation du serveur CA EEM en mode silencieux (page 23)
Suppression du serveur CA EEM en mode silencieux (page 25)

Présentation de l'installation

L'installation de CA EEM sur les systèmes d'exploitation Windows consiste à installer les applications suivantes.

Serveur CA EEM

Le serveur CA EEM vous permet de définir des stratégies d'autorisation sur les ressources d'application à l'aide d'une interface Web. L'interface administrative Web permet de gérer des identités et des stratégies d'accès. L'infrastructure de sécurité permet de mettre en oeuvre des règles d'après la logique métier (à l'aide de ressources et d'attributs utilisateur) définies dans des magasins d'utilisateurs centralisés et d'autres systèmes d'entreprise.

Kit de développement logiciel (SDK) de CA EEM

Le SDK de CA EEM vous permet d'intégrer des contrôles de sécurité d'après l'identité au sein des applications. Le SDK comprend des bibliothèques, des classes java, des fichiers d'en-tête et un didacticiel. Il vous permet de mettre en oeuvre CA EEM dans n'importe quelle application. Pour plus d'informations sur la mise en oeuvre de CA EEM à l'aide du SDK, consultez le *Manuel de programmation*.

Chaque application s'installe séparément et fonctionne indépendamment de l'autre.

Installation du serveur

Vous pouvez installer le serveur CA EEM à l'aide de l'assistant d'installation ou de la ligne de commande. Utilisez la ligne de commande pour installer CA EEM en mode silencieux et lancez l'assistant d'installation pour une installation interactive.

L'environnement d'exécution Java (JRE) ne fait plus partie de la configuration minimale requise pour installer et utiliser CA EEM. Vous pouvez donc installer et utiliser CA EEM avec ou sans le JRE. Si vous souhaitez installer CA EEM sans le JRE, vous devez ignorer l'écran de sélection du chemin du JRE dans l'assistant d'installation. Si vous souhaitez installer le serveur CA EEM en mode silencieux sans le JRE, vous devez régler le paramètre javahome sur "None" (Aucun).

Les sections suivantes décrivent le mode d'installation du serveur CA EEM.

Informations complémentaires

Non-affichage de l'écran du chemin du JRE dans l'assistant d'installation (page 15)
Liste de contrôle de configuration de l'assistant (page 14)
Installation du serveur à l'aide de l'assistant d'installation (page 16)
Installation du serveur CA EEM en mode silencieux (page 23)

Liste de contrôle de configuration de l'assistant

Lorsque vous installez le serveur CA EEM sous Windows, vous devez disposer des informations suivantes.

Champ	Valeur
Chemin d'installation CA EEM	Emplacement de l'ordinateur où vous prévoyez d'installer CA EEM
Chemin d'installation du JRE	Emplacement de l'installation du JRE sur l'ordinateur **Remarque** : Si vous souhaitez installer et utiliser CA EEM sans le JRE, vous devez définir la variable Javahome sur None (Aucun) dans la ligne de commande avant d'exécuter l'assistant d'installation de CA EEM.
Mot de passe EiamAdmin	Mot de passe associé à l'administrateur de CA EEM, EiamAdmin
Répertoire de sauvegarde	Emplacement de l'ordinateur où vous prévoyez

Champ	Valeur
	de sauvegarder les fichiers provenant d'une installation antérieure de CA EEM **Remarque :** Cette information est requise uniquement si vous mettez à niveau une version antérieure de CA EEM vers la version actuelle.

Non-affichage de l'écran du chemin du JRE dans l'assistant d'installation

L'environnement d'exécution Java (JRE) ne fait plus partie de la configuration minimale requise pour installer et utiliser CA EEM. Si vous souhaitez installer CA EEM sans le JRE, vous devez procéder comme suit.

1. Définissez le paramètre javahome sur "None" (Aucun).

   Remarque : Si vous définissez le paramètre javahome sur "None" (Aucun), l'assistant d'installation n'affiche pas l'écran de sélection du chemin Java.

2. Installez CA EEM à l'aide de l'assistant d'installation.

Définition du paramètre Javahome

Vous devez définir le paramètre javahome sur la valeur "None" (aucun) avant d'utiliser l'assistant d'installation pour installer CA EEM. Définissez le paramètre javahome à partir de la ligne de commande, comme suit :

EEMServer_*[numéro_version]*_win32.exe -s -a /z"javahome=None; "

Installation du serveur à l'aide de l'assistant d'installation

L'assistant d'installation du serveur CA EEM vous guide tout au long du processus d'installation et fournit des options permettant de définir les paramètres d'installation.

Pour installer le serveur CA EEM

1. Effectuez l'une des opérations suivantes.
   - Ouvrez l'explorateur Windows et double-cliquez sur le package d'installation EEMServer_[*numéro_version*].[*numéro_compilation*]_win32.exe sur l'ordinateur cible.
   - A l'invite de commande, saisissez la commande suivante en utilisant les paramètres d'installation.

     EEMServer_*[numéro_version].[numéro_compilation]*_win32.exe -s -a /z "eiampath=<*chemin_installation_personnalisé_CA_EEM*>; etdirpath=<*chemin_installation_personnalisé_CA_Directory*>; igpath=<*chemin_installation_personnalisé_iGateway*>;"

     Vous pouvez fournir un chemin d'installation personnalisé à l'aide des paramètres d'installation. Pour plus d'informations sur les paramètres d'installation, consultez la section Paramètres d'installation du serveur.

     L'assistant d'installation apparaît.
2. Suivez les instructions de l'assistant d'installation pour effectuer l'installation.

Informations complémentaires :

Non-affichage de l'écran du chemin du JRE dans l'assistant d'installation (page 15)

Mise à niveau du serveur

Vous pouvez mettre à niveau l'installation du serveur CA EEM vers la version actuelle.

Pour mettre à niveau une installation du serveur CA EEM

1. Exécutez le fichier EEMServer_<numéro_version>_win32.exe sur l'ordinateur cible.
2. En fonction de la version du serveur CA EEM installée, l'une des situations suivantes se produit.
   - Si la version du serveur CA EEM est antérieure à la version en cours d'installation, l'assistant d'installation sauvegarde la version existante et effectue automatiquement une mise à niveau vers la version la plus récente.
   - Si la version du serveur CA EEM est identique à celle en cours d'installation, l'assistant d'installation vous invite à désinstaller le serveur CA EEM. Vous pouvez désinstaller et réinstaller le serveur CA EEM.
   - Si la version en cours d'installation est antérieure à la version existante, l'assistant d'installation affiche un message d'erreur et interrompt l'installation.

La mise à niveau du serveur CA EEM met à jour les éléments suivants.

- Serveur CA EEM dans le dossier \\CA\SharedComponents\iTechnology
- iGateway
- CA Directory

Tous les certificats P12 sont migrés vers des certificats PEM.

Informations complémentaires :

Liste de contrôle de configuration de l'assistant (page 14)
Installation du serveur à l'aide de l'assistant d'installation (page 16)

Démarrage du serveur

Pour gérer les identités et les stratégies d'accès des applications enregistrées, vous devez démarrer le serveur CA EEM.

Pour démarrer à l'aide du serveur CA EEM

1. Effectuez l'une des opérations suivantes.
   - Entrez l'URL https://*nom_hôte* ou *adresse_IP*:5250/spin/eiam dans votre navigateur. Si vous utilisez l'ordinateur du serveur CA EEM, choisissez le chemin http://*hôte_local*:/5250/spin/eiam.
   - Sélectionnez Démarrer, Programmes, CA, Embedded Entitlements Manager, UI EEM sous Windows.

     Une page de connexion s'affiche.
2. Entrez les informations suivantes dans la boîte de dialogue de connexion.
   a. Sélectionnez une instance d'application que vous avez enregistrée pour ce produit en utilisant la fenêtre déroulante Application. <Global> est le paramètre par défaut. Le nom d'utilisateur par défaut de l'administrateur est EiamAdmin.

      Remarque : Vous pouvez ajouter des utilisateurs globaux pour la connexion et définir leur nom d'utilisateur selon vos préférences.

   b. Entrez votre mot de passe. Il s'agit du mot de passe que vous avez spécifié pendant l'installation du serveur CA EEM pour EiamAdmin.

   c. Sélectionnez Mémoriser mes paramètres pour conserver les mêmes paramètres lors de la prochaine connexion au serveur CA EEM.
3. Cliquez sur Connexion.

   La page d'accueil de l'interface CA EEM s'affiche. Pour plus d'informations sur l'utilisation du serveur CA EEM, consultez l'*Aide en ligne*.

Activation de l'accessibilité dans le serveur CA EEM

Les fonctionnalités d'accessibilité dans le serveur CA EEM permettent aux utilisateurs d'utiliser leurs produits, quelle que soit la capacité, et la documentation de prise en charge permet d'accomplir des tâches cruciales pour l'entreprise. Lorsque vous activez l'accessibilité, les utilisateurs peuvent accomplir des tâches cruciales en utilisant uniquement le clavier ou à l'aide d'un lecteur d'écran.

Pour activer l'accessibilité :

1. Effectuez l'une des opérations suivantes :
   - Entrez l'URL https://*nom_hôte* ou *adresse_IP*:5250/spin/eiam dans votre navigateur. Si vous utilisez l'ordinateur du serveur CA EEM, choisissez le chemin http://*hôte_local*:/5250/spin/eiam.
   - Sélectionnez Démarrer, Programmes, CA, Embedded Entitlements Manager, UI EEM sous Windows.

     Une page de connexion s'affiche.
2. Entrez les informations suivantes dans la boîte de dialogue de connexion.
   a. Sélectionnez une instance d'application que vous avez enregistrée pour ce produit en utilisant la fenêtre déroulante Application. <Global> est le paramètre par défaut. Le nom d'utilisateur par défaut de l'administrateur est EiamAdmin.

      Remarque : Vous pouvez ajouter des utilisateurs globaux pour la connexion et définir leur nom d'utilisateur selon vos préférences.

   b. Entrez votre mot de passe. Il s'agit du mot de passe que vous avez spécifié pendant l'installation du serveur CA EEM pour EiamAdmin.

   c. Sélectionnez Mémoriser mes paramètres pour conserver les mêmes paramètres lors de la prochaine connexion au serveur CA EEM.
3. Cliquez sur Activer l'accessibilité.

   L'accessibilité est activée dans l'interface CA EEM.
4. Cliquez sur Connexion.

   La page d'accueil de l'interface CA EEM s'affiche.

Suppression du serveur

Vous pouvez désinstaller le serveur CA EEM via l'option Ajout/Suppression de programmes du Panneau de configuration.

Remarque : Vous ne pouvez pas supprimer le serveur CA EEM si des applications sont enregistrées dans CA EEM. Avant de désinstaller le serveur CA EEM, vous devez annuler l'enregistrement des applications. Consultez l'*Aide en ligne* pour plus d'informations sur l'annulation des enregistrements d'applications.

Installer SDK

L'assistant d'installation du kit de développement logiciel (SDK) de CA EEM vous guide tout au long du processus d'installation.

Pour installer le SDK de CA EEM

1. Ouvrez l'explorateur Windows et double-cliquez sur le package d'installation EEMSDK_<numéro_version>_win32.exe ou exécutez le fichier d'installation à partir de l'invite de commande.

   L'assistant d'installation apparaît.

2. Cliquez sur le bouton J'accepte pour accepter les Conditions générales.

   Remarque : Le bouton J'accepte devient actif uniquement si l'utilisateur lit ou fait défiler l'intégralité du texte des conditions générales.

   La boîte de dialogue Sélectionnez l'emplacement de destination apparaît: Par défaut, l'assistant d'installation installe le SDK de CA EEM à l'emplacement suivant : C:\Program Files\CA\Embedded IAM SDK

3. Cliquez sur Suivant.

   Or

   Cliquez sur Parcourir et sélectionnez le répertoire d'installation du SDK de CA EEM, puis cliquez sur Suivant.

   L'installation du SDK de CA EEM commence alors.

4. Cliquez sur Terminer.

   Le SDK de CA EEM est installé.

   Remarque : Une variable d'environnement %EIAM_SDK% est créée pendant l'installation pour indiquer le chemin d'installation. Utilisez cette variable dans le chemin d'accès de l'explorateur pour ouvrir le dossier d'installation.

Démarrage du kit de développement logiciel

Pour démarrer le SDK de CA EEM, cliquez sur Démarrer, Programmes, CA, Embedded Entitlements Manager, EEM SDK.

La fenêtre de documentation du SDK de CA EEM s'affiche.

Suppression du kit de développement logiciel

Vous pouvez désinstaller le SDK de CA EEM via l'option Ajout/Suppression de programmes du Panneau de configuration.

Paramètres d'installation du serveur

Lorsque vous installez CA EEM sous Windows, vous devez collecter des informations sur les paramètres de ligne de commande suivants.

-eiampath

Indique le chemin d'installation du serveur CA EEM. Le chemin d'accès par défaut est C:\Program Files\CA\SharedComponents\Embedded IAM.

-etdirpath [chemin]

Spécifie le chemin d'installation de CA Directory. Le chemin par défaut est C:\Program Files\CA\Directory.

-igpath [chemin]

Spécifie le chemin d'installation de iGateway. Le chemin par défaut est C:\Program Files\CA\SharedComponents\iTechnology.

backupdir

Spécifie l'emplacement de sauvegarde des données de l'installation.

-capkiinstalldir

Spécifie le chemin d'accès au dossier d'installation du module CAPKI. Le chemin par défaut est C:\Program Files\CA\SC\CAPKI.

-javahome [répertoire]

Définit la variable JAVA_HOME sur [répertoire] lorsque le programme d'installation d'iGateway est sollicité. Le programme d'installation CA EEM vous invite à définir la variable, même si elle a déjà été définie. Aucune valeur par défaut n'a été définie pour ce paramètre.

Remarque : Si vous souhaitez installer CA EEM sans java, vous devez définir javahome sur None (aucun).

CA EEM utilise les paramètres suivants au cours de l'installation de CA Directory. Vous pouvez configurer les paramètres en fonction de vos besoins.

Important : Avant de personnaliser les numéros de port par défaut, assurez-vous qu'aucun autre service n'est configuré sur les mêmes ports.

-dxadminport

Indique le port sur lequel DXadmind écoute les demandes réalisées par DXmanager. Ce port est utilisé pour la communication LDAP entre DXadmind et DXmanager. *DXadmind* est un processus en arrière-plan qui s'exécute sur chaque hôte qui contient un DSA. DXmanager utilise DXadmind pour communiquer avec les DSA.

Par défaut : 2123

-dsaport

Spécifie le port que le DSA utilise pour écouter les demandes qui lui sont destinées.

Valeur par défaut : 509

-ssldport

Spécifie le port que CA Directory utilise pour écouter le serveur SSLD. Le serveur SSLD est un processus en arrière-plan qui gère l'authentification, le chiffrement et le déchiffrement SSL et TLS pour CA Directory.

Valeur par défaut : 21847

-routerport

Spécifie le port que le DSA utilise pour se connecter au DSA du routeur. Le DSA d'un routeur ne comporte ni données locales ni magasin de données. Il sert uniquement à acheminer le trafic vers d'autres DSA.

Valeur par défaut : 1684

-dxdbsize

Spécifie la taille maximale du magasin de données de CA EEM.

Valeur par défaut : 500 Mo

-dxuser

Spécifie un utilisateur non DSA capable d'installer, d'administrer et de désinstaller CA Directory. Le paramètre dxuser peut représenter un utilisateur de système local ou de réseau.

Remarque : Si vous avez installé CA Directory à l'aide d'un utilisateur de système local défini en tant que dxuser, cet utilisateur risque d'être supprimé lors de la désinstallation. Ainsi, si vous installez CA Directory à l'aide d'un utilisateur de système local défini en tant que dxuser, veillez à ce que cet utilisateur ne serve pas à exécuter d'autres programmes.

Remarque : Sous Microsoft Windows Server 2003, la longueur de la chaîne que vous pouvez utiliser dans la ligne de commande est limitée à 8 191 caractères. Sous Microsoft Windows 2000, cette longueur est limitée à 2 047 caractères. Pour plus d'informations sur la longueur de la commande InstallShield, consultez les *Notes de parution*.

Installation du serveur CA EEM en mode silencieux

L'installation du serveur CA EEM en mode silencieux exige l'exécution des deux tâches suivantes.

1. Création du fichier de réponse
2. Exécution de la commande désignant le fichier de réponse

   Le fichier journal eiaminstall.log, créé pendant l'installation silencieuse, enregistre toutes les erreurs d'installation.

Remarque : Si vous installez le serveur CA EEM en mode silencieux, vous pouvez également le supprimer en mode silencieux.

Création du fichier de réponse

Vous pouvez enregistrer les entrées de votre installation dans un fichier de réponse, utilisé pour installer le serveur CA EEM en mode silencieux. Vous devez créer un fichier de réponse pour chaque compilation à installer.

Pour créer un fichier de réponse

1. Exécutez le package d'installation du serveur CA EEM sur l'ordinateur cible.
2. A l'invite de commande, saisissez la commande suivante pour créer un fichier de réponse dans le répertoire spécifié.

   EEMServer_[*numéro_version*].[*numéro_compilation*]_win32.exe -s -a /r /f1"*nom_chemin_fichier_réponse*"

   Exemple :

   EEMServer_8.4.0.55_win32.exe -s -a /r /f1"c:\resp.iss"
3. Spécifiez des valeurs pour les paramètres d'installation, qui sont stockées dans le fichier de réponse.

Exécution de la commande spécifiant le fichier de réponse

Les exemples suivants illustrent les options permettant d'effectuer une installation en mode silencieux.

- Pour installer le serveur CA EEM en mode silencieux, entrez la commande suivante à l'invite de commande.

  EEMServer_[*numéro_version*].[*numéro_compilation*]_win32.exe -s -a /s /f1"*nom_chemin_fichier_réponse*"

  Exemple :

  EEMServer_8.4.0.55_win32,exe -s -a /s /f1"c:\resp.iss"
- Pour créer un fichier journal d'installation pendant l'installation en mode silencieux, entrez la commande suivante à l'invite de commande.

  EEMServer_[*numéro_version*].[*numéro_compilation*]_win32.exe -s -a /s /v"/qn /L*v <chemin_où_créer_fichier_journal>" /f1"*nom_chemin_fichier_réponse*"

  Exemple :

  EEMServer_8.4.0.55_win32,exe -s -a /s /v"/qn /L*v c:\install.txt" /f1"c:\resp.iss"

Cette commande installe le serveur CA EEM en mode silencieux en utilisant le fichier de réponse spécifié.

Remarque : Vous pouvez fournir les paramètres d'installation avec le script d'installation. Pour plus d'informations sur les paramètres, consultez la section Paramètres d'installation du serveur.

Suppression du serveur CA EEM en mode silencieux

Vous devez utiliser un fichier de réponse créé à partir de la même compilation du serveur CA EEM pour désinstaller correctement le produit. Pour désinstaller le serveur CA EEM en mode silencieux, entrez la commande suivante à l'invite de commande.

EEMServer_[*numéro_version*].[*numéro_compilation*]_win32.exe -s -a /s /f1"*nom_chemin_fichier_réponse*" /z"uninstall"

Exemple :

EEMServer_8.4.0.55_win32,exe -s -a /s /f1"c:\resp.iss" /z"uninstall"

Cette commande désinstalle le serveur CA EEM en mode silencieux.

Remarque : Vous ne pouvez pas supprimer le serveur CA EEM si des applications sont enregistrées dans CA EEM. Avant de désinstaller le serveur CA EEM, vous devez annuler l'enregistrement des applications. Consultez l'*Aide en ligne* pour plus d'informations sur l'annulation des enregistrements d'applications.

Chapitre 3 : Installation sous Linux et UNIX

Ce chapitre traite des sujets suivants :

Présentation de l'installation (page 27)
Installation du serveur (page 28)
Mise à niveau du serveur (page 29)
Suppression du serveur (page 29)
Installation du kit de développement logiciel (page 30)
Démarrage du SDK de CA EEM (page 30)
Suppression du kit de développement logiciel (page 31)
Paramètres du script d'installation du serveur (page 32)
Installation du serveur en mode silencieux (page 34)
Suppression du serveur CA EEM en mode silencieux (page 34)

Présentation de l'installation

L'installation de CA EEM sur les systèmes d'exploitation Linux et UNIX consiste à installer les applications suivantes.

Serveur CA EEM

Le serveur CA EEM vous permet de définir des stratégies d'autorisation sur les ressources d'application à l'aide d'une interface Web. L'interface administrative Web permet de gérer des identités et des stratégies d'accès. L'infrastructure de sécurité permet de mettre en oeuvre des règles d'après la logique métier (à l'aide de ressources et d'attributs utilisateur) définies dans des magasins d'utilisateurs centralisés et d'autres systèmes d'entreprise.

Kit de développement logiciel (SDK) de CA EEM

Le SDK de CA EEM vous permet d'intégrer des contrôles de sécurité d'après l'identité au sein des applications. Le SDK comprend des bibliothèques, des classes java, des fichiers d'en-tête et un didacticiel. Il vous permet de mettre en oeuvre CA EEM dans n'importe quelle application. Pour plus d'informations sur la mise en oeuvre de CA EEM à l'aide du SDK, consultez le *Manuel de programmation*.

Chaque application s'installe séparément et fonctionne indépendamment de l'autre.

Installation du serveur

Le serveur CA EEM pour Linux et UNIX utilise un script de commandes shell auto-extractible qui vous guide tout au long du processus d'installation. Pendant l'installation, le script affiche les informations de licence et invite à fournir les paramètres d'installation. Une fois les paramètres d'installation spécifiés, l'installation commence.

Pour installer le serveur CA EEM pour Linux and UNIX

1. Exécutez le script d'installation EEMServer_[*numéro_version*].[*numéro_compilation*]_[*nom_système_exploitation*].sh sur l'ordinateur cible.

   Exemple :

   EEMServer_8.4.0.55_sunos.sh

   Le fichier est décompressé et l'installation commence.

2. Tapez O pour accepter les conditions générales du contrat de licence (ou N pour refuser et abandonner l'installation).

   Le script vous invite à fournir les paramètres d'installation.

3. Entrez les paramètres d'installation.

   Remarque : Pour plus d'informations sur les paramètres d'installation possibles, consultez la section Paramètres du script d'installation du serveur.

   Exemple :

   a. Entrez le chemin d'installation du serveur CA EEM (ou acceptez la valeur par défaut).

   Un écran de confirmation affiche les valeurs saisies pour les paramètres d'installation.

4. Si les informations sur l'écran de confirmation sont correctes, tapez O pour poursuivre l'installation. Pour quitter le programme d'installation, tapez N.

5. Entrez le mot de passe EiamAdmin.

   Remarque : Le nom d'utilisateur par défaut de l'administrateur est EiamAdmin.

   Le déroulement de la procédure d'installation est tributaire des paramètres de la ligne de commande et du type de package de serveur CA EEM installé.

   Le script d'installation termine l'installation du serveur CA EEM sur votre ordinateur.

Mise à niveau du serveur

Vous pouvez mettre à niveau l'installation du serveur CA EEM vers la version actuelle.

Pour mettre à niveau une installation du serveur CA EEM

1. Exécutez EEMServer_[*numéro_version*].[*numéro_compilation*]_[*nom_système_exploitation*] sur l'ordinateur cible.
2. En fonction de la version du serveur CA EEM installée, l'une des situations suivantes se produit.
   - Si la version du serveur CA EEM est antérieure à la version en cours d'installation, l'assistant d'installation effectue automatiquement une mise à niveau vers la version la plus récente.
   - Si la version du serveur CA EEM est identique à celle en cours d'installation, l'assistant d'installation vous invite à désinstaller le serveur CA EEM. Vous pouvez désinstaller et réinstaller le serveur CA EEM.
   - Si la version en cours d'installation est antérieure à la version existante, l'assistant d'installation affiche un message d'erreur et interrompt l'installation.

   Pour plus d'informations sur l'installation du serveur CA EEM, consultez la section Installation du serveur (page 28).

La mise à niveau du serveur CA EEM met à jour les éléments suivants.

- Serveur CA EEM dans le dossier \\CA\SharedComponents\iTechnology
- iGateway
- CA Directory

Suppression du serveur

Pour désinstaller le serveur CA EEM, exécutez le script eiamuninstall.sh à partir du répertoire d'installation.

Remarque : Vous ne pouvez pas supprimer le serveur CA EEM si des applications sont enregistrées dans CA EEM. Avant de désinstaller le serveur CA EEM, vous devez annuler l'enregistrement des applications. Consultez l'*Aide en ligne* pour plus d'informations sur l'annulation des enregistrements d'applications.

Installation du kit de développement logiciel

Le SDK de CA EEM pour Linux et UNIX utilise un script de commandes shell auto-extractible qui vous guide tout au long du processus d'installation. Pendant l'installation, le script affiche les informations de licence et invite à fournir les paramètres d'installation. Une fois les paramètres d'installation spécifiés, l'installation commence.

Pour installer le SDK de CA EEM pour Linux and UNIX

1. Exécutez le script d'installation EEMSDK_[*numéro_version*].[*numéro_compilation*]_[*nom_système_exploitation*].sh sur l'ordinateur cible.

   Exemple :

   EEM_8.4.0.55_sunos.sh

   Le fichier est décompressé et l'installation commence.

2. Tapez O pour accepter les conditions générales du contrat de licence (ou N pour refuser et abandonner l'installation).
3. Entrez le chemin d'installation du SDK de CA EEM (ou acceptez la valeur par défaut).
4. Sélectionnez le produit à installer.

   Le SDK de CA EEM est installé sur votre ordinateur.

Démarrage du SDK de CA EEM

Pour lancer le SDK de CA EEM, allez à l'emplacement /opt/CA/eIAMSDK/Doc/index.html avec votre navigateur Web (ou vers l'emplacement d'installation du SDK de CA EEM).

Suppression du kit de développement logiciel

Vous pouvez désinstaller le SDK de CA EEM des systèmes d'exploitation Linux et UNIX.

Pour supprimer le SDK de CA EEM

1. Exécutez le script d'installation EEMSDK_[*numéro_version*].[*numéro_compilation*]_[*nom_système_exploitation*].sh sur l'ordinateur cible.

   Exemple :

   EEM_8.4.0.55_sunos_linux.sh

   Le fichier est décompressé.

2. Sélectionnez le produit à désinstaller/supprimer.

   Le script d'installation supprime le SDK de CA EEM de l'ordinateur.

Paramètres du script d'installation du serveur

Pendant l'installation de CA EEM, vous devez collecter des informations sur les paramètres de ligne de commande sollicités par le script d'installation.

Le script accepte les paramètres de ligne de commande suivants.

backupdir

Spécifie l'emplacement de sauvegarde des données de l'installation.

-capkiinstalldir

Spécifie le chemin d'accès au dossier d'installation du module CAPKI.

Valeur par défaut : /opt/CA/SharedComponents/capki

CA EEM utilise les paramètres suivants au cours de l'installation de CA Directory. Vous pouvez configurer les paramètres en fonction de vos besoins.

Important : Avant de personnaliser les numéros de port par défaut, assurez-vous qu'aucun autre service n'est configuré sur les mêmes ports.

-dxadminport

Indique le port sur lequel DXadmind écoute les demandes réalisées par DXmanager. Ce port est utilisé pour la communication LDAP entre DXadmind et DXmanager. *DXadmind* est un processus en arrière-plan qui s'exécute sur chaque hôte qui contient un DSA. DXmanager utilise DXadmind pour communiquer avec les DSA.

Par défaut : 2123

-dsaport

Spécifie le port que le DSA utilise pour écouter les demandes qui lui sont destinées.

Valeur par défaut : 509

-ssldport

Spécifie le port que CA Directory utilise pour écouter le serveur SSLD. Le serveur SSLD est un processus en arrière-plan qui gère l'authentification, le chiffrement et le déchiffrement SSL et TLS pour CA Directory.

Valeur par défaut : 21847

-routerport

Spécifie le port que le DSA utilise pour se connecter au DSA du routeur. Le DSA d'un routeur ne comporte ni données locales ni magasin de données. Il sert uniquement à acheminer le trafic vers d'autres DSA.

Valeur par défaut : 1684

-dxdbsize

Spécifie la taille maximale du magasin de données de CA EEM.

Valeur par défaut : 500 Mo

-dxuser

Spécifie un utilisateur non DSA capable d'installer, d'administrer et de désinstaller CA Directory. Le paramètre dxuser peut représenter un utilisateur de système local ou de réseau.

Remarque : Si vous avez installé CA Directory à l'aide d'un utilisateur de système local défini en tant que dxuser, cet utilisateur risque d'être supprimé lors de la désinstallation. Ainsi, si vous installez CA Directory à l'aide d'un utilisateur de système local défini en tant que dxuser, veillez à ce que cet utilisateur ne serve pas à exécuter d'autres programmes.

-eiamadminpw [mot de passe]

Définit le mot de passe EiamAdmin sur [mot de passe].

-eiampath

Définit le chemin d'installation du serveur CA EEM. La valeur par défaut est /opt/CA/SharedComponents/EmbeddedIAM.

-etdirpath [chemin]

Définit le chemin d'installation de CA Directory.

-igpath [répertoire]

Définit le chemin d'iGateway. Le chemin choisi doit être complet, comme -iisystem. Le chemin par défaut est /opt/CA/SharedComponents/iTechnology.

-javahome [répertoire]

Définit le répertoire d'accueil JAVA_HOME. Ce paramètre adopte par défaut le contenu de la variable d'environnement JAVA_HOME et n'est demandé que si $JAVA_HOME n'est pas défini.

Remarque : Si vous souhaitez installer CA EEM sans Java, vous devez définir javahome sur "none" (aucun). Ce n'est pas applicable à HP-UX.

-logfile [nom de fichier]

Oblige le programme d'installation à consigner les informations du journal dans [nom de fichier], par défaut dans /tmp/eiam-install.log

-silent

Exécute l'installation en mode silencieux. Si un paramètre requis n'est pas spécifié sur la ligne de commande, l'installation échoue et imprime un message approprié. Ce paramètre n'apporte pas de changement au système si tous les paramètres nécessaires ne sont pas désignés.

-tempdir [répertoire]

Désigne le répertoire à utiliser pour le stockage du fichier temp. Le chemin par défaut est /tmp/eiam_temp. Ce chemin doit être complet et présent dans son propre sous-répertoire. Ce script utilise rm -rf pour supprimer le répertoire désigné pour l'exécution du script.

Installation du serveur en mode silencieux

Pour installer le serveur CA EEM en mode silencieux sur Linux ou UNIX, entrez la commande suivante à l'invite de commande.

EEMServer_[*numéro_version*].[*numéro_compilation*]_[*nom_système_exploitation*].sh -silent -eiamadminpw *mot_passe -répertoire javahome*

Exemple : La commande suivante pour les systèmes d'exploitation Sun inclut les paramètres minimum requis :

EEMServer_8.4.0.55_sunos.sh -silent -eiamadminpw *mot_passe -répertoire javahome*

Vous pouvez spécifier des paramètres d'installation supplémentaires. La plupart des paramètres d'installation ont des valeurs par défaut. Pour plus d'informations sur les paramètres du script, consultez la section Paramètres du script d'installation du serveur.

Le fichier est décompressé et l'installation commence.

Suppression du serveur CA EEM en mode silencieux

Pour supprimer le serveur CA EEM, exécutez eiamuninstall.sh -silent à partir du répertoire d'installation.

Remarque : Vous ne pouvez pas supprimer le serveur CA EEM si des applications sont enregistrées. Vous devez annuler l'enregistrement de toutes les applications avant de pouvoir désinstaller correctement le serveur CA EEM. Pour plus d'informations sur l'annulation de l'enregistrement d'une application, consultez l'*Aide en ligne*.

Chapitre 4 : Configuration du SDK CA EEM

Nouveaux fichiers binaires nécessaires à la création d'applications à l'aide du SDK CA EEM

Les nouveaux fichiers binaires suivants doivent être utilisés conjointement avec les fichiers DLL du SDK CA EEM provenant des anciennes versions afin d'intégrer le SDK r8.4 SR02 CA EEM dans vos applications :

Java

- xml-apis.jar

C++

Copiez les fichiers suivants à partir du dossier EIAMSDK/lib/$OS en fonction de votre système d'exploitation :

Windows

- log4cxx.dll
- log4cxx.lib
- libexpat-2.0.1.dll
- libexpat-2.0.1.dll

HP-UX

- *log4cxx* tel que liblog4cxx.sl, liblog4cxx.sl.10, liblog4cxx.sl.10.0
- libapr* tel que libapr-1.sl.3, libaprutil-1.sl.3, libapr-1.sl.3.3, libaprutil-1.sl.3.4
- libexpat-2.0.1.dll

UNIX HP-UX 11i

- *log4cxx* tel que liblog4cxx.so, liblog4cxx.so.10, liblog4cxx.so.10.0
- libexpat*

Création d'applications à l'aide des nouveaux fichiers binaires Java

1. Mettez à jour ClassPath avec les références au fichier xml-apis.jar.
2. Mettez à jour votre programme d'installation pour créer un package contenant les nouveaux fichiers binaires et le fichier de configuration de l'enregistreur.
3. Déployez les nouveaux fichiers binaires et le fichier de configuration de l'enregistreur, ainsi que les fichiers binaires du SDK CA EEM.

Fichiers requis pour exécuter les applications utilisant le SDK C++ de CA EEM

Les binaires suivants sont requis pour intégrer et exécuter les applications utilisant le SDK C++ de CA EEM :

Windows

- ipthread.dll
- libcurl_7_18_2.dll
- libexpat-2.0.1.dll
- log4cxx.dll
- msvcm80.dll
- msvcm90.dll
- msvcp71.dll
- msvcp80.dll
- msvcp90.dll
- msvcr70.dll
- msvcr71.dll
- msvcr80.dll
- msvcr90.dll
- pcre.dll
- pthread.dll
- pthreadVCE.dll
- xerces-c_2_8.dll
- zlib.dll
- Microsoft.VC80.CRT.manifest
- Microsoft.VC90.CRT.manifest

HP-UX

- liblog4cxx.sl, liblog4cxx.sl.10 et liblog4cxx.sl.10.0
- libapr-1.sl.3, libapr-1.sl.3.3 et libaprutil-1.sl.3.4
- libexpat-2.0.1.sl, libxerces-c.sl.28 , libcurl.sl.4, libpcre.sl.0, libexpat.sl.2 libz.sl et liblog4cxx.sl.10.0

Linux

- libxerces-c.so.28
- libcurl.so.4
- libexpat.so.2 pour linux_k24 et libexpat-2.0.1.so pour linux_26
- libpcre.so.0
- libz.so.1
- liblog4cxx.so.10.0.0

AIX

- libxerces-c28.a libcurl.4.so libexpat-2.0.1.a libpcre.a libz.so
- liblog4cxx.a

Sun Solaris

- libxerces-c.so.28
- libcurl.so.4 libpcre.so
- libexpat.so.2 libz.so
- liblog4cxx.so.10.0.0

Création d'applications à l'aide des nouveaux fichiers binaires C++

1. Ajoutez les nouvelles bibliothèques livrées avec le SDK CA EEM en ajoutant les lignes suivantes à votre fichier makefile :

   ```
   -llog4cxx -llibexpat
   ```

2. Mettez à jour votre programme d'installation pour créer un package contenant les nouveaux fichiers binaires, le fichier eiam.config et le fichier eiam.log4cxx.config.
3. Déployez les nouveaux fichiers binaires, le fichier eiam.config et le fichier eiam.log4cxx.config, ainsi que les fichiers binaires du SDK CA EEM.

Remarque : Vous devez inclure les fichiers d'en-tête de l'enregistreur à votre code source.

Fichiers requis pour la création et l'exécution des applications utilisant le SDK C# CA EEM

Les binaires suivants sont requis pour intégrer et exécuter les applications utilisant le SDK C# de CA EEM :

- log4net.dll
- CPoz.dll
- iclient.dll
- CsharpSDK.dll

Remarque : Les fichiers CAPICOM.dll et InterOP.CAPICOM.dll ne sont pas requis pour créer des applications utilisant le SDK C#. Supprimez-les du package.

Mise en package du SDK C# de CA EEM dans les applications

1. Ajoutez les DLL du dossier suivant comme assemblages référencés lors de la création de l'application :

   %EIAM_SDK%\lib\csharp

2. Mettez à jour votre programme d'installation pour mettre en package les nouveaux fichiers binaires, le fichier eiam.config et le fichier eiam.log4net.config.

   Remarque : Le fichier eiam.config et les fichiers eiam.lognet.config se trouvent dans le dossier %EIAM_SDK%\bin.

3. Déployez les DLL référencées, le fichier eiam.config et le fichier eiam.log4net.config sur les ordinateurs clients.

Configuration du SDK CA EEM

Les rubriques suivantes expliquent la configuration du SDK CA EEM à l'aide de la classe Safe::Configurator.

Informations complémentaires :

A propos du fichier eiam.config (page 40)
Journalisation du SDK CA EEM (page 91)
Configuration du SDK CA EEM C++ (page 47)
Configuration du SDK Java CA EEM à l'aide de SafeConfigurator (page 46)

A propos du fichier eiam.config

Vous devez utiliser le fichier eiam.config pour contrôler les données de configuration du CA EEM telles que :

- Le tampon cyclique
- Le fichier de configuration de l'enregistreur
- Le dossier SAF pour le stockage des fichiers d'audit
- Le mode compatible FIPS

Le fichier eiam.config se compose des paramètres configurables suivants :

CyclicBuffer size (Taille du tampon cyclique)

Spécifie le nombre de messages enregistrés contenus dans un tampon cyclique. Le tampon cyclique stocke le nombre spécifié de messages enregistrés dans la mémoire. Quand il atteint la taille spécifiée, un nouveau message enregistré remplace le plus ancien dans le tampon. Si l'application plante, vous pouvez récupérer les derniers messages enregistrés dans le noyau.

Valeur par défaut : 500

Minimum : 0

Maximum : 1 000

enable (activer)

Indique si le tampon cyclique a été activé. S'il est paramétré sur False, le tampon cyclique est alors désactivé. Nul besoin donc de spécifier les valeurs des paramètres CyclicBuffer size (Taille du CyclicBuffer), dump (vidage) et file (fichier).

Valeur : [*true*|*false*]

Valeur par défaut : true

Important : Le tampon cyclique a été activé par défaut que vous ayez ou non activé la journalisation. Si vous activez le tampon cyclique, les performances de CA EEM seront affectées.

dump (vidage)

Spécifie si le contenu du tampon cyclique a été écrit dans un fichier en cas de modification ou de mise à jour du fichier eiam.config.

Valeur : [*true*|*false*]

Valeur par défaut : false

file

Spécifie le nom de fichier du fichier de vidage. Si le vidage est paramétré sur False, les messages enregistrés ne seront pas écrits dans un fichier de vidage. L'extension de fichier est .log.

Fichier de configuration de l'enregistreur

Indique le chemin absolu des fichiers de configuration de l'enregistreur pour les SDK java et C++ CA EEM. Les informations de journalisation CA EEM sont stockées dans les fichiers de configuration de l'enregistreur. eiam.log4cxx.config et eiam.log4j.config sont les deux fichiers de configuration de l'enregistreur pour le SDK C++ CA EEM et le SDK Java CA EEM.

Répertoire Saf (system authorization facility : fonction d'autorisation d'accès)

Le dossier SAF où sont stockés les fichiers d'audit pour le traitement.

Network sockettimeout (délai d'expiration du connecteur logiciel du réseau)

Spécifie le délai d'expiration du connecteur logiciel en millisecondes.

Valeur par défaut : 120000 (2 secondes)

Informations complémentaires :

Journalisation du SDK CA EEM (page 91)

Exemple d'un fichier eiam.config

Vous trouverez ci-dessous un exemple du fichier eiam.config :

```
<EiamConfiguration>
 <!-- Interne à EIAM : Configuration du tampon cyclique -->
 <CyclicBuffer size="500" dump="false" file="dump.log" enable="true" />
 <!-- Chemin d'accès absolu au fichier de configuration de l'enregistreur. Pour Java, utilisez :-
file="eiam.log4j.config" -->
 <LoggerConfiguration file="eiam.log4cxx.config"/>
 <!--  Chemin d'accès absolu au dossier SAF dans lequel les fichiers d'audit seront stockés pour le traitement-->
 <Saf directory="audit"/>
  <!-- Délai d'expiration du connecteur logiciel en millisecondes. La valeur par défaut est de 2 minutes -->
 <Network sockettimeout="120000"/>
 <SDK type="Java">
        <iTechSDK>
                <FIPSMode>true</FIPSMode>
                <JCEProvider>JsafeJCE</JCEProvider>
                <Security>
                        <digestAlgorithm>SHA1</digestAlgorithm>
                </Security>
                <Debug>
                        <logLevel>trace</logLevel>
                </Debug>
        </iTechSDK>
 </SDK>
 <SDK type="C++">
        <iTechSDK>
                <FIPSMode></FIPSMode>
                <Commons>
                        <etpkiCryptoLib></etpkiCryptoLib>
                </Commons>
                <TransportConfig>
                        <!--les valeurs possibles sont SSLV23 / SSLV3 / TLSV1-->
                        <secureProtocol></secureProtocol>
                </TransportConfig>
                <Security>
                        <!--les valeurs possibles sont MD5/SHA1/SHA256/SHA384/SHA512-->
                        <digestAlgorithm></digestAlgorithm>
                </Security>
                <Debug>
                        <!--les valeurs possibles sont ERROR/WARNING/TRACE/NOLEVEL-->
                        <logLevel></logLevel>

                        <!--les valeurs possibles sont true/false -->
                        <logToFile></logToFile>

                        <!--nom du fichier journal-->
                        <logFile></logFile>
```

```
                    <!--taille du fichier journal en Mo (entier positif)-->
                    <maxLogSize></maxLogSize>
                </Debug>
            </iTechSDK>
        </SDK>
</EiamConfiguration>
```

Activation de la journalisation iTechnology de SDK

Vous pouvez activer la journalisation iTechnology du SDK uniquement pour le SDK C++ de CA EEM et le SDK Java de CA EEM. Pour le SDK C# de CA EEM, utilisez le fichier de configuration de l'enregistreur.

Pour activer la journalisation iTechnology du SDK, ouvrez le fichier eiam.config et éditez les balises suivantes :

- logLevel
- logToFile
- logFile
- maxLogSize

Pour le SDK Java de CA EEM, éditez les balises mentionnées précédemment dans la section de <SDK type ="Java">. Pour le SDK C++ de CA EEM, éditez les balises mentionnées dans la section <SDK type ="C++">.

Avant la configuration du SDK Java de CA EEM en mode FIPS uniquement

Pour configurer le SDK Java de CA EEM en mode FIPS uniquement, procédez comme suit :

1. Configurez l'environnement d'exécution Java (JRE) pour qu'il autorise l'utilisation des bibliothèques Java Cryptography Extension (JCE) tierces.
2. Ajoutez les bibliothèques Crypto-J comme fournisseur de JCE dans le fichier Java.security.

   Remarque : Pour plus d'informations sur la configuration du JRE avec JCE, consultez la documentation de JCE appropriée.
3. Activez le mode FIPS uniquement dans le fichier eiam.config.

Configuration du SDK Java de CA EEM en mode FIPS uniquement

Lorsque vous configurez le SDK de CA EEM en mode FIPS uniquement, CA EEM utilise les bibliothèques cryptographiques conformes à la norme FIPS 140-2 pour chiffrer et déchiffrer les données sensibles.

Pour configurer le SDK Java de CA EEM en mode FIPS uniquement :

1. Ouvrez le fichier eiam.config et éditez les balises suivantes dans la section <SDK type="Java"> :
   - FIPSMode
   - JCEProvider
   - digestAlgorithm
2. Enregistrez et fermez le fichier eiam.config.
3. Redémarrez votre application.

   Le SDK Java de CA EEM est configuré en mode FIPS uniquement.

Configuration du SDK C++ de CA EEM en mode FIPS uniquement

Lorsque vous configurez le SDK de CA EEM en mode FIPS uniquement, CA EEM utilise les bibliothèques cryptographiques conformes à la norme FIPS 140-2 pour chiffrer et déchiffrer les données sensibles.

Pour configurer le SDK C++ de CA EEM en mode FIPS uniquement :

1. Ouvrez le fichier eiam.config et éditez les balises suivantes dans la section <SDK type="C++"> :
   - FIPSMode
   - etpkiCryptoLib
   - secureProtocol
   - digestAlgorithm
2. Enregistrez et fermez le fichier eiam.config.
3. Redémarrez votre application.

   Le SDK C++ de CA EEM est configuré en mode FIPS uniquement.

Configuration du SDK C# de CA EEM en mode FIPS uniquement

Lorsque vous configurez le SDK C# de CA EEM en mode FIPS uniquement, CA EEM utilise les bibliothèques cryptographiques conformes à la norme FIPS 140-2 pour chiffrer et déchiffrer les données sensibles.

Remarque : Le SDK C# de CA EEM ne prend pas en charge les certificats P11.

Pour configurer le SDK C# de CA EEM en mode FIPS uniquement :

1. Ouvrez le fichier eiam.config et éditez les balises suivantes dans la section <SDK type="C#"> :
   - FIPSMode
   - digestAlgorithm
2. Enregistrez et fermez le fichier eiam.config.
3. Redémarrez votre application.

   Le SDK C# de CA EEM est configuré en mode FIPS uniquement.

Définition des informations SafeContext

La balise <SafeContext> du fichier eiam.config contient des informations requises pour générer un contexte sécurisé à l'aide de la classe SafeContextFactory. Toutes les balises SafeContext du fichier eiam.config sont identifiées au moyen d'une balise unique refID. Pour générer un contexte sécurisé, vous devez transférer cette balise refID dans SafeContextFactory. Les avantages de la spécification des informations SafeContext dans le fichier eiam.config sont les suivants :

Pour définir les informations SafeContext :

1. Ouvrez le fichier eiam.config et les balises suivantes dans la section <SafeContext> :
   - refID
   - Backend
   - Application
   - Locale
   - Authentication Type
2. Enregistrez et fermez le fichier eiam.config.

Configuration du SDK Java CA EEM à l'aide de SafeConfigurator

Vous devez configurer le SDK CA EEM à l'aide de la classe Safe::Configurator. Pour configurer le SDK CA EEM, effectuez la procédure suivante :

Remarque : Vous devez configurer eiam.config avant de configurer le SDK CA EEM.

1. Ajoutez l'interface API suivante à votre code pour initialiser le SDK CA EEM pendant le démarrage de l'application :

   ```
   SafeConfigurator.getInstance().init(nom du fichier);
   ```

   Où

   nom du fichier

   Indique le chemin d'accès absolu du fichier eiam.config que vous avez défini pour votre application.

   Remarque : Toutes les opérations du SDK CA EEM au-delà de cette ligne sont enregistrées en fonction des niveaux de traçage de la journalisation dans la configuration de l'enregistreur.

2. Ajoutez l'interface API suivante à votre code pendant l'arrêt de votre application :

   ```
   m_config.term();
   ```

   Remarque : Pour chaque appel d'initialisation que vous effectuez avec m_config.init(*nom du fichier*), vous devez l'arrêter par une interface API m_config.term() correspondante. Les méthodes init et term sont "thread-safe" et comptées en référence. La bibliothèque Safe est lancée pendant le premier appel init() et arrêtée quand le compte de référence arrive à zéro.

Informations complémentaires :

A propos du fichier eiam.config (page 40)
A propos des fichiers de configuration de l'enregistreur (page 92)

Configuration du SDK CA EEM C++

Vous devez configurer le SDK CA EEM à l'aide de la classe Safe::Configurator. Pour configurer le SDK CA EEM, effectuez la procédure suivante :

Remarque : Vous devez configurer eiam.config avant de configurer le SDK CA EEM.

1. Ajoutez l'interface API suivante à votre code pour initialiser le SDK CA EEM pendant le démarrage de l'application :

   Safe::Configurator::getInstance()->init(*Nom du fichier*);

   Où

   Nom du fichier

   Indique le chemin d'accès absolu du fichier eiam.config que vous avez défini pour votre application.

2. Ajoutez l'interface API suivante à votre code pendant l'arrêt de votre application :

   Safe::Configurator::getInstance()->term();

   Remarque : Pour chaque appel d'initialisation que vous effectuez avec Safe::Configurator::getInstance()->init(nom du fichier), vous devez arrêter l'appel avec une interface API Safe::Configurator::getInstance()->term() correspondante. Les méthodes init et term sont "thread-safe" et comptées en référence. La bibliothèque Safe est lancée pendant le premier appel init() et arrêtée quand le compte de référence arrive à zéro.

Informations complémentaires :

A propos du fichier eiam.config (page 40)
A propos des fichiers de configuration de l'enregistreur (page 92)

Initialisez le SDK C# de CA EEM

Configurez le SDK de CA EEMà l'aide de la classe SafeConfigurator. Pour configurer le SDK CA EEM, effectuez la procédure suivante :

Remarque : Vous devez configurer eiam.config avant de configurer le SDK de CA EEM. Si vous ne configurez pas le fichier eiam.config, le SDK de CA EEM est initialisé avec la configuration par défaut suivante :

- Mode non FIPS
- Affichage d'une erreur de journalisation et activation de la journalisation de la console
- Désactivation de l'emplacement du SAF

Pour initialiser le SDK de CA EEM, effectuez la procédure suivante :

1. Ajoutez l'interface API suivante à votre code pour initialiser le SDK CA EEM pendant le démarrage de l'application :

   SafeConfigurator.getInstance().Init(*nom_fichier*);

   Où

   nom_fichier

   Indique le chemin d'accès absolu du fichier eiam.config que vous avez défini pour votre application.

   Remarque : Si vous ne mentionnez pas le nom de fichier, le SDK de CA EEM s'initialise avec les valeurs par défaut.

2. Incluez l'interface API suivante à votre code pendant l'arrêt de votre application :

   SafeConfigurator.getInstance().term();

   Remarque : Pour plus d'informations sur la classe SafeConfigurator, reportez-vous au *Manuel de programmation*.

Chapitre 5 : Prise en charge de la norme FIPS 140-2

Ce chapitre traite des sujets suivants :

Présentation de la norme FIPS 140-2 (page 49)
Modes de sécurité pris en charge dans CA EEM (page 50)
Configuration du serveur CA EEM en mode FIPS uniquement (page 51)
Configuration de votre application en mode FIPS uniquement (page 56)

Présentation de la norme FIPS 140-2

La norme FIPS (Federal Information Processing Standards) 140-2 indique les conditions requises pour l'utilisation des algorithmes cryptographiques dans un système de sécurité protégeant les données sensibles et non classifiées. Le serveur CA EEM intègre la bibliothèque cryptographique Crypto-C ME v2.0 de RSA, qui a été validée comme conforme aux *Conditions de sécurité requises pour les modules cryptographiques* établies par la norme FIPS 140-2. Le numéro de certificat de validation de ce module est 608.

Le SDK Java de CA EEM utilise une version conforme à la norme FIPS de la bibliothèque cryptographique BSAFE Crypto-J 4.0 de RSA. Le SDK C++ de CA EEM intègre ETPKI 4.1.x, qui utilise les bibliothèques de cryptographie de RSA.

CA EEM peut fonctionner en mode non FIPS ou en mode FIPS uniquement. Les limites cryptographiques, c'est-à-dire la façon dont CA EEM applique le chiffrement, sont les mêmes dans les deux modes, mais les algorithmes sont différents.

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

En mode FIPS uniquement, CA EEM utilise les algorithmes suivants :

- SHA1 comme algorithme Digest par défaut pour chiffrer les mots de passe et signer les demandes de serveur. En mode FIPS uniquement, vous pouvez utiliser l'un des algorithmes suivants :
  - SHA1
  - SHA256
  - SHA384
  - SHA512
- TLS v1.0 pour la communication avec les annuaires LDAP externes si la connexion LDAP se fait sur TLS.

Modes de sécurité pris en charge dans CA EEM

CA EEM prend en charge deux modes de fonctionnement : le mode non FIPS et le mode FIPS uniquement. La fonctionnalité de CA EEM est la même dans ces deux modes. La différence entre ces deux modes réside dans les algorithmes cryptographiques utilisés pour le stockage et la vérification des mots de passe ainsi que dans la communication des données sensibles entre CA EEM et d'autres produits tels que les répertoires LDAP, CA SiteMinder, etc.

Non FIPS

Mode qui utilise des techniques non conformes à la norme FIPS pour la cryptographie. Dans ce mode, MD5 est l'algorithme par défaut utilisé pour chiffrer et déchiffrer les données sensibles. Les nouvelles installations ou les mises à niveau sont toujours exécutées en mode non FIPS. En mode non FIPS, le serveur CA EEM est rétrocompatible avec les clients CA EEM. Vous pouvez utiliser CA EEM r8.4 SDK pour vous connecter à un serveur CA EEM r8.4 SP3 par exemple.

FIPS uniquement

Mode qui utilise uniquement des techniques conformes à la norme FIPS pour la cryptographie. Ce mode n'est pas compatible avec les clients s'exécutant en mode non FIPS. Avec les serveurs CA EEM r8.4 SP3 s'exécutant en mode FIPS uniquement, vous pouvez utiliser uniquement des clients en mode FIPS uniquement du SDK de CA EEM r8.4 SP3.

Configuration du serveur CA EEM en mode FIPS uniquement

En mode FIPS uniquement, vous devez configurer le produit CA EEM pour qu'il utilise des algorithmes conformes à la norme FIPS. Le serveur CA EEM et les clients du SDK de CA EEM peuvent communiquer uniquement s'ils sont tous configurés en mode FIPS uniquement. De même, le serveur CA EEM en mode FIPS uniquement peut communiquer uniquement avec les répertoires LDAP configurés pour utiliser des algorithmes conformes à la norme FIPS. Pour configurer l'environnement CA EEM en mode FIPS uniquement, procédez comme suit :

- Vérifiez les conditions requises pour la configuration du serveur CA EEM en mode FIPS uniquement.
- Configurez le serveur CA EEM en mode FIPS uniquement.

Conditions requises pour la configuration du serveur CA EEM en mode FIPS uniquement.

Les conditions suivantes sont requises pour la configuration du serveur CA EEM en mode FIPS uniquement :

- Vérifiez que les autres produits CA utilisant iGateway (CA ITM, CA ELM, etc.) fonctionnent en mode FIPS uniquement. iGateway ne peut pas être initialisé en mode FIPS uniquement et en mode non FIPS simultanément. Lorsque iGateway est initialisé en mode FIPS-uniquement, tous les produits l'utilisant doivent également fonctionner en mode FIPS uniquement. Ouvrez le fichier iGateway.conf et vérifiez la valeur de la balise suivante :

  FIPSMode

  Si la valeur de cette balise est définie sur False, cela signifie que le produit utilisant iGateway fonctionne en mode non FIPS. Selon la configuration d'iGateway, décidez si vous souhaitez activer CA EEM en mode FIPS uniquement.

- Vérifiez les versions de pile utilisées par les autres produits CA, ouvre le fichier spin.conf et notez la valeur des étiquettes suivantes : <Spindle Name> et <version>. Dans la documentation du produit correspondant, vérifiez si ces versions sont compatibles avec la norme FIPS.

  Remarque : Le fichier iGateway.conf et les fichiers spin.conf sont stockés à l'emplacement suivant :

  - **Windows** : %IGW_LOC%
  - **Linux et UNIX** : /opt/CA/SharedComponents/iTechnology

Opérations préalables à la configuration de CA EEM en mode FIPS uniquement

Vérifiez que votre environnement remplit la configuration requise minimale avant de migrer l'environnement devant utiliser le mode FIPS uniquement. Imprimez les informations suivantes et utilisez-les comme liste de contrôle :

- ☐ Mettez à niveau votre serveur CA EEM vers CA EEM r8.4 SP3.
- ☐ Vérifiez que les produits qui sont intégrés ou qui sont reliés à CA EEM sont configurés pour utiliser le mode FIPS uniquement.

Configuration du serveur CA EEM en mode FIPS uniquement.

Lorsque vous configurez le serveur CA EEM en mode FIPS uniquement, CA EEM utilise les bibliothèques cryptographiques conformes à la norme FIPS 140-2 pour chiffrer et déchiffrer les données sensibles.

Remarques :

- En mode FIPS uniquement, utilisez IE7 (ou version ultérieure) ou Firefox 3.0 (ou version ultérieure) pour afficher l'interface d'administration de CA EEM. Pour plus d'informations sur la configuration de Firefox en mode FIPS 140-2, consultez le site de support de Firefox.
- La procédure suivante permet également de changer le mode de sécurité du serveur CA EEM et de le faire passer de FIPS à non FIPS ou de non FIPS à FIPS uniquement.

Pour configurer le serveur CA EEM en mode FIPS uniquement :

1. Arrêtez le service iGateway.
2. Arrêtez les services CA Directory à l'aide des commandes suivantes :

   Windows

   ```
   dxserver stop all
   ssld stop
   ```

   Linux et UNIX

   ```
   su - dsa -c "dxserver stop all"
   su - dsa -c "ssld stop"
   ```

3. Ouvrez le fichier iGateway.conf et définissez la balise suivante sur ON :

   ```
   <FIPSMode>ON<FIPSMode>
   ```

   Remarque : Pour basculer le mode de FIPS uniquement à non FIPS, définissez la balise FIPSMode sur OFF.

4. Dans l'invite de commande, exécutez les commandes suivantes :

   Windows

   ssld remove iTechPoz-Server
   ssld install iTechPoz-Server -certfiles "%DXHOME%/config/ssld/personalities" -ca "%DXHOME%/config/ssld/iTechPoz-trusted.pem" -port 21847 -fips

   Linux et UNIX

   su - dsa
   ssld remove iTechPoz-Server
   ssld install iTechPoz-Server -certfiles $DXHOME/config/ssld/personalities -ca $DXHOME/config/ssld/iTechPoz-trusted.pem -port 21847 -fips

   Remarque : L'option -port permet de spécifier le port ssld. Si vous avez configuré un port ssld différent, remplacez 21847 juste avant par le numéro de ce port. De la même façon, si vous faites passer le mode de sécurité de FIPS uniquement à non FIPS, utilisez les commandes dans cette étape sans l'option -fips.

5. Démarrez les services CA Directory à l'aide des commandes suivantes :

   Windows

   ssld start
   dxserver start all

   Linux et UNIX

   su - dsa -c "ssld start"
   su - dsa -c "dxserver start all"

6. Démarrer le service iGateway.

   CA EEM est configuré en mode FIPS uniquement.

Vérification du mode FIPS du serveur CA EEM

Pour vérifier que le serveur CA EEM est en mode FIPS uniquement, procédez comme suit :

1. Entrez l'URL https://*nom_hôte* ou *adresse_IP*:5250/spin/eiam/about.csp dans votre navigateur.

   La page A propos de s'affiche.

2. Vérifiez que l'étiquette FIPS: est définie sur Activé.

   Si tel est le cas, cela indique que le serveur CA EEM est en mode FIPS uniquement.

Communication entre le serveur CA EEM et les répertoires LDAP externes

La communication entre le serveur CA EEM et un répertoire externe dépend du type de connexion LDAP entre ces deux éléments : chiffrée ou non chiffrée. Les modes suivants de fonctionnement du serveur CA EEM et du répertoire externe sont pris en charge selon le chiffrement :

Activation du chiffrement au niveau du serveur CA EEM pour la communication LDAP

Lorsque le serveur CA EEM est configuré pour utiliser un canal chiffré de communication avec un répertoire LDAP externe, s'il fonctionne en mode FIPS, le répertoire LDAP doit également être configuré pour utiliser le mode compatible avec la norme FIPS.

Configuration de CA EEM pour l'utilisation des certificats de serveur dans un périphérique PKCS#11

Pour utiliser un périphérique PKCS#11 de nCipher avec le serveur CA EEM ou le SDK de CA EEM, configurez le périphérique et définissez la propriété suivante comme suit :

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=all
```

Remarque : Pour plus d'informations sur la configuration du périphérique nCipher avec un jeton matériel, reportez-vous à la documentation de nCipher.

Pour configurer le serveur CA EEM pour qu'il utilise des certificats stockés dans un périphérique PKCS#11, procédez comme suit :

1. Arrêtez le service iGateway.
2. Ouvrez le fichier iGateway.conf et définissez les valeurs suivantes pour les balises <Connector name="defaultport"> CA Portal5250</port> :

   certType

   Indique le type de certificat à utiliser. Les types de certificat pris en charge sont p12, pem et p11.

   Valeur par défaut : pem

   Type : Childnode

Utilisation du certificat P11

<pkcs11Lib/> : chemin d'accès à la bibliothèque PKCS11 fournie par le jeton

<token/> : ID de jeton

<userpin/> : code confidentiel crypté de l'utilisateur

<id/> : ID de certificat et de clé privée

<sensitive/> : indique que la clé privée est sensible. Les clés sensibles ne sont pas transformées étant donné que les clés logicielles et l'opération de cryptographie sont réalisées via le matériel cryptopki (les clés non sensibles peuvent être traitées comme des clés sensibles, mais les clés sensibles ne peuvent pas être transformées ou considérées comme des clés non sensibles)

Valeur par défaut : False

3. Enregistrez et fermez le fichier iGateway.conf.
4. Démarrez les services iGateway.

Configuration de CA EEM pour le stockage des certificats de serveur dans un périphérique PKCS#11

Pour stocker les certificats CA EEM dans un périphérique PKCS#11, procédez comme suit :

1. Arrêtez le service iGateway.
2. Ouvrez le fichier iGateway.conf et définissez les valeurs suivantes pour les balises <CertificateManager> :

   certType

   Indique le type de certificat à utiliser. Les types de certificat pris en charge sont p12, pem et p11.

   Valeur par défaut : pem

   Type : Childnode

Utilisation du certificat P11

<pkcs11Lib><pkcs11Lib/> : chemin d'accès à la bibliothèque PKCS11 fournie par le jeton

<token><token/> : ID de jeton

<userpin><userpin/> : code confidentiel crypté de l'utilisateur

<id><id/> : ID de certificat et de clé privée

<sensitive><sensitive/> : indique que la clé privée est sensible. Les clés sensibles ne sont pas transformées étant donné que les clés logicielles et l'opération de cryptographie sont réalisées via le matériel cryptopki (les clés non sensibles peuvent être traitées comme des clés sensibles, mais les clés sensibles ne peuvent pas être transformées ou considérées comme des clés non sensibles) : facultatif (défini par défaut sur false)

3. Enregistrez et fermez le fichier iGateway.conf.
4. Démarrez les services iGateway.

Configuration de votre application en mode FIPS uniquement

Pour configurer votre application en mode FIPS uniquement, vérifiez que le SDK de CA EEM fonctionne en mode FIPS uniquement et utilise uniquement des techniques conformes à la norme FIPS pour la cryptographie. Le fichier de configuration du SDK de CA EEM, eiam.config contrôle le mode sécurisé de fonctionnement du SDK de CA EEM. Avant de configurer le SDK de CA EEM en mode FIPS uniquement, vérifiez ce qui suit :

- Vérifiez que la version de votre SDK de CA EEM est r8.4 SP3.
- Convertissez les certificats P12 existants utilisés par CA EEM en certificats PEM.
- Initialisez le SDK CA EEM en mode FIPS uniquement.

Convertissez les certificats P12 utilisés par votre application en certificats PEM.

CA EEM prend en charge les certificats P12, PEM et PKCS#11, mais vous devez prendre en compte ce qui suit :

- La prise en charge de P12 est désactivée (non disponible) en mode FIPS uniquement. Pour compenser, la prise en charge des certificats PEM et PKCS#11 a été ajoutée dans ce mode.

Remarque : Le SDK C# de CA EEM prend en charge uniquement les certificats PEM en mode FIPS uniquement, les certificats P12 et PEM en mode non FIPS.

Si vous utilisez des certificats P12, vous devez donc migrer ces certificats à l'un des formats de certificat pris en charge par le mode FIPS uniquement. Pour transformer des certificats P12 en certificats PEM, servez-vous de igwCertUtil. L'utilitaire igwCertUtil permet de transformer, de créer ou de supprimer des certificats. Il se trouve dans le répertoire suivant :

Windows

%IGW_LOC%

UNIX et Linux

$IGW_LOC

Utilitaire igwcertutil : permet de créer, de copier, de convertir et de supprimer des certificats

Applicable sous Windows, UNIX et Linux

La commande create utilise le format suivant :

igwCertUtil -version *version* -create -cert *inputcert*-params -issuer issuercert -params [-debug] [-silent]

La commande convert utilise le format suivant :

igwCertUtil -version version -conv -cert *inputcert*-params -target newcert-params [-debug] [-silent]

La commande copy utilise le format suivant :

igwCertUtil -version version -copy -cert *inputcert*-params -target newcert-params [-debug] [-silent]

La commande delete utilise le format suivant :

igwCertUtil -version version -delete -cert *cert*-params [-debug] [-silent]

-version *version*

Indique la version d'igwCertUtil utilisée lors de la création, de la conversion, de la copie ou de la suppression des certificats. La version sert à garantir la rétrocompatibilité. Si igwCertUtil est modifié, l'ancien comportement est attribué à la balise de version.

-cert *inputcert*-parms

Indique le certificat sous forme de chaîne XML lors de la création, de la conversion ou de la copie des certificats.

-issuer *issuercert*-parms

Indique le certificat utilisé pour signer le certificat nouvellement généré lors de la création d'un certificat. Si aucun certificat n'est spécifié, un certificat autosigné est créé.

-target *newcert*-parms

Indique la configuration du nouveau certificat lors de la conversion (ou de la copie) d'un certificat existant.

-cert *cert*-parms

-debug

(Facultatif) Active le débogage pour igwCertUtil.

-silent

(Facultatif) Active le mode silencieux pour igwCertUtil.

Les codes d'erreur suivants sont renvoyés par igwCertUtil :

- CERTUTIL_ERROR_UNKNOWN (-1) : une erreur inconnue ou indéfinie s'est produite.
- CERTUTIL_SUCCESS (0) : opération réussie
- CERTUTIL_ERROR_USAGE (1) : transfert d'arguments de ligne de commande incorrects
- CERTUTIL_ERROR_READCERT (2) : impossibilité de lire le certificat
- CERTUTIL_ERROR_WRITECERT (3) : impossibilité d'écrire dans le certificat
- CERTUTIL_ERROR_DELETECERT (4): impossibilité de supprimer le certificat

Exemple : conversion de certificats P12 en certificats PEM

L'exemple suivant décrit la procédure de conversion d'un certificat e P12 en certificat PEM :

```
igwCertUtil -version 4,6.0,0 -conv  -cert
"<Certificate><certType>p12</certType><certURI>testCert.p12</certURI><certPW>password</certPW></Certificate>" -target "<Certificate><certType>pem</certType>
<certURI>testCert.cer</certURI><keyURI>testCert.key</keyURI></Certificate>"
```

Exemple : conversion de certificats P12 en certificats PKCS#11

```
igwCertUtil -version 4,6.0,0 -conv  -cert
"<Certificate><certType>p12</certType><certURI>testCert.p12</certURI><certPW>password</certPW></Certificate>" -target "<Certificate><certType>p11</certTyp
><pkcs11Lib>pathto-pkcs11Lib</pkcs11Lib><token>pkcs11token</token><userpin>user
in</userpin><id>certid</id></Certificate>"
```

Initialisez le SDK de CA EEM en mode FIPS uniquement.

Le SDK de CA EEM peut être initialisé en mode FIPS uniquement par le biais de la configuration du fichier eiam.config. Pour configurer le fichier eiam.config, consultez le chapitre Configuration du SDK de CA EEM (page 35).

Chapitre 6 : Sauvegarde et restauration du serveur CA EEM

Ce chapitre traite des sujets suivants :

Sauvegarde du système de fichiers (page 61)
Sauvegarde des fichiers et dossiers du serveur CA EEM (page 62)
Procédures de restauration (page 63)
Démarrage du service iGateway. (page 63)
Arrêt du service iGateway (page 63)

Sauvegarde du système de fichiers

Nous vous recommandons de sauvegarder les serveurs CA EEM régulièrement ou à chaque modification apportée aux environnements des serveurs CA EEM. Vous pouvez vous servir des sauvegardes du serveur CA EEM pour restaurer ce dernier en cas de dommage.

Vous devez sauvegarder les fichiers et dossiers CA EEM suivants.

Description des données	Noms de fichiers sous Windows	Noms de fichiers sous Linux
Fichiers de configuration	■ iPoz.conf ■ Eiam.conf ■ iPoz.map ■ Spin.conf ■ iPozDsa.pem ■ iPozRouterDsa.pem ■ logDepot.conf ■ calmReporter.conf	■ iPoz.conf ■ Eiam.conf ■ iPoz.map ■ Spin.conf ■ iPozDsa.pem ■ iPozRouterDsa.pem ■ eiam-type ■ Sponsorfiles ■ logDepot.conf ■ calmReporter.conf

Description des données	Noms de fichiers sous Windows	Noms de fichiers sous Linux
Informations sur les événements	■ logdepotdb ■ Dossier calm_catalog ■ Dossier calm_archive	■ logdepotdb ■ Dossier calm_catalog ■ Dossier calm_archive
Dossiers	■ Registre système ■ Dossier iTechnology	■ Dossier iTechnology ■ Paramètres d'environnement

Sauvegarde des fichiers et dossiers du serveur CA EEM

Nous vous recommandons de sauvegarder les serveurs CA EEM régulièrement ou à chaque modification apportée aux environnements des serveurs CA EEM. Vous pouvez vous servir des sauvegardes du serveur CA EEM pour restaurer ce dernier en cas de dommage.

Pour sauvegarder les fichiers et dossiers du serveur CA EEM

1. Arrêtez iGateway.
2. Sauvegardez les fichiers de configuration, les informations sur les événements et les dossiers de CA EEM.
3. Sauvegardez les données CA EEM stockées dans CA Directory.

   Les fichiers de configuration, les événements et les dossiers du serveur CA EEM sont sauvegardés.

Informations complémentaires :

Sauvegarde du système de fichiers (page 61)
Sauvegarde des données CA EEM stockées dans CA Directory (page 65)

Procédures de restauration

Vous devez restaurer vos données CA EEM dans les buts suivants.

- Récupérer une installation CA EEM endommagée
- Récupérer un environnement de serveur CA EEM qui ne fonctionne pas comme souhaité

Pour récupérer les fichiers de configuration et les données CA EEM

1. Arrêtez iGateway.
2. Renommez tous les fichiers .conf de CA EEM sauvegardés en .conf.merge et copiez les fichiers de configuration renommés dans le dossier iTechnology. Les fichiers .conf.merge servent à fusionner les fichiers de configuration sauvegardés avec les nouveaux.
3. Restaurez les données CA EEM.
4. Démarrez iGateway.

Informations complémentaires :

Sauvegarde des données CA EEM stockées dans CA Directory (page 65)

Démarrage du service iGateway.

Pour démarrer le service iGateway, vous devez saisir les commandes suivantes.

Windows

net start igateway

Linux et UNIX

$IGW_LOC/S99igateway start

Arrêt du service iGateway

Pour arrêter le service iGateway, vous devez saisir les commandes suivantes.

Windows

net stop igateway

Linux et UNIX

$IGW_LOC/S99igateway stop

Chapitre 7 : Sauvegarde des données CA EEM stockées dans CA Directory

Ce chapitre traite des sujets suivants :

Introduction à la terminologie CA Directory (page 65)
Utilisation de DXtools (page 66)
Sauvegarde des données CA Directory (page 68)
Restauration des données CA Directory (page 73)

Introduction à la terminologie CA Directory

Cette section précise la terminologie CA Directory utilisé dans le présent document.

DSA

Un *DSA* est un processus qui gère tout ou une partie d'un espace de noms de répertoire.

This also needs to be expanded to make it accessible to readers new to CA Directory. Lorsque vous installez le serveur CA EEM, vous pouvez configurer les paramètres CA Directory suivants.

DXmanager

DXmanager est une application Web qui vous permet de créer, configurer, surveiller et contrôler votre structure de répertoires.

Console DSA

La *console DSA* vous permet de vous connecter à un DSA afin de fournir des commandes DXserver, recevoir des informations de suivi et agir en tant qu'agent utilisateur.

DXtools

DXtools représente un ensemble d'utilitaires de ligne de commande fourni avec CA Directory. Ces outils vous permettent de gérer l'administration des répertoires, d'exploiter les données LDIF, de charger et décharger des données vers et depuis un répertoire et d'extraire et convertir des schémas à utiliser avec CA Directory.

LDIF (LDAP Data Interchange Format)

Les *fichiers LDIF* sont des fichiers texte qui contiennent des informations sur les répertoires au format LDIF. Vous pouvez utiliser les fichiers LDIF pour transférer les informations sur les répertoires entre des serveurs de répertoire LDAP ou pour décrire un ensemble de modifications à appliquer à un répertoire.

Utilisation de DXtools

Vous pouvez exécuter DXtools comme suit.

- Exécutez les commandes DXtools sur l'hôte, à l'aide de la console DSA.
- Exécutez les commandes DXtools sur un hôte distant, à l'aide de la console DSA, sur un réseau TCP/IP.
- Ajoutez les commandes DXtools à vos scripts.

Tous les outils renvoient zéro si l'opération réussit ou une valeur non nulle en cas d'erreur.

Variable d'environnement DXHOME

Pour certains outils, il est nécessaire de définir la variable d'environnement DXHOME sur le chemin de base de DXserver. Cette opération s'effectue automatiquement à l'installation de CA Directory.

Certains outils recherchent les fichiers de configuration DSA dans le dossier *config* sous le chemin de DXHOME.

Codes de sortie de DXtools

Les outils DXtools partagent des codes de sortie communs, bien que tous les codes de sortie ne s'appliquent pas à tous les outils. Les codes de sortie sont les suivants.

0

Opération réussie

1

Le DSA correspondant est en cours d'exécution.

2

Un ou plusieurs des fichiers du magasin de données existent déjà.

3

L'emplacement spécifié pour le répertoire n'existe pas ou ne désigne pas un répertoire.

4

Le type de fichier spécifié est incorrect ; il s'agit par exemple d'un répertoire.

5

Ce fichier présente un problème d'autorisation.

6

Le nom de chemin complet du fichier du magasin de données est trop long, peut-être parce que l'emplacement spécifié pour le répertoire du magasin de données est trop long.

7

Une erreur est survenue lors de la tentative de suppression des anciens fichiers du magasin de données.

8

Une erreur est survenue lors de la tentative de modification du nom des anciens fichiers du magasin de données.

9

Une erreur est survenue lors de la tentative de création ou de remplissage de l'un des fichiers.

10

La taille du magasin de données est inférieure ou égale à zéro.

11

Espace insuffisant sur le périphérique ou mémoire indisponible lors de la tentative de création du fichier

12

Accès insuffisant (peut-être en raison d'autorisations insuffisantes) pour créer le fichier ou définir l'accès au fichier

13

La variable d'environnement DXHOME n'est pas définie.

14

La variable d'environnement DXHOME n'est pas valide.

15

Le DSA correspondant existe déjà.

16

Impossible de démarrer le DSA créé. Pour plus de détails, consultez les fichiers journaux associés.

17

Paramètres de ligne de commande fournis incorrects ou inconnus

18

Le DSA correspondant n'existe pas.

Sauvegarde des données CA Directory

Pour sauvegarder les données CA Directory, procédez comme suit.

1. Connectez-vous à un DSA local.
2. Prenez un instantané du magasin de données du DSA par défaut en cours d'exécution. Cette opération s'appelle un vidage en ligne. Utilisez la commande suivante pour prendre l'instantané.

   dump *dxgrid-db*

   Remarque : Remplacez dxgrid-db par le nom DSA iTechPoz-Servern pour sauvegarder CA EEM.
3. Utilisez l'outil DXdumpdb pour sauvegarder le vidage en ligne (fichiers .zdb), c'est-à-dire la copie instantanée du magasin de données, dans un fichier LDIF.

Informations complémentaires :

Connexion à une console DSA locale (page 68)
Vidage en ligne du magasin de données (page 69)
Commande dump dxgrid-db : copie instantanée cohérente d'un magasin de données (page 70)

Connexion à une console DSA locale

Vous pouvez vous connecter à un DSA en local sous UNIX ou Windows si un port de console a été défini pour celui-ci.

Pour se connecter à une console DSA locale

1. Ouvrez une fenêtre d'invite de commande sur l'hôte exécutant le DSA.
2. Entrez la commande suivante.

   telnet localhost *numéro_port_local*

   numéro_port_local

   Indique le numéro de port de la console DSA auquel vous souhaitez vous connecter.

Vidage en ligne du magasin de données

Vous pouvez prendre une copie instantanée cohérente du magasin de données d'un DSA en cours d'exécution (vidage en ligne). Le DSA effectue les mises à jour avant de réaliser le vidage en ligne et ne lance pas de nouvelle mise à jour tant que la copie n'est pas terminée.

Le fichier du magasin de données est copié dans un fichier ayant l'extension .z, le fichier de la base de données est *dxgrid-db*.zdb.

Remarque : Chaque vidage écrase le fichier de sauvegarde précédent. Si vous souhaitez conserver le fichier de sauvegarde, copiez-le vers un autre emplacement avant le vidage suivant.

Commande dump dxgrid-db : copie instantanée cohérente d'un magasin de données

La commande *dump dxgrid-db* fait une copie instantanée cohérente du magasin de données d'un DSA en cours d'exécution (vidage en ligne). Le DSA effectue les mises à jour avant d'exécuter cette commande et ne lance pas de nouvelle mise à jour tant que la copie n'est pas terminée.

Le fichier du magasin de données est copié dans un fichier ayant l'extension .z, le fichier de la base de données est *dxgrid-db*.zdb.

Remarque : Chaque vidage écrase le fichier de sauvegarde précédent. Si vous souhaitez conserver le fichier de sauvegarde, copiez-le vers un autre emplacement avant le vidage suivant.

L'outil DXdumpdb peut exporter des données à partir d'un magasin de données créé à l'aide de la commande dump.

La commande présente le format suivant

dump *dxgrid-db* [période *début période*];

période *début période*

Indique que le vidage en ligne s'effectue à intervalles réguliers (facultatif).

début

Définit le nombre de secondes à compter du dimanche 00:00:00 GMT.

Remarque : L'heure de début est définie à l'aide de l'heure GMT et non de l'heure locale.

période

Définit le nombre de secondes entre les vidages en ligne.

Exemple : Exécution d'un vidage en ligne toutes les heures

La commande suivante prend un instantané du magasin de données toutes les heures.

dump *dxgrid-db* 0 3600

Remarque : Veillez à créer un job cron sous UNIX ou une tâche planifiée sous Windows pour copier le fichier sauvegardé dans un endroit sûr. Chaque vidage écrase les fichiers de sauvegarde précédents.

Utilisation d'un fichier LDIF pour sauvegarder et charger des données

Les *fichiers LDIF* sont des fichiers texte qui contiennent des informations sur les répertoires au format LDIF. Vous pouvez utiliser les fichiers LDIF pour transférer les informations sur les répertoires entre des serveurs de répertoire LDAP ou pour décrire un ensemble de modifications à appliquer à un répertoire.

CA Directory est fourni avec l'outil DXdumpdb, qui vous permet de décharger les données d'un magasin de données dans un fichier LDIF. Vous pouvez ensuite charger les données du fichier LDIF dans un magasin de données afin de récupérer le contenu des répertoires.

Sauvegarde d'un répertoire dans un fichier LDIF

Pour sauvegarder un répertoire dans un fichier LDIF

1. Connectez-vous en tant qu'utilisateur *dsa* (sous UNIX) ou en tant qu'administrateur DXserver (sous Windows).
2. Utilisez la commande suivante pour sauvegarder le magasin de données dans le fichier LDIF :

   dxdumpdb -f *nom_fichier* -z *nom_DSA*

   -f *nom_fichier*

   Indique le chemin et le nom du fichier dans lequel les données sont vidées.

   -z

   Indique que DXdumpdb effectue le vidage à partir de la copie du magasin de données qui est produite par la commande dump dxgrid-db de la console.

   nom_DSA

   Indique le nom du DSA.

Outil DXdumpdb : exportation des données d'un magasin de données vers un fichier LDIF

Utilisez l'outil DXdumpdb pour exporter les données d'un magasin de données vers un fichier LDIF.

Remarque : Pour obtenir la liste des codes d'état renvoyés par toutes les commandes DXtools, y compris celle-ci, consultez la section Codes de sortie de DXtools (page 66).

Cette commande suit la syntaxe suivante.

dxdumpdb *options DSA*

options

Désigne au moins une des options suivantes.

-f *nom_fichier*

Indique le fichier qui doit accueillir les données exportées. Si cette option n'est pas spécifiée, la sortie apparaît au format standard ou à l'écran.

-v

S'exécute en mode documenté. Cette option active le suivi des erreurs et de l'état. Pour que l'option -v fonctionne, vous devez également spécifier l'option -f.

-z

Indique que DXdumpdb effectue le vidage à partir de la copie du magasin de données qui est produite par la commande *dump dxgrid-db* de la console.

DSA

Définit le DSA. DXdumpdb recherche le magasin de données à exporter vers un fichier LDIF dans les fichiers de configuration de ce DSA.

Exemple : Extraction des données Democorp à l'écran

L'exemple suivant imprime les données LDIF du magasin de données du DSA *democorp* à l'écran.

```
dxdumpdb democorp
```

Exemple : Sauvegarde d'un vidage en ligne du magasin de données

L'exemple suivant exporte un vidage en ligne du magasin de données vers un fichier LDIF.

```
dxdumpdb -f eembackup -z iTechPoz-Servern
```

Restauration des données CA Directory

Pour restaurer CA Directory, procédez comme suit.

1. Arrêtez le DSA.
2. Utilisez l'outil DXloaddb pour charger un magasin de données à partir d'un fichier LDIF.

Outil DXloaddb : chargement d'un magasin de données à partir d'un fichier LDIF

Utilisez l'outil DXloaddb pour charger un magasin de données à partir d'un fichier LDIF. Le magasin de données doit déjà exister. Toutes les informations précédentes du magasin de données sont supprimées.

Remarques sur l'utilisation :

- Il n'est pas nécessaire de trier le fichier LDIF.
- DXloaddb hache un mot de passe saisi en texte clair dans le fichier LDIF.

  Si un algorithme de hachage est spécifié dans la configuration DSA, DXloadbdb l'utilise. Sinon, il utilise SHA-1.
- Par défaut, DXloaddb utilise la configuration DSA pour gérer les attributs opérationnels.
  - Si *op-attrs* = *true*, les attributs opérationnels du fichier LDIF sont chargés dans le magasin de données.

    Toute entrée du fichier LDIF qui ne comporte pas un attribut createTimestamp en obtient un dans le magasin de données.
  - Si *op-attrs* = *false*, les attributs opérationnels du fichier LDIF sont ignorés et des attributs non opérationnels sont créés par DXloaddb.

Cette commande suit la syntaxe suivante.

dxloaddb [*options*] *dsa fichier_ldif*

options

Désigne au moins une des options suivantes.

-n

Indique que DXloaddb n'exécute aucune action.

-O

Indique que DXloaddb comprend des attributs opérationnels standard, tels que les attributs de stratégie de mots de passe (par exemple, le nombre de tentatives de connexion) et les attributs d'horodatage. Si cette option est spécifiée, DXloaddb crée des attributs opérationnels qui ne sont pas définis dans le fichier LDIF.

-s

Indique que DXloaddb produit les statistiques suivantes concernant le magasin de données.

- Taille totale des données en Mo
- Nombre total d'entrées
- Nombre d'entrées ignorées
- Niveau de remplissage du fichier du magasin de données en Ko
- Nombre moyen d'entrées par Mo

-v

Indique la sortie documentée.

fichier_ldif

Nom du fichier LDIF à charger dans le magasin de données

DSA

Définit le DSA dont vous souhaitez charger le magasin de données.

Exemple : Création et chargement d'un magasin de données

Un magasin de données doit être créé et chargé selon la séquence suivante.

dxnewdb
dxloaddb

Exemple : Chargement de données LDIF dans un magasin de données

L'exemple suivant charge les données du fichier democorp.ldif dans le magasin de données democorp.

```
dxloaddb democorp democorp.ldif
```

Le texte suivant est un extrait possible du fichier democorp.ldif.

```
dn: o=Democorp, c=US
oc: organization
dn: ou=Administration, o=Democorp, c=US
oc: organizationalUnit
dn: cn=Fred Jones, ou=Administration, o=Democorp, c=US
oc: organizationalPerson
postalAddress: 11 Main Street $ Newtown
surname: Jones
title: Manager
telephonenumber: +1 (123) 456 7890
telephonenumber: +1 (987) 654 3210
dn: ou=Sales, o=democorp, c=US
oc: organizationalUnit
```

L'attribut telephonenumber apparaît deux fois car il prend plusieurs valeurs

Chapitre 8 : Configuration du basculement

Ce chapitre traite des sujets suivants :

Basculement (page 77)
Basculement du magasin de données d'application (page 78)
Basculement du serveur CA EEM (page 83)
Configuration des fichiers CA EEM (page 84)
Fédération d'artefacts (page 87)

Basculement

Le basculement correspond à la capacité à assurer un flot de données et un fonctionnement ininterrompus lorsque les données deviennent indisponibles.

Pour que le basculement CA EEM fonctionne, vous devez joindre une application au produit CA EEM installé sur un serveur afin d'obtenir des informations sur d'autres serveurs. Les informations relatives à la configuration des autres serveurs sont disponibles dans le fichier iPoz.conf utilisé pour le basculement.

Vous pouvez configurer CA EEM pour prendre en charge deux types de scénarios de basculement.

- Basculement de magasin de données
- Basculement de serveur (page 83)

Remarque : Dans ce scénario, nous supposons que les noms d'hôte sont Server1 et Server2... et ServerN.

Basculement du magasin de données d'application

Le serveur CA EEM utilise CA Directory en tant que magasin de données d'application. Ce magasin de données d'application prend en charge le basculement et la récupération. Synchronisez les éléments suivants au niveau de tous les serveurs inclus dans la configuration de basculement :

1. Heure système
2. Mode de sécurité (non FIPS ou FIPS uniquement)
3. Magasin de données d'application
4. Assurez que la recherche DNS est correcte.

Important : Sauvegardez les magasins de données d'application avant de les synchroniser. Pour plus d'informations sur la sauvegarde le magasin de données, consultez la section Sauvegarde des données CA EEM stockées dans CA Directory (page 65).

Configuration du basculement du magasin de données d'application

Remarque : Réalisez les étapes de la procédure suivante sur le serveur principal. Toute les étapes concernant les serveurs secondaires sont explicitement mentionnées.

Pour effectuer cette procédure, vous devez avoir installé le serveur CA EEM avec les valeurs par défaut suivantes :

- dsa user : dsa
- data dsa port : 509
- group membership : etrdir

Si vous avez personnalisé l'un de ces paramètres, remplacez les valeurs par défaut par les valeurs personnalisées.

Pour configurer le basculement du magasin de données d'application :

1. A l'aide des commandes suivantes, arrêtez les services CA EEM sur tous les serveurs inclus dans la configuration de basculement :

   Windows

   net stop igateway
   dxserver stop all
   ssld stop

   Linux et UNIX

   $IGW_LOC/S99igateway stop
   su - dsa -c "dxserver stop all"
   su - dsa -c "ssld stop"

2. Copiez les fichiers suivants de chaque serveur CA EEM secondaire au serveur principal (Serveur1 par exemple), dans les dossiers respectifs :

   Windows

   %DXHOME%\config\knowledge\iTechPoz-*HostnameOfServerN*.dxc
   %DXHOME%\config\knowledge\iTechPoz-*HostnameOfServerN-Router*.dxc
   %DXHOME%\config\ssld\personalities\iTechPoz-*HostnameOfServerN*.pem
   %DXHOME%\config\ssld\personalities\iTechPoz-*HostnameOfServerN*-Router.pem

   Linux et UNIX

   $DXHOME/config/knowledge/iTechPoz-*HostnameOfServerN*.dxc
   $DXHOME/config/knowledge/iTechPoz-*HostnameOfServerN-Router*.dxc
   $DXHOME/config/ssld/personalities/iTechPoz-*HostnameOfServerN*.pem
   $DXHOME/config/ssld/personalities/iTechPoz-*HostnameOfServerN*-Router.pem

3. Copiez le fichier suivant des serveurs secondaires à un dossier temporaire sur le serveur principal Serveur1 :

   UNIX et Linux

   $DXHOME/config/ssld/iTechPoz-trusted.pem

   Windows

   %DXHOME%\config\ssld\iTechPoz-trusted.pem

4. Modifiez les fichiers de configuration (iTechPoz-*HostnameOfServerN*.dxc) de tous les serveurs sur Serveur1 comme suit :

   Modifiez la ligne suivante :

   address = tcp localhost port 509

   #address = tcp HostnameOfServerN port 509, tcp localhost port 509

   #dsa-flags = multi-write

   Et entrez :

   #address = tcp localhost port 509

   address = tcp HostnameOfServerN port 509, tcp localhost port 509

   dsa-flags = multi-write

   Remarques :

   - CA EEM utilise le numéro de port 509 comme le port DSA de données par défaut. Si vous avez configuré le serveur CA EEM pour qu'il utilise un port DSA de données personnalisé, remplacez 509 par le numéro de port personnalisé.
   - Pour utiliser des adresses IP et non pas des noms d'hôte, entourez l'adresse IP de guillemets droits (" ").

5. Modifiez iTechPoz.dxg du Serveur1 afin d'inclure les références du serveur secondaire.

   Exemple :

   ```
   # iTechPoz - iTechnology Repozitory
   # Source the knowledge files of the iTechPozRouter and iTechPoz DSAs.
   source "iTechPoz-HostnameofServer1-Router.dxc";
   source "iTechPoz-HostnameofServer1.dxc";
   source "iTechPoz-HostnameOfServer2-Router.dxc";
   source "iTechPoz-HostnameOfServer2.dxc";
   source "iTechPoz-ServerN-Router.dxc";
   source "iTechPoz-ServerN.dxc";
   ```

6. Créez un fichier iTechPoz-trusted.pem en concaténant le contenu du fichier iTechPoz-trusted.pem de chaque serveur secondaire ave le serveur1.

   Windows

   type <chemin absolu d'accès au fichier iTechPoz-trusted.pem du Serveur2> >> <chemin d'accès absolu au fichier iTechPoz-trusted.pem du Serveur1>

   UNIX ou Linux

   cat <chemin absolu d'accès au fichier iTechPoz-trusted.pem du Serveur2> >> <chemin d'accès absolu au fichier iTechPoz-trusted.pem du Serveur1>

   Exemple : saisissez "C:\Program Files\CA\Directory\dxserver\config\ssld\iTechPoz-trusted_2.pem" >> "C:\Program Files\CA\Directory\dxserver\config\ssld\iTechPoz-trusted.pem

7. Concaténez le contenu du fichier iTechPoz-trusted.pem de chaque serveur secondaire avec le fichier iTechPoz-trusted.pem résultant du Serveur1.

8. Copiez les fichiers suivants du serveur principal aux dossiers respectifs sur tous les serveurs secondaires :

   Remarque : Sauvegardez le fichier iTechPoz-trusted.pem et les fichiers de DSA de données et de routeur (iTechPoz*) des serveurs secondaires avant de procéder à la copie.

   UNIX et Linux

   $DXHOME/config/ssld/iTechPoz-trusted.pem
   $DXHOME/config/ssld/personalities/iTechPoz-*.pem
   $DXHOME/config/knowledge/iTechPoz*

   Windows

   %DXHOME%\config\ssld\iTechPoz-trusted.pem
   %DXHOME%\config\ssld\personalities\iTechPoz-*.pem
   %DXHOME%\config\knowledge\iTechPoz*

9. Editez le fichier iTechPoz.dxg sur chaque serveur secondaire. Le fichier iTechPoz.dxg doit contenir les informations suivantes :

   # iTechPoz - iTechnology Repozitory
   # Source the knowledge files of the iTechPozRouter and iTechPoz DSAs.
   source "iTechPoz-HostnameOfServerN-Router.dxc";
   source "iTechPoz-HostnameOfServerN.dxc";
   source "iTechPoz-HostnameOfServer1-Router.dxc";
   source "iTechPoz-HostnameOfServer1.dxc";
   source "iTechPoz-HostnameOfServer2-Router.dxc";
   source "iTechPoz-HostnameOfServer2.dxc";
   source "iTechPoz-ServerKRouter.dxc";
   source "iTechPoz-ServerK.dxc";

   Remarque : Les entrées pour localhost doivent apparaître avant celles des autres serveurs.

10. Définissez la possession et l'appartenance à un groupe pour les fichiers suivants sur dsa et etrdir respectivement, pour tous les serveurs CA EEM qui s'exécutent sous UNIX ou Linux. Exécutez les commandes suivantes :

    chown dsa:etrdir /opt/CA/Directory/dxserver/config/ssld/iTechPoz-trusted.pem
    chown dsa:etrdir /opt/CA/Directory/dxserver/config/knowledge/iTechPoz*

11. A l'aide des commandes suivantes, démarrez les services CA EEM sur tous les serveurs :

    Windows

    ssld start
    dxserver start all
    net start igateway

    Linux et UNIX

    su - dsa -c "ssld start"
    su - dsa -c "dxserver start all"
    $IGW_LOC/S99igateway start

    La configuration de basculement du magasin de données d'application a été enregistrée.

Basculement du serveur CA EEM

Remarque : veillez à installer la même version de serveur CA EEM sur tous les serveurs de l'installation de basculement (Server1, Server2,... et ServerN) et de synchroniser leur heure système.

Vous pouvez configurer Server1 pour qu'il fasse confiance aux sessions et certificats de tous les autres serveurs dans l'installation du basculement. Répétez la procédure suivante sur tous les serveurs de l'installation de basculement.

Pour configurer Server1 pour le basculement

1. Entrez l'URL https://server1:5250/spin.
2. Sélectionnez Administrateur iTech et cliquez sur OK.

   L'écran Connexion s'ouvre.
3. Entrez les informations d'identification de connexion comme suit, en fonction de l'option Type sélectionnée dans l'écran Connexion.

   Hôte

   Connectez-vous en tant que root ou administrateur.
4. Cliquez sur l'onglet Configuration, ajoutez ServerN comme Nom d'hôte dans le volet Hôtes iAuthority de confiance et cliquez sur Faire confiance.

   Une entrée est ajoutée au fichier iControl.conf et Server1 commence à faire confiance aux sessions de ServerN.

   Remarque : ajoutez tous les autres serveurs d'installation de basculement au volet Hôtes iAuthority de confiance.
5. Cliquez sur l'onglet iAuthority, entrez ServerN dans le champ Etiquette, recherchez l'emplacement du fichier de certificat PEM dans le volet Ajouter une racine sécurisée et cliquez sur Ajouter une racine sécurisée.

   Remarque : Le fichier de certificat PEM (rootcert.pem) se trouve dans le répertoire iTechnology de ServerN.

   Une entrée est ajoutée au fichier iAuthority.conf et Server1 commence à faire confiance aux certificats de ServerN.

   Remarque : ajoutez des entrées de certificat à tous les autres serveurs dans l'installation de basculement.

Configuration des fichiers CA EEM

Vous devez configurer le serveur CA EEM Server1 afin de recevoir la liste des serveurs disponibles en cas de besoin, qui sont des versions répliquées.

Pour configurer le serveur CA EEM Server1

1. Ouvrez le répertoire iTechnology de Server1.
   - **Windows** : %IGW_LOC%
   - **Linux et UNIX** : /opt/CA/SharedComponents/iTechnology (par défaut)
2. Ouvrez le fichier iPoz.conf et ajoutez la balise suivante :

   <BackboneMember>Server2</BackboneMember>
3. Démarrez et arrêtez iGateway.

   Windows

   net stop igateway
   net start igateway

   Linux et UNIX

   /opt/CA/SharedComponents/iTechnology/S99igateway stop
   /opt/CA/SharedComponents/iTechnology/S99igateway start

Vous devez également configurer le serveur CA EEM Server2 afin de recevoir la liste des serveurs disponibles en cas de besoin, qui sont des versions répliquées.

Pour configurer le serveur CA EEM Server2

1. Ouvrez le répertoire iTechnology de Server2.
   - **Windows** : %IGW_LOC%
   - **Linux et UNIX** : /opt/CA/SharedComponents/iTechnology (par défaut)
2. Ouvrez le fichier iPoz.conf et ajoutez la balise suivante :

   ```
   <BackboneMember>Server1</BackboneMember>
   ```

3. Démarrez et arrêtez iGateway.

   Windows

   ```
   net stop igateway
   net start igateway
   ```

   Linux et UNIX

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

Remarque : répétez la procédure précédente sur tous les serveurs CA EEM configurés dans l'installation de basculement.

Chapitre 9 : Fédération d'artefacts

Activation de la fédération d'artefacts

Si vous souhaitez utiliser la fédération d'artefacts, procédez comme décrit ci-dessous sur tous les serveurs CA EEM définis pour le basculement.

Activation de la fédération d'artefacts

1. Arrêtez le service iGateway.
2. Localisez et ouvrez le fichier iPoz.conf.
3. Modifiez la balise suivante :

   ```
   <ArtifactManager SessionTimeout="10"
   RequestTimeout="30"ArtifactStore="local/federated"></ArtifactManager>
   ```

   Où

   SessionTimeOut

   Indique la durée d'expiration (en minutes) des sessions exportées.

   Valeur par défaut : 10 minutes

   Plage:

   RequestTimeOut

   Indique la durée d'expiration (en minutes) des demandes de lancement.

   Valeur par défaut : 30 minutes

   Plage:

   ArtifactStore

   Indique l'emplacement de stockage des artefacts. La valeur "local" indique que les artefacts d'un serveur CA EEM ne sont pas disponibles sur d'autres serveurs CA EEM dans la configuration du basculement. Pour que les artefacts soient disponibles sur tous les serveurs CA EEM, définissez la valeur de ce paramètre sur "federated".

   Valeur : [local|federated]

   Valeur par défaut : local

   Remarque : Les paramètres SessionTimeOut et RequestTimeOut sont également présents dans le fichier eiam.conf. Si vous spécifiez ces paramètres dans le fichier eiam.conf, les valeurs du fichier eiam.conf prévalent.
4. Enregistrez et fermez le fichier.
5. Redémarrez les services iGateway.

   La fédération des artefacts est activée.

Chapitre 10 : Intégration avec CA SiteMinder

Ce chapitre traite des sujets suivants :

Intégration de CA SiteMinder dans CA EEM (page 89)
Configuration de la journalisation côté serveur CA EEM pour les modules CA SiteMinder (page 90)

Intégration de CA SiteMinder dans CA EEM

Pour intégrer CA SiteMinder dans CA EEM, exécutez les tâches suivantes dans l'Administrateur CA SiteMinder.

- Créez un agent dans CA SiteMinder pour communiquer entre CA EEM et le serveur de stratégie CA SiteMinder. Assurez-vous que l'agent prend en charge les agents 4.x.
- Créez un administrateur ou utilisez l'administrateur par défaut existant "SiteMinder" sur l'intégralité du système.
- Créez un répertoire utilisateur CA SiteMinder pour l'autorisation, répertoire utilisé par CA EEM pour extraire les attributs LDAP.
- Paramétrez le champ UniversalID afin d'identifier de façon unique un utilisateur dans le répertoire, tel que sAMAccountName ou UID. Vous pouvez définir le paramètre UniversalID à partir de l'interface utilisateur SiteMinder, Répertoires utilisateur, Propriétés, l'onglet Attributs utilisateur.
- Définissez l'attribut du mot de passe (RW) sur l'onglet Attribut de l'utilisateur sur userPassword.
- Créez un magasin de données CA SiteMinder pour l'authentification, magasin utilisé par CA EEM pour authentifier les utilisateurs.

  Remarque : Si les magasins d'utilisateurs d'authentification et d'autorisation sont les mêmes, utilisez le magasin d'utilisateurs existant créé pour l'autorisation.
- Créez un domaine avec le filtre de ressources défini sur "/iamt.html".
- Créez un domaine CA SiteMinder et ajoutez les répertoires utilisateurs, l'administrateur et le domaine au domaine.

Pour plus d'informations sur CA SiteMinder, consultez la documentation CA SiteMinder.

Configuration de la journalisation côté serveur CA EEM pour les modules CA SiteMinder

Pour configurer le niveau de journalisation pour l'intégration CA SiteMinder

1. Créez un fichier avec le contenu suivant et enregistrez-le sous le nom sm_log.properties :

   ```
   #filename: sm_log.properties
   #set the default logging level for the root logger
   .level = INFO
   #set the default logging level for the logger name com.ca.eiam
   com.ca.eiam.level = ALL
   ```

2. Dans le fichier sm.properties, remplacez le niveau de journalisation de l'enregistreur com.ca.eiam par l'une des valeurs suivantes :

   SEVERE

   Messages indiquant une erreur grave.

   WARNING

   Avertissements

   INFO

   Messages d'information

   CONFIG

   Messages de configuration statique

   FINE

   Informations de suivi

   ALL

   Indique que tous les niveaux de messages sont journalisés.

3. Enregistrez le fichier à l'emplacement suivant :

   Windows

   %IGW_LOC%

   Linux et UNIX

   /opt/CA/SharedComponents/iTechnology

4. Arrêtez le service iGateway.
5. Ouvrez le fichier iGateway.conf à partir de l'emplacement spécifié à l'étape 3 et ajoutez les balises suivantes à l'intérieur des balises <JVMSettings></JVMSettings> :

   ```
   <Properties name="eiam.sm">
   <system-properties>java.util.logging.config.file=sm_log.properties</system-properties>
   </Properties>
   ```

6. Enregistrez et fermez le fichier.
7. Démarrez le service iGateway.

Chapitre 11 : Journalisation du SDK CA EEM

Pour les SDK Java et C++, le nouveau processus de journalisation intégré à CA EEM utilise respectivement log4j et log4cxx comme cadres d'enregistreurs. L'ancien processus de journalisation utilisait un enregistreur d'utilitaire safe::util. Cette nouvelle fonctionnalité vous offre les avantages suivants :

- Nul besoin de redémarrer votre application si vous mettez à jour ou modifier les niveaux de journal.
- Vous pouvez gérer les propriétés de journalisation, telles que le nom de fichier, la taille du fichier, le nombre de fichiers journaux de sauvegarde, etc. en modifiant les paramètres du fichier de configuration de l'enregistreur.
- Vous pouvez classer par catégorie les messages enregistrés du SDK CA EEM en fonction des appels réseau et des statistiques de performance.

Remarque : La journalisation dans le SDK C# CA EEM n'est pas mise à jour. Vous devez continuer à utiliser safe::util pour consigner des messages dans le SDK C# CA EEM.

La journalisation vous permet d'enregistrer des messages, des erreurs et des informations générées par le SDK CA EEM. Dans le SDK CA EEM, la journalisation est contrôlée par les fichiers suivants :

- eiam.log4cxx.config
- eiam.log4j.config

Ces trois fichiers font partie du package SDK CA EEM, et sont placés par défaut dans le dossier Bin comme indiqué ci-dessous.

UNIX

/opt/CA/eIAMSDK/bin

Windows

C:\Program Files\CA\Embedded IAM SDK\safetool

A propos des fichiers de configuration de l'enregistreur

Les fichiers de configuration de l'enregistreur, eiam.log4cxx.config et eiam.log4j.config, permettent de configurer la journalisation du SDK CA EEM. Ces fichiers contiennent les composants majeurs suivants :

- Annexeurs
- Enregistreurs
- Enregistreur racine

Ces composants contiennent des paramètres configurables qui vous permettent de personnaliser le processus de journalisation en fonction des besoins de votre entreprise.

Annexeur

Un annexeur contient des paramètres qui contrôlent la journalisation de chaque enregistreur. Par défaut, les fichiers de configuration de l'enregistreur contiennent les annexeurs suivants :

SDK

Consigne les messages SDK dans un fichier journal. Spécifie le chemin d'accès y compris le nom de fichier du fichier journal.

Valeur par défaut : eiam.cppsdk.log

Remarque : Si vous déployez votre application sous le serveur Tomcat sur Windows, assurez-vous de bien utiliser une barre oblique (/) dans le chemin au lieu de la barre oblique inversée(\). Si vous utilisez une barre oblique inversée, le fichier journal ne sera pas créé au chemin spécifié ; au lieu de cela, il sera créé dans le dossier Apache Tomcat.

Réseau

Consigne les messages liés à l'appel réseau dans un fichier.

Valeur par défaut :eiam.network.cpp.log

Performances

Consigne les messages liés à l'appel des performances dans un fichier.

Valeur par défaut :eiam.network.cpp.log

Console

Affiche les messages enregistrés sur la console.

Par défaut, l'annexeur SDK est désactivé. Pour activer d'autres annexeurs, supprimez les chaînes de commentaire (<!-- et -->) de leur code respectif.

Un annexeur se compose des paramètres configurables suivants :

file

Spécifie le nom de fichier du journal de l'annexeur.

append

Indique si un ensemble de messages enregistré est ajouté au fichier journal. Si la valeur est true, l'ensemble de messages du journal est ajouté au dernier message du fichier journal.

BufferedIO

Indique si le dernier message enregistré a été mis en tampon. Si la valeur est True, les derniers messages enregistrés seront conservés en mémoire avant l'écriture dans le fichier journal. Ceci réduit les opérations d'E/S et a un effet positif si le niveau de journal est élevé.

Valeur : *[true|false]*

Valeur par défaut : False

Remarque : La taille par défaut du paramètre BufferedIO est de 8 Ko.

MaxFileSize

Spécifie la taille maximum du fichier journal. Si un fichier journal dépasse la taille maximum, un nouveau fichier journal log.1 est créé et le contenu du premier fichier est transféré vers le second. Le fichier journal contient désormais les derniers messages enregistrés. Si ce fichier dépasse aussi la taille maximum, un nouveau fichier journal intitulé log.2 est alors créé. Le contenu du fichier log.1 est transféré dans le fichier log.2, et le contenu du fichier journal est transféré dans le fichier log.1.

Valeur par défaut : 10 Mo

Minimum :10 Ko

Maximum : 2 Go

Remarque : La taille minimum du paramètre maxFileSize doit être supérieure ou égale à la taille du paramètre BufferedIO.

maxBackupIndex

Spécifie le nombre maximum de fichiers journaux de sauvegarde utilisés pour l'archivage des anciens journaux. Si le nombre de fichiers journaux dépasse la valeur d'index de sauvegarde maximum, le fichier muni des messages enregistrés les plus anciens sera supprimé.

Valeur par défaut : 1

Minimum : 1

Maximum : 12

ConversionPattern

Spécifie le format d'un message enregistré. Configure les modificateurs de format et les caractères de conversion pour définir le modèle de conversion.

Remarque : Pour de plus amples informations sur les modèles de conversion, consultez la rubrique log4j sur www.apache.org.

Exemple : Annexeur SDK

```
<appender name="SDK" class="org.apache.log4j.RollingFileAppender">
    <!-- Fichier journal sdk actif -->
    <param name="file" value="eiam.cppsdk.log" />
    <param name="append" value="true" />
    <param name="BufferedIO" value="false"/>
    <param name="maxFileSize" value="10000KB" />
    <param name="maxBackupIndex" value="1" />
    <layout class="org.apache.log4j.PatternLayout">
    <!-- Modèle du message enregistré -->
    <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
    </layout>
</appender>
```

Annexeur dans eiam.log4net.config

Un annexeur contient des paramètres qui contrôlent la journalisation de chaque enregistreur. Par défaut, les fichiers de configuration de l'enregistreur contiennent les annexeurs suivants :

SDK

Consigne les messages SDK dans un fichier journal. Spécifie le chemin d'accès y compris le nom de fichier du fichier journal.

Valeur par défaut : EIAM.C#SDK.log

Remarque : Si vous déployez votre application sous le serveur Tomcat sur Windows, assurez-vous de bien utiliser une barre oblique (/) dans le chemin au lieu de la barre oblique inversée(\). Si vous utilisez une barre oblique inversée, le fichier journal ne sera pas créé au chemin spécifié ; au lieu de cela, il sera créé dans le dossier Apache Tomcat.

Réseau

Consigne les messages liés à l'appel réseau dans un fichier.

Valeur par défaut : EIAM.NETWORK.C#SDK.log

Performances

Consigne les messages liés à l'appel des performances dans un fichier.

Valeur par défaut : EIAM.PERFORMANCE.C#SDK.log

Console

Affiche les messages enregistrés sur la console.

Par défaut, l'annexeur SDK est désactivé. Pour activer d'autres annexeurs, supprimez les chaînes de commentaire (<!-- et -->) de leur code respectif.

Un annexeur se compose des paramètres configurables suivants :

file

Spécifie le nom de fichier du journal de l'annexeur.

appendToFile

Indique si un ensemble de messages enregistré est ajouté au fichier journal. Si la valeur est true, l'ensemble de messages du journal est ajouté au dernier message du fichier journal.

maxSizeRollBackups

Indique le nombre maximum de fichiers journaux utilisés pour la sauvegarde des anciens journaux. Si le nombre de fichiers journaux dépasse la valeur d'index de sauvegarde maximum, le fichier muni des messages enregistrés les plus anciens sera supprimé.

Par défaut : 1

Minimum : 1

Maximum : 12

rollingStyle

Indique si le dernier message enregistré a été mis en tampon. Si la valeur est True, les derniers messages enregistrés seront conservés en mémoire avant l'écriture dans le fichier journal. Ceci réduit les opérations d'E/S et a un effet positif si le niveau de journal est élevé.

Valeur : *[true|false]*

Valeur par défaut : *f*alse

Remarque : La taille par défaut du paramètre BufferedIO est de 8 Ko.

maximumFileSize

Spécifie la taille maximum du fichier journal. Si un fichier journal dépasse la taille maximum, un nouveau fichier journal log.1 est créé et le contenu du premier fichier est transféré vers le second. Le fichier journal contient désormais les derniers messages enregistrés. Si ce fichier dépasse aussi la taille maximum, un nouveau fichier journal intitulé log.2 est alors créé. Le contenu du fichier log.1 est transféré dans le fichier log.2, et le contenu du fichier journal est transféré dans le fichier log.1.

Valeur par défaut : 10 Mo

Valeur minimum :10 Ko

Valeur maximum : 2 Go

Remarque : La taille minimum du paramètre maxFileSize doit être supérieure ou égale à la taille du paramètre rollingStyle.

ConversionPattern

Spécifie le format d'un message enregistré. Configure les modificateurs de format et les caractères de conversion pour définir le modèle de conversion.

Remarque : Pour de plus amples informations sur les modèles de conversion, consultez la rubrique log4j sur le site www.apache.org.

Enregistreur

Les enregistreurs vous permettent de contrôler la catégorisation des messages enregistrés liés au réseau et aux performances en fonction des niveaux, ainsi que leur affichage lors de l'exécution. Par défaut, les enregistreurs Network (Réseau) et Performance (performances) sont désactivés. Pour activer un enregistreur, supprimez les chaînes de commentaire de leur code respectif.

Un enregistreur contient les paramètres suivants :

logger name

Spécifie le nom d'un enregistreur.

additivity

Indique si les messages enregistrés liés au réseau et aux performances sont dupliqués dans le fichier journal SDK.

Valeur : *[true|false]*

Valeur par défaut : False

level value

Indique le niveau de journal d'un enregistreur.

Valeur : [*Trace*|*Debug*|*Info*|*Warn*|*Error*|*Fatal*|*Off*]

Vous trouverez ci-dessous les niveaux de journal, dans l'ordre de priorité :

Remarque : Plus le niveau de journal est élevé, plus les performances sont réduites CA EEM.

Trace

Indique un débogage de faible niveau. Il contient un flux de contrôle et transfère des arguments.

Debug

Indique les messages utilisés pour le diagnostic de problème. Il contient des informations contextuelles.

Info

Indique les informations contextuelles qui suivent l'exécution à un niveau grossier d'un environnement de production.

Warn

Indique un problème potentiel dans le système. Par exemple, si la catégorie de message correspond à la sécurité, un message d'avertissement doit s'afficher si une attaque de dictionnaire est détectée.

Error

Indique un problème critique dans le système. Le problème est irrécupérable et nécessite une intervention manuelle.

Fatal

Indique une exception d'application irrécupérable.

Off

Indique l'absence de journalisation.

Remarque : Le niveau de journal de l'annexeur SDK par défaut doit être Erreur.

Exemple : Enregistreur de performances

```
<logger name="Perform" additivity="false">
    <level value="trace"/>
    <appender-ref ref="Performance" />
</logger>
```

Enregistreur racine

L'enregistreur racine contrôle le niveau de journal de tous les annexeurs. Cependant, si le niveau de journal de l'annexeur référencé dans l'enregistreur racine est différent du niveau de journal spécifié dans l'annexeur parent, le niveau de journal ayant la plus haute priorité supplante celui qui a la plus basse.

Par exemple, si le niveau de journal d'un enregistreur racine est Erreur et que le niveau de journal de l'annexeur Network (Réseau) est Trace, le niveau de journal Trace supplante le niveau Erreur et le système traitera les messages enregistrés ayant le niveau de journal Trace lors de l'exécution.

Exemple : Enregistreur racine

```
<root>
    <priority value="error" />
    <appender-ref ref="SDK" />
    <appender-ref ref="Console" />
</root>
```

Configuration des fichiers de l'enregistreur

CA EEM vous permet de configurer les messages enregistrés liés au réseau, aux performances, à la console et aux classes SDK.

Pour configurer les fichiers de l'enregistreur

1. Ouvrez le fichier de configuration de l'enregistreur, eiam.log4cxx.config ou eiam.log4j.config, dans un éditeur de texte.
2. Activez les enregistreurs et les annexeurs.
3. Mettez à jour les paramètres de l'annexeur.
4. Enregistrez le fichier de configuration de l'enregistreur.

Exemple d'un fichier eiam.log4cxx.config

Vous trouverez ci-dessous un exemple du fichier eiam.log4cxx.config :

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">
<!-- Notez que ce fichier est lu par le sdk toutes les 60 secondes -->

<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/">

    <appender name="SDK" class="org.apache.log4j.RollingFileAppender">
        <!-- Fichier journal sdk actif -->
        <param name="file" value="eiam.cppsdk.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="false"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- Modèle du message enregistré -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
    </appender>

    <appender name="Network" class="org.apache.log4j.RollingFileAppender">
        <!-- Fichier de consignation des appels réseau -->
        <param name="file" value="eiam.network.cpp.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="true"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- Modèle du message enregistré -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
```

```
    </appender>

    <appender name="Performance" class="org.apache.log4j.RollingFileAppender">
        <!-- Fichier de consignation des appels performances -->
        <param name="file" value="eiam.performance.cpp.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="true"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- Modèle du message enregistré -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
    </appender>

    <appender name="Console" class="org.apache.log4j.ConsoleAppender">
        <!-- Journaux de la console -->
        <layout class="org.apache.log4j.PatternLayout">
        <!-- Modèle du message enregistré -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
    </appender>

    <!-- Supprimez le commentaire pour activer la journalisation des performances -->
    <!--
    <logger name="Perform" additivity="false">
        <level value="trace"/>
        <appender-ref ref="Performance" />
    </logger>
     -->

    <!-- Supprimez le commentaire pour activer la journalisation du réseau -->
    <!--
    <logger name="Network" additivity="false">
        <level value="trace"/>
        <appender-ref ref="Network" />
    </logger>
     -->

    <root>
        <priority value="error" />
        <appender-ref ref="SDK" />
        <!-- <appender-ref ref="Console" /> -->
    </root>
</log4j:configuration>
```

Exemple de fichier eiam.log4net.config

Exemple de fichier eiam.log4net.config :

```
<?xml version="1.0" encoding="utf-8" ?>

<Log4net>
	<appender name="SDK" type="log4net.Appender.RollingFileAppender">
		<file value="EIAM.C#SDK.log" />
		<appendToFile value="true" />
		<maxSizeRollBackups value="1" />
		<maximumFileSize value="10000KB" />
		<rollingStyle value="Size" />
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>

	<appender name="Network" type="log4net.Appender.RollingFileAppender">
		<file value="EIAM.NETWORK.C#SDK.log" />
		<appendToFile value="true" />
		<maxSizeRollBackups value="1" />
		<maximumFileSize value="10000KB" />
		<rollingStyle value="Size" />
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>

	<appender name="Performance" type="log4net.Appender.RollingFileAppender">
		<file value="EIAM.PERFORMANCE.C#SDK.log" />
		<appendToFile value="true" />
		<maxSizeRollBackups value="1" />
		<maximumFileSize value="10000KB" />
		<rollingStyle value="Size" />
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>

	<appender name="ConsoleAppender" type="log4net.Appender.ConsoleAppender">
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>
```

```
        <!-- Uncomment to enable Performance Logging -->
        <!--
        <logger name="Perform" additivity="false">
                <level value="ERROR"/>
                <appender-ref ref="Performance" />
        </logger>-->

        <!-- Uncomment to enable Network Logging -->
        <!--<logger name="Network" additivity="false">
                <level value="ERROR"/>
                <appender-ref ref="Network" />
        </logger>-->

        <root>
                <level value="ERROR" />
                <appender-ref ref="SDK" />
                <!--        <appender-ref ref="ConsoleAppender" />      -->
        </root>
</log4net>
```

Exemple de fichier eiam.lo4j.config

Exemple du fichier eiam.log4cxx.config :

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">

<!-- Note that this file is read by the sdk every 60 seconds -->

<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/">

        <appender name="SDK" class="com.ca.eiam.log4j.RollingFileAppender">
                <!-- The active sdk log file -->
                <param name="file" value="eiam.javasdk.log" />
                <param name="append" value="true" />
                <param name="BufferedIO" value="false"/>
                <param name="maxFileSize" value="10000KB" />
                <param name="maxBackupIndex" value="1" />
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
                </layout>
        </appender>

        <appender name="Network" class="com.ca.eiam.log4j.RollingFileAppender">
                <!-- The file to log Network calls -->
                <param name="file" value="eiam.network.java.log" />
                <param name="append" value="true" />
                <param name="BufferedIO" value="false"/>
                <param name="maxFileSize" value="10000KB" />
                <param name="maxBackupIndex" value="1" />
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
                </layout>
        </appender>

        <appender name="Performance" class="com.ca.eiam.log4j.RollingFileAppender">
                <!-- The file to log Performance calls -->
                <param name="file" value="eiam.performance.java.log" />
                <param name="append" value="true" />
                <param name="BufferedIO" value="false"/>
                <param name="maxFileSize" value="10000KB" />
                <param name="maxBackupIndex" value="1" />
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
```

```
                </layout>
        </appender>

        <appender name="Console" class="com.ca.eiam.log4j.ConsoleAppender">
                <!-- Logs to Console -->
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
                </layout>
        </appender>

        <!-- Uncomment to enable Performance Logging -->
        <!--
        <logger name="Perform" additivity="false">
                <level value="trace"/>
                <appender-ref ref="Performance" />
        </logger>
        -->

        <!-- Uncomment to enable Network Logging -->
        <!--
        <logger name="Network" additivity="false">
                <level value="trace"/>
                <appender-ref ref="Network" />
        </logger>
        -->

        <root>
                <priority value="error" />
                <appender-ref ref="SDK" />
                <!-- <appender-ref ref="Console" /> -->
        </root>

</log4j:configuration>
```

Chapitre 12 : Configuration de la prise en charge d'un serveur de répertoire externe

Ce chapitre traite des sujets suivants :

Configuration d'un répertoire externe avec CA EEM (page 105)
Configuration du serveur CA EEM pour l'échappement des barres obliques dans les noms de domaine renvoyés par les répertoires externes (page 107)
Configuration de la prise en charge d'un basculement de répertoire externe (page 107)
Connexion aux serveurs LDAP via TLS (page 108)
Connexion à des serveurs LDAP via SSL (page 108)

Configuration d'un répertoire externe avec CA EEM

Si vous utilisez des magasins de répertoires externes différents pour l'authentification et pour l'autorisation, configurez CA EEM comme suit :

- A l'aide du fichier iPoz.conf, configurez l'annuaire d'authentification externe avec CA EEM.
- A l'aide de l'interface administrative de CA EEM, configurez le serveur CA EEM avec le répertoire d'autorisation externe.

  Remarque : Pour plus d'informations sur la configuration des références au répertoire externe, consultez l'aide en ligne.

Pour configurer le serveur CA EEM pour qu'il utilise un répertoire externe pour l'authentification, définissez les options suivantes dans le fichier iPoz.conf localisé dans le dossier /CA/SharedComponents/iTechnology après l'installation.

Remarque : Vous devez arrêtez iGateway avant de modifier le fichier iPoz.conf et le redémarrez ensuite.

UseExternalAuthDirectory

Indique si vous souhaitez utiliser un répertoire externe différent pour l'authentification. Tapez True si c'est le cas. Le paramètre par défaut est False.

ExternalAuthDirType

Indique le type de répertoire externe. Les types actuellement pris en charge sont CA Identity Manager , Custom Mapped Directory, Microsoft Active Directory, Novell eDirectory, Novell eDirectory-CN et Sun One Directory.

ExternalAuthDirUserDn

Indique le paramètre UserDn pour le type de répertoire externe spécifié.

ExternalAuthDirPassword

Désigne le mot de passe utilisateur au format chiffré.

Remarque : Vous devez chiffrer le mot de passe à l'aide de la commande suivante et le coller dans le fichier ipoz.conf.

/iTechnology/safex -munge <*mot de passe en texte clair*>

ExternalAuthDirHost

Indique le nom de l'hôte sur lequel le répertoire externe a été configuré.

ExternalAuthDirPort

Désigne le port que le répertoire externe écoute.

ExternalAuthDirUserSearchPreFilter

Désigne le filtre de pré-recherche en fonction du répertoire externe. Vous pouvez rechercher n'importe quelle classe d'objets, les utilisateurs par exemple.

ExternalAuthDirUserSearchPostFilter

Désigne le filtre de post-recherche en fonction du répertoire externe. Vous pouvez rechercher n'importe quelle classe d'objets, les utilisateurs par exemple.

ExternalDirCacheFolder

Indique si le serveur CA EEM doit mettre en cache les dossiers des répertoires externes. Si cette balise est définie sur True, le serveur CA EEM met en cache les dossiers externes et vous pouvez accéder à ces dossiers à l'aide de l'interface administrative de CA EEM. Si cette balise est définie sur False, CA EEM n'affiche pas les dossiers des répertoires externes dans l'interface administrative de CA EEM.

Valeur : [True|False]

Valeur par défaut : **True**

Configuration du serveur CA EEM pour l'échappement des barres obliques dans les noms de domaine renvoyés par les répertoires externes

Pour configurer le serveur CA EEM pour qu'il utilise un répertoire externe pour l'authentification, définissez l'options suivante dans le fichier iPoz.conf localisé dans le dossier /CA/SharedComponents/iTechnology après l'installation.

Remarque : Vous devez arrêtez iGateway avant de modifier le fichier iPoz.conf et le redémarrez ensuite.

ExternalDirEscapeSlash

Spécifie si CA EEM doit ignorer la barre oblique (/) dans le nom distinctif renvoyé par des répertoires externes. Si vous souhaitez que CA EEM ignore la barre oblique, paramétrez cette balise sur True.

Remarque : CA EEM doit être configuré pour ignorer la barre oblique dans les noms distinctifs, sinon CA EEM ne pourra pas retrouver les objets.

Valeur : [True|False]

Valeur par défaut : **False**

Configuration de la prise en charge d'un basculement de répertoire externe

Vous pouvez étendre la capacité de CA EEM pour vous rabattre sur un autre serveur de répertoire externe qui soit une version répliquée du serveur.

Vous pouvez effectuer cette opération en fournissant le mappage correspondant dans le fichier iPoz.conf.

Remarque : Avant d'apporter toute modification au fichier iPoz.conf, vous devez arrêter iGateway et le redémarrer ensuite.

ExternalDirHostBackup

Indique le nom d'hôte du serveur de répertoire externe répliqué.

ExternalAuthDirHostBackup

Indique le nom d'hôte de l'autre serveur de répertoire externe à utiliser pour l'authentification des utilisateurs.

Connexion aux serveurs LDAP via TLS

Pour établir une connexion TLS au serveur LDAP, vous devez configurer le serveur LDAP pour qu'il accepte les certificats anonymes. Pour configurer EEM pour qu'il se connecte à LDAP sur TLS, procédez comme suit :

Pour configurer CA EEM pour qu'il se connecte à LDAP sur TLS :

1. Ouvrez l'interface utilisateur de CA EEM.
2. Cliquez sur Configurer, Serveur EEM.
3. Cliquez sur Utilisateurs globaux/Groupes globaux.

   Le volet Configuration du serveur EEM apparaît.
4. Activez l'option Référencer à partir d'un répertoire externe.
5. Entrez les détails de configuration.

   Remarque : Pour plus d'informations sur la configuration, consultez l'aide en ligne.
6. Sélectionnez Utiliser la couche TLS (Transport Layer Security).
7. Cliquez sur Enregistrer.

Connexion à des serveurs LDAP via SSL

Pour établir une connexion SSL aux serveurs LDAP, vous devez disposer des certificats suivants.

Certificat de l'autorité de certification

Vous pouvez obtenir ce certificat auprès d'une autorité de certification telle que Verisign ou Thwate. Ce certificat stipule que les certificats émis par cette autorité de certification sont valides et fiables.

Certificat du serveur LDAP

Vous devez obtenir ce certificat auprès d'une autorité de certification fiable. Ce certificat contient des informations sur le serveur LDAP et identifie le serveur LDAP auprès du client.

Remarque : Pour les connexions SSL, CA EEM prend en charge uniquement les certificats .pem.

Connexion de CA EEM à un serveur LDAP via SSL

Le processus suivant décrit le mode de communication entre le serveur CA EEM et le serveur LDAP via SSL.

1. Le serveur CA EEM se connecte au serveur LDAP à l'aide d'un certificat émanant d'une autorité de certification.
2. Le serveur LDAP vérifie le certificat de l'autorité de certification et, si le certificat est valide, établit une liaison avec le serveur CA EEM.
3. Le serveur LDAP envoie sa clé publique au serveur CA EEM pendant l'établissement de la liaison. La clé publique sert à chiffrer les données envoyées au serveur LDAP.
4. Le serveur CA EEM utilise la clé publique pour chiffrer les données et envoie ces dernières au serveur LDAP.
5. Le serveur CA EEM envoie un nom d'utilisateur et un mot de passe requis pour l'authentification auprès du serveur LDAP.

Configuration des connexions SSL

Vous devez suivre les procédures ci-dessous pour configurer la communication SSL entre le serveur LDAP et le serveur CA EEM.

1. Configuration du serveur LDAP pour utiliser des certificats
2. Configuration du serveur CA EEM pour communiquer via SSL

Configuration du serveur LDAP pour utiliser des certificats SSL

Pour configurer le serveur LDAP afin d'utiliser SSL, procédez comme suit.

1. Obtenez un certificat auprès d'une autorité de certification et installez le certificat dans le magasin de certificats fiables sur le serveur LDAP.
2. Obtenez un certificat de serveur auprès de l'autorité de certification et installez le certificat dans le magasin de certificats de serveur sur le serveur LDAP.
3. Dans le serveur LDAP, autorisez les connexions SSL.

Activation de SSL dans le serveur CA EEM

Pour activer SSL dans le serveur

1. Copiez le certificat de l'autorité de certification du serveur LDAP et enregistrez-le sur l'ordinateur exécutant le serveur CA EEM.
2. Ouvrez le fichier ipoz.conf et modifiez les balises suivantes.

   <ExternalDirSSL>

   Indique si la communication SSL est activée ou désactivée. Vous devez définir cette balise sur "true" pour activer la communication SSL.

   <ExternalDirCACertPath>

   Indique l'emplacement de stockage du certificat de l'autorité de certification sur l'ordinateur exécutant le serveur CA EEM.
3. Redémarrez iGateway.

Chapitre 13 : Configuration de la prise en charge d'un grand nombre de stratégies

Ce chapitre traite des sujets suivants :

Prise en charge d'un grand nombre de stratégies (page 111)
Configuration d'autres paramètres du serveur CA EEM sur AIX (page 111)
Configuration du client (page 112)

Prise en charge d'un grand nombre de stratégies

Remarque : CA EEM prend en charge un grand nombre de stratégies uniquement dans un environnement client compatible avec le kit de développement logiciel C++.

Vous devez configurer le serveur CA EEM et les clients avant d'enregistrer des applications qui utilisent un grand nombre de stratégies.

Remarque : CA EEM prend en charge jusqu'à 20 000 stratégies sur la plate-forme HP-UX.

Configuration d'autres paramètres du serveur CA EEM sur AIX

Vous devez effectuer les étapes supplémentaires suivantes pour configurer le serveur CA EEM afin de prendre en charge l'utilisation d'un grand nombre de stratégies sur AIX.

Pour configurer le serveur CA EEM sur AIX

1. A l'invite de commande AIX, modifiez les paramètres réseau à l'aide de la commande suivante :

   ```
   no -o tcp_nodelayack=1
   ```

2. A l'invite de commande AIX, augmentez la limite de processus à l'aide de la commande suivante :

   ```
   ulimit -d unlimited
   ulimit -f unlimited
   ```

Configuration du client

Vous devez configurer le client de manière à prendre en charge l'utilisation d'un grand nombre de stratégies.

Configuration du client pour tous les systèmes d'exploitation

Pour prendre en charge le déploiement d'un grand nombre de stratégies, vous devez configurer des clients pour tous les systèmes d'exploitation.

- Augmentez la durée de mise à jour du cache de l'application afin d'éviter les mises à jour du cache pendant l'enregistrement des applications à l'aide de Safex.

  Pour plus d'informations sur la mise à jour du cache, consultez le *Manuel de programmation.*

  Remarque : Nous vous recommandons de définir la durée de mise à jour du cache sur 3 600 secondes lors de l'enregistrement afin d'éviter les mises à jour du cache au cours de l'enregistrement. Après l'enregistrement, modifiez la durée de mise à jour du cache sur 30 secondes, ce qui correspond au paramètre par défaut.

- Activez la remise fiable d'événement.

  Pour plus d'informations sur la remise fiable d'événement, consultez le *Manuel de programmation*.

Chapitre 14 : Archivage des événements

Ce chapitre traite des sujets suivants :

Présentation (page 113)
Utilitaire de dégivrage des fichiers de base de données sauvegardée (page 114)

Présentation

CA EEM vous permet de générer des rapports sur les événements déclenchés par le serveur CA EEM et de gérer ces rapports. Le système d'archivage organise les fichiers archivés en trois états, décrits ci-dessous.

Fichiers de base de données compressée

Désigne les fichiers d'archive créés lorsque le nombre d'événements dépasse la quantité maximale de lignes dans une base de données d'événements. Les fichiers archivés compressés peuvent être consultés et consignés dans des rapports à partir du serveur CA EEM. Aucune donnée ne peut être insérée dans un fichier de base de données compressée. Les fichiers de base de données compressée sont disponibles sur le serveur CA EEM uniquement pendant la durée spécifiée dans le champ Nbre max. de jours d'archivage, parmi les paramètres du journal d'événements.

Fichiers de base de données sauvegardée

Désigne les fichiers d'archive à l'état compressé qui sont sauvegardés manuellement à un autre emplacement. Vous ne pouvez pas effectuer de recherches dans un fichier de base de données sauvegardée ni créer des rapports à partir d'un fichier de ce type. Les fichiers de base de données sauvegardée doivent être dégivrés avant d'être utilisés à des fins d'interrogation ou de génération de rapports.

Fichiers de base de données dégivrée

Désigne les fichiers d'archive à l'état sauvegardé qui sont restaurés afin que les utilisateurs puissent y effectuer des recherches ou générer des rapports à partir du serveur CA EEM. Les fichiers de base de données dégivrée sont disponibles dans le répertoire d'archivage uniquement pendant le nombre d'heures spécifié en tant que stratégie d'événement, dans les paramètres du journal d'événements.

Pour modifier les paramètres du journal d'événements

1. Connectez-vous à CA EEM.

   La page d'accueil de CA EEM apparaît.

2. Cliquez sur Gestion des rapports, Configuration, Services, Paramètres du journal d'événements.

   Les paramètres du journal d'événements apparaissent.

Remarque : Pour plus d'informations sur la configuration des services en vue de gérer des rapports, consultez l'*Aide en ligne*.

Utilitaire de dégivrage des fichiers de base de données sauvegardée

CA EEM fournit un utilitaire de dégivrage des fichiers de base de données sauvegardée. Vous devez dégivrer les fichiers sauvegardés et les restaurer à l'état compressé avant de pouvoir exécuter des requêtes dans les fichiers et afficher les rapports actifs. L'utilitaire sem offre cette fonctionnalité. Vous pouvez le télécharger à partir du site de support à l'adresse http://www.ca.com/fr/support/.

Pour installer l'utilitaire sem

1. Extrayez les fichiers compressés de l'utilitaire sem.
2. Définissez les variables d'environnement en fonction du système d'exploitation.

   Linux ou Solaris

   Export LD_LIBRARY_PATH = <*dossier_extraction_sem*>:$LD_LIBRARY_PATH

   AIX

   Export LIBPATH = <*dossier_extraction_sem*> :$LIBPATH

   HP-UX

   Export SHLIB_PATH= <*dossier_extraction_sem*> :$SHLIB_PATH

Remarque : Sous Windows, pour installer l'utilitaire sem, à partir de la ligne de commande, vous devez naviguer jusqu'au dossier extrait et exécuter sem.exe.

Syntaxe de l'utilitaire SEM

L'utilitaire sem présente la syntaxe suivante.

sem -h <nom_hôte> -u <utilisateur> -p <mot_passe> -listcolddb | -defrost <archive>

-h

Indique le nom d'hôte de l'ordinateur contenant les fichiers de base de données sauvegardée.

-u

Indique le nom d'utilisateur servant à l'authentification auprès du serveur CA EEM.

-p

Indique le mot de passe associé au nom d'utilisateur qui sert à l'authentification auprès du serveur CA EEM.

-listcolddb

Répertorie tous les fichiers de base de données sauvegardée stockés sur l'ordinateur hôte.

-defrost <archive>

Dégivre le fichier d'archive spécifié.

-fips

Indique que l'utilitaire sem utilise des algorithmes conformes à la norme FIPS.

Remarque : L'utilitaire sem doit être utilisé avec l'option -fips si le serveur CA EEM est configuré en mode FIPS uniquement.

Le tableau suivant décrit les valeurs renvoyées par l'utilitaire sem.

Valeur renvoyée	Description
0	Terminé
1	Arguments non valides
2	Nom d'utilisateur non valide
3	Echec d'authentification
4	Impossible de répertorier les fichiers de base de données sauvegardée
5	Impossible de dégivrer un fichier de base de données sauvegardée
6	Erreur d'initialisation

Dégivrage des fichiers de base de données sauvegardée

Vous devez dégivrer les fichiers sauvegardés et les restaurer à l'état compressé avant de pouvoir exécuter des requêtes dans les fichiers et afficher les rapports actifs.

Remarque : Avant le dégivrage, les fichiers de base de données sauvegardée doivent être copiés dans le répertoire d'archivage iTechnology\calm_archive.

Pour restaurer et dégivrer les fichiers de base de données sauvegardée :

1. Copiez le dossier calm_archive sauvegardé dans le dossier calm_archive actif.
2. Exécutez l'utilitaire sem à partir de la ligne de commande afin d'extraire une liste de tous les fichiers de base de données sauvegardée.

   sem -h <*nom_hôte*> -u <*nom_utilisateur*> -p <*mot_passe*> -listcolddb

   Serveur CA EEM en mode FIPS uniquement.

   sem -h <*nom_hôte*> -u <*nom_utilisateur*> -p <*mot_passe*> -fips -listcolddb
3. Exécutez l'utilitaire sem pour dégivrer les fichiers de base de données sauvegardée.

   sem -h <*nom_hôte*> -u <*nom_utilisateur*> -p <*mot_passe*> -defrost <*archive*>

   Serveur CA EEM en mode FIPS uniquement.

   sem -h <*nom_hôte*> -u <*nom_utilisateur*> -p <*mot_passe*> -fips -defrost <*archive*>

   Les fichiers de base de données sauvegardée sont restaurés et dégivrés.